International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Threats and Mitigation Strategies in Remote Work Scenarios: A Cybersecurity Perspective Post - COVID-19

Dhaval Gogri

Fremont, USA
Email: *dhaval. gogri17[at]gmail.com*

Abstract: ***The Covid - 19 pandemic brings far - reaching implications to the workplace, with adoption of remote work dramatically accelerated as well as new significant cybersecurity threats. There is a strong need to push for more stringent cybersecurity practices than ever, now that malware, ransomware, and phishing attacks are increasing cyber threats. This review paper synthesizes the emerging challenges and trends in cybersecurity prompted by the pandemic, focusing specifically on the surge of cyber threats that have exploited vulnerabilities in decentralized work structures. The paper cites evidence of the rise in cyberattacks targeting various institutions, from ransomware to phishing and Distributed Denial of Service (DDoS) incidents, and outlines the motives that fuel these increased activities. Discuss the paper as a whole. The paper reviews various tools and technologies that organizations use to combat these threats; this includes VPNs, RBI, and advanced endpoint protection solutions. Also, it highlights that there is a need for all - rounded mitigation strategies such as user education, MFA, and very robust endpoint security measures. This review establishes the analysis of nexus between Covid - 19 and cybersecurity - critical to further research continuously being done in proactively creating organizational resilience against the ever - evolving cyber threats in a post - pandemic digital environment.***

Keywords: Cyber Threats, Mitigation Strategies, COVID - Pandemic, VPN, RBI, Endpoint Protection

1. Introduction

Our way of life has drastically changed as a result of the Pandemic of COVID - 19, which has also caused a excessive contract of indecision and fear [1] [2]. Companies have been forced to swiftly and extensively adapt to the requirement for remote work. Some companies have rethought their physical workplaces and regulations to make it possible for employees to work remotely without proper training or preparation. As it stands, most of these companies and groups lack the plans necessary to pull off such a dramatic change so quickly. Efforts at the national level to better monitor the spread of the COVID - 19 virus [3], also helped to significantly boost the numeral of companies that enable their workers to work remotely by recommending remote work for anybody whose work circumstances permit it. However, throughout the pandemic, online dangers have escalated, underscoring the necessity for businesses to modify their methods of cyber - risk management [4] [5].

With the proliferation of remote work comes a pressing need to priorities cybersecurity. Remote work environments introduce unique security challenges, including unsecured Wi - Fi networks, endpoint vulnerabilities, and the potential for data openings [6]. Therefore, the security of remote working needs to be ensured to ensure sensitive data is protected, regulatory compliance is met, and the cyber threat profile is managed when dealing with organisational assets. One of the biggest challenges here would be ensuring remote and multi - location/ device access to corporate resources securely in a manner that ensures discretion and morality of data. In fact, most of the remote workers are even not aware of the cybersecurity best practices they may incidentally be violating. Also, another reason, which increases security risks and hence would be difficult for the organizations to enforce uniform security policies and controls, is use of personal devices and unsecured networks. The spread of the main cyberthreats caused by COVID - 19 is shown in Figure 1.

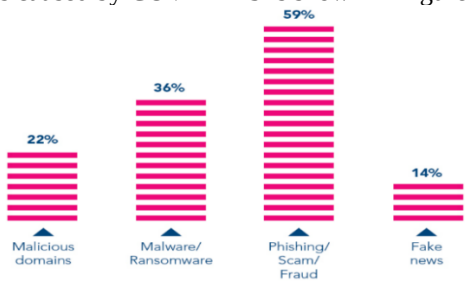

Figure 1: Distributed of the key COVID - 19 inflicted cyber threats [7]

This would call for intense security measures that fit within the remote work environment, which will include endpoint protection solution deployments, multi - factor authentication for remote access, and data encryption both at rest and in motion. Besides, investment in training and awareness programs by organisations would create an enlightenment amongst the employees to be working remotely on what cyberspace risks are and best practices in cybersecurity. The companies can thus protect their valuable digital assets by using a proactive means to secure remote workforces and implementing novel cybersecurity solutions that mitigate risks in today's landscape of working remotely.

The objective of this research work is to critically evaluate the effect of COVID - 19 on cybersecurity through distant work and identify effective strategies for risk mitigation in the wake of related risks. Motivations for the Study The organisational, national, and international imperative are based on significant and rapid shifts toward remote work, which expose organisations to new vulnerabilities and cyber threats. This research helps in building organizational resilience and a culture of cybersecurity awareness by

discussing the challenges and providing actionable solutions: consequently, it strengthens businesses to be well - equipped for future disruptions.

The following contribution of this paper as:

- Highlights new cyber threats arising from the shift to remote work during the pandemic.
- Provides actionable cybersecurity measures tailored for remote work environments.
- Proposes a structured framework for cybersecurity training to promote a security - conscious culture.
- Introduces metrics for organizations to evaluate their cybersecurity readiness and adaptability.
- Offers guidance on developing flexible cybersecurity strategies for future disruptions.

The following paper are organized as: Section II provide the Covid - 19 Pandemic Impacts on Cybersecurity, Section II discusses the Rise Of Remote Work Post - Covid - 19 with tools and technologies, Section III give the overview of Overview Of Cyber Threats in Remote Work Scenarios, Section IV and V discussed the Mitigation Strategies For Securing Remote Work and Remote Work Post - Covid - 19 Presents Several Challenges with future work, Then Section VI provide the existing work on this research are with comparative analysis table and last Section VII provide paper conclusion.

2. Covid - 19 Pandemic Impacts On Cyber Security

Cross - border transmission of infectious diseases affects state security, including the cybersecurity environment, as the COVID - 19 experience shows. With the sudden shift to decentralized work, new vulnerabilities emerged; thus, the number of cyberattacks dramatically increased. Use of personal devices, unsafe home connections, and cloud spaces provided the fraudulent individuals with new opportunities to act on the visible weaknesses [8]. This exceptional shift led the businesses to modify their security strategies for focusing on the issues of continuing remote access solutions, protection of end points, and the staff awareness. The figure 2 demonstrations the effect of COVID - 19.

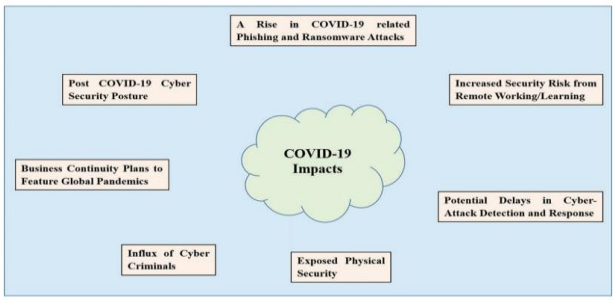

Figure 2: Impact of COVID – 19

Some COVID - 19 impacts are discussed below:

- **Post COVID - 19 Cyber Security Posture:** The pandemic of COVID - 19 has significantly impacted the world economy, with some analysts projecting a recession as one of its aftereffects [9] [10]. In such a situation, the organisations are downsizing by severing business lines in order to reduce their financial losses. This also applies to supposedly non - critical cybersecurity operations.
- **Exposed Physical Security:** In certain places, having a dependable power source and quick internet connection may be considered a luxury. As a result, employees of these businesses must rely on public areas to access free internet and electricity [11]. This conduct may unintentionally expose the computer hardware and private data stored on the device to theft or damage.
- **Influx of Cybercriminals:** In order to deal with the consequences of COVID - 19, businesses throughout the world are reducing their workforces. The majority of professionals have also lost their sources of income as a result of the various travel restrictions imposed by governments worldwide. Since idle internet users who have lost their employment due to COVID - 19 may perceive this as a chance to profit from the pandemic, this action is likely to accelerate the expansion of cybercriminals. [12]

3. Rise of Remote Work Post - Covid - 19

Situations where employees effort remotely, usually from home or another remote place, are referred to as remote work scenarios [13]. This strategy makes use of digital technology to sustain productivity, connectedness, and teamwork inside the company [14]. The COVID - 19 epidemic hastened the industry - wide adoption of remote work. Business continuity, employee wellness, and meeting evolving workplace expectations were the three main reasons why organisations embraced remote work.

Figure 3: Illustration of remote work scenarios

Here is a figure 3 illustration of remote work scenarios, showcasing people working from different locations using a variety of digital tools. This picture embodies the adaptability and connectedness common to contemporary remote work settings.

1) Tools and Technologies in Remote Work Scenarios

Remote work relies heavily on internet - based tools, such as:

a) Video Conferencing Software

Some of the available platforms targeted toward real - time communications include: Microsoft Teams, Zoom and Google Meet. Like Zoom, Microsoft Teams, andGoogle Meet, these platforms offer virtual meetings and collaborations: this has proven to be very important in enhancing how teams can relate to each other through such features as screen sharing and breakout rooms but becomes a security risk if not properly managed [15].

b) Collaboration Platforms

Tools like Slack, Microsoft Teams, and Google Workspace make the communication and project management seamless using the instant messaging and file exchange facilities. They, in fact, encourage collaboration but can become a perfect information - overload nightmare, and transparent communication protocols need to be set up [16].

c) Cloud Storage Services

Teams may safely access and share files and modify documents in real time with the help of services like Google Drive, Dropbox, and OneDrive. They also have backup and recovery capabilities from data loss but should have controls of access in place to prevent accidental leaking of sensitive information [17].

d) VPNs (Virtual Private Networks)

VPN provide companies with a safe encoded construction to the resources of the company and keeps sensitive information safe while accessing company networks from an external source. It helps to maintain the privacy of the data but decreases internet speed; therefore, their usage should be looked after and is also communicated to the employees so that they can use them appropriately [18]. Figure 4 shows the VPN.

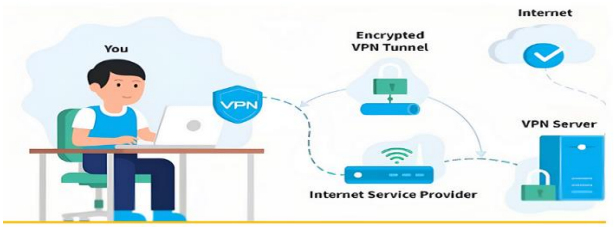

Figure 4: Virtual Private Networks

Because it reroutes traffic through an overseas server, a VPN encrypts your data and conceals an IP address, thus increasing privacy and making surfing quite safe, especially on public Wi - Fi networks. VPNs are therefore a crucial aspect of keeping yourself safe online and anonymously online.

e) RBI (Remote Browser Isolation)

RBI is a security technology that isolates the browsing activity from the corporate network, therefore isolating potential threats. Security is improved since phishing attacks and web - based threats are minimized [19] [20]. Implementing RBI can improve the user experience and at the same time maintain productivity while guarding sensitive corporate information. The following figure 5 shows the Remote Browser Isolation.

Figure 5: Remote browser isolation processes

This is illustrated as figure 5. RBI technology is applied in the case of remote browser isolation to make sure that process depicted above is enacted. The moment the user requests a website, RBI initiates a session with the destination website. Then code on that website is executed safely in an isolated environment so that no potential infections reach the user's device. Full browsing is transmitted to a user without risk in form of a safe visual stream. It also ensures that the user will be able to interact with any perhaps maliciously - infected website, since threats have different manifestations.

f) Endpoint Protection

Endpoint protection solutions secure those devices, such as laptops, smartphones, and tablets connected to the corporate network. They protect the endpoint from malware, ransomware, and other cyber threats so that each endpoint is secured and monitored. Organizations have to ensure robust measures of endpoint security in cases of a remote work environment as it rises above the threat of increased cyberattacks [21].

g) Secure Access

In this area, secure access technologies like [22] IAM and Zero Trust security models are engaged to limit exposure in a company since they ensure the exclusive involvement of only authorized users with the resources of a company [23] [24] [25]. The systems are intended to enhance authentication levels to multi - factor authentication, for example, to establish the identity of users before access is given [26], This translates to an adoption of the Zero Trust approach that enables continuous validation and monitoring of access regarding data and applications to minimize the risks coming from unauthorized access and data breaches.

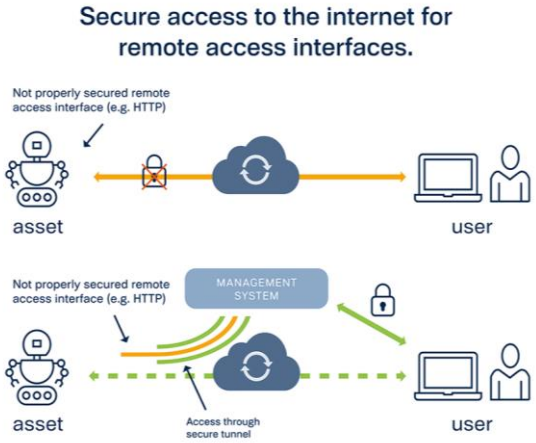

Figure 6: Secure remote access interfaces

Figure 6 The above figure describes how the proper security of the remote - access interfaces is a requirement. On top, an asset has been connected directly with a user through an unsecured remote - access interface and hence exposes it to possible exploits. On the other hand, at the bottom, the asset and the user have been connected through a secured tunnel as shown, which prevents illegal entry and hacking of data. This denies unauthorized access and protects the sensitive information from attacks.

2) Benefits of Remote Work Scenarios

Benefits of Remote Work Scenarios, such as:

- Increased Flexibility: They are allowed to have more freedom of where and when they are to work.
- Reduced Commute Time: Then, the end of the daily commute eliminates time spent traveling and reduces stress.
- Potential Productivity Gains: Some employees report higher productivity due to fewer office - related distractions.

4. Overview of Cyber Threats in Remote Work Scenarios

The shift to remote work has upended traditional IT defenses, making online access the norm and exposing many companies unprepared for this sudden change. Without the protection of company networks, end users are now the frontline of cybersecurity. Education has become a critical defense [27] [28], especially with a surge in coronavirus - related malware, including trojans and ransomware, spreading rapidly across virtual private networks. With attackers increasingly exploiting vulnerabilities in sectors like healthcare [29]and finance [30], cybersecurity has become more challenging than ever [31] [32]. The pandemic has only intensified the requirement for vigorous security procedures in a highly interconnected digital creation. As remote work becomes the norm, organizations must prioritize cybersecurity education and proactive defenses to safeguard their systems from evolving threats. [33] [34]. The figure 7 shows the cyber security threats in remote work scenario.

Critical infrastructure (CI) involves elements that are fundamental to the normal operations of the human society [1], an can be defined as referring to any asset, system or part thereof which is critical for the maintenance of vital societal functions, health, safety, security, economic or social well - being of people, and the disruption or destruction of which would have a very substantial impact as a result of the failure to maintain those functions [2]. Arguably, it may be viewed as a nation's economic "central nervous system" [3] – making it difficult for nations without a properly functional, or indeed with vulnerable CI to attain and sustain its national goals of social and economic progress and development. Examples of CIs include; Energy (electricity, oil, natural gas), Chemical, Industrial Control, Dams, Defence Industries, Emergency Services, Financial Services, Food and Agriculture, Government facilities, Commercial Services, Health and Public Health, Transportation, (Railways, Roads, Highways, Aviation, Shipping and Ports), Water and Waste water, Information Technology and Telecommunication, Nuclear [2], [4], [5].

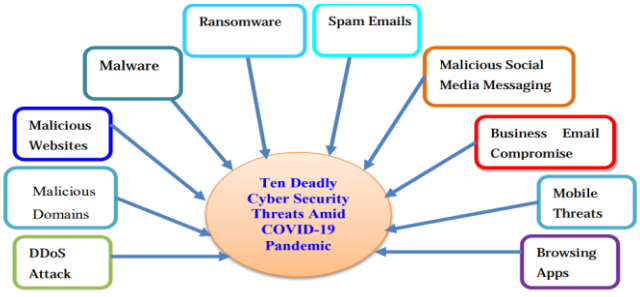

Figure 7: Cyber Security Threats in remote work scenario

The following are the types of cyberattacks in remote work

- **DDOS Attack:** During the current coronavirus outbreak, there was a significant increase in Distributed Denial of Service (DDoS) assaults on several healthcare organisations and government agencies. The goal of this distributed denial of service attack is to disrupt the company's normal operations by flooding its websites with fake and automated users.
- **Malicious Domains:** The phrase "coronavirus" has recently surfaced on a lot of registered domains on the Internet, and it is becoming more and more common in these and many other registered domains every day. In addition to launching spam campaigns and new websites, cybercriminals also carry out DOS assaults that impact the servers of several businesses and other types of attacks like phishing and malware insertion.
- **Malware:** In the current coronavirus pandemic scenario, cybercriminals are constantly spreading malware around the world. A trojan is introduced into the victim's computer through a variety of websites and links, and if the user enters the page or clicks on a link, it starts to reason a diversity of cyber glitches.
- **Ransomware:** Numerous ransomware attacks are now underway, targeting various sectors of society such as educational institutions, government entities, and hospitals. Ransomware, once activated, encrypts the victim's server's private files, locks them, and then demands payment to decrypt them.
- **Spam Emails:** Spam emails have always been used extensively by hackers and spammers to achieve their goals. Spam emails with coronavirus - related information have spread around the world during the coronavirus epidemic, interfering with users' regular activities.
- **Malicious Social Media Messaging:** These days, social media is easily accessible to everyone. Attackers take use of this to carry out their malevolent actions, such as infecting the victim's computer with a trojan, etc. Further, it has come to light that hackers have seized the opportunity to offer free [35].

5. Mitigation Strategies for Securing Remote Work

Continuous efforts to lessen or completely eradicate the long - term danger that natural hazards and their consequences pose to people and property are known as mitigation. By altering the built environment, some steps may be done to lower the risk and possible outcomes of man - made hazards, hence reducing the loss of life and property [36]. Additionally, it lessens vulnerability by lowering the possibility of further losses [36]. Mitigation facilitates a more efficient and expedited recovery process by minimising unexpected incidents and their consequences. It reduces unforeseen challenges, ensuring a more streamlined response to disruptions [37]. Additionally, as previously noted, effective mitigation can eliminate the need for extensive restoration of operations, thereby enhancing overall resilience and preparedness. [38]

a) Types of mitigation techniques For Securing Remote Work

Mitigation efforts must be adopted in view of the obstacles and complexity that digital inequalities provide to the

population's resistance to COVID - 19. These remedies aim to lessen the impact of digital inequality on COVID - 19 vulnerability as well as the consequences of the COVID - 19 crisis on digital disparities [39]. Figure 8 shows some mitigation Strategies of cyber - attacks in COVID - 19 duration.

Figure 8: Mitigations Strategies

The following mitigation Strategies of cyber - attacks discussed below:

- **User Education**: The weakest link in a security system determines how strong it is. It is often believed that humans are the weakest link in security systems. Therefore, reducing an organisation's vulnerability to cyberattacks requires raising user understanding of cybersecurity through continual training. Just 11% of companies, according to a new report, have given cybersecurity training to non - cybersecurity staff members in the previous 12 months.
- **Endpoint Protection**: That was the case with endpoint protection tools as more and more remote employees used personal devices for work. Endpoint protection services make use of real - time protection, malware, and threat identification, plus automated remediation for other corporate - owned and personally - owned devices for remote work.
- **Remote browser isolation (RBI):** RBI proved to be a new way to shield far users from Web threats. In this way, while using online browsers at RBI, malicious applications are not downloaded to the general users' computers and plates are not switched for the money; the virus is not sent to the users' computers.
- **Virtual Private Network (VPN):** Data transmissions between two Internet - connected devices can be securely encrypted using a VPN and have become the de facto norm for online privacy. A virtual private network VPN allows companies to extend security policies to remote workers while maintaining the privacy and integrity of sensitive information.
- **Enable multi - factor authentication (MFA):** In addition to a login and password, MFA uses a one - time code sent to a mobile device by SMS or an authentication app to further strengthen security. Password guessing, theft, and brute force cyberattacks may be greatly mitigated with the use of MFA. An employee's login credentials, password, and a one - time code sent to her mobile device will be required before she may get access to the workplace network from the comfort of her own home.
- **Ensure all devices firmware is up - to - date:** Update the firmware and operating system of all devices and equipment to the most recent versions to protect them from known vulnerabilities. Maintaining up - to - date security patches may reduce the possibility of a zero - day attack.
- **Ensure that up - to - date anti - malware software is activated in all network - connected devices:** Cybercriminals use a variety of viruses to attack susceptible individuals. Regular and current anti - malware software may lower the likelihood of malware - driven cyberattacks because millions of new malware strains are created each year [40].

6. Remote Work Post - Covid - 19 Presents Several Challenges and Future Work in Cybersecurity

The shift to isolated work post - COVID - 19 presents several challenges in cybersecurity:

- **Increased Attack Surface:** The attack surface is greatly increased when personal devices and home networks are used for work, making it challenging for IT teams to sufficiently safeguard every endpoint.
- **Lack of Visibility:** Organizations often have limited visibility into the devices and networks employees use remotely, leading to potential blind spots in identifying threats or suspicious activities.
- **Human Error:** Employees unfamiliar with best security practices in a remote setting are more prone to Human mistakes include using weak passwords, falling for phishing schemes, and managing sensitive data improperly.
- **Difficulty in Implementing Security Policies:** Consistently applying and enforcing security policies across a dispersed workforce can be challenging, especially when employees use different systems and devices.
- **Scalability of Security Solutions:** Many organizations were forced to scale remote access quickly, and their existing security solutions were not designed for this rapid growth, leading to compromised effectiveness and gaps in security coverage.
- To address these challenges, future work in cybersecurity for remote work environments can focus on:
- **Adaptive Security Solutions:** Development of more adaptive security solutions that can automatically adjust to dynamic environments, such as EDR systems that monitor devices in real - time and take proactive actions.
- **Zero Trust Security Models:** Continuing to evolve and adopt Zero Trust models that assume no implicit trust, with ongoing verification of users and devices regardless of location.
- **Advanced User Awareness Programs:** Enhancing user awareness and education through immersive training, such as virtual simulations and gamified experiences, to better prepare remote employees to recognize and react to potential threats.
- **AI - Driven Threat Detection:** Leveraging artificial intelligence to improve threat detection capabilities in remote settings. Machine learning models can analyze patterns to identify anomalies in user behavior and prevent potential breaches.
- **Unified Endpoint Management (UEM):** Future efforts should also emphasize Unified Endpoint Management to

provide better control and monitoring of all devices used for remote work, ensuring consistent policy enforcement and security updates.

- **Improved VPN and Network Security**: Research into more secure, scalable, and user - friendly VPN alternatives or secure access service edge (SASE) solutions will be crucial for ensuring secure remote connectivity.

Addressing these challenges through continuous development in cybersecurity technology, user training, and proactive policies will be key to ensuring the long - term security of remote work environments.

7. Literature Review

This section explores the existing body of work in the field of cyber security threats and mitigation strategies in pandemic. This paper analyses the COVID - 19 pandemic from a cyber - crime perspective and highlights the range of cyber - attacks experienced globally during the pandemic. Cyber - attacks are analysed and considered within the context of key global events to reveal the modus - operandi of cyber - attack campaigns. The analysis shows how following what appeared to be large gaps between the initial outbreak of the pandemic in China and the first COVID - 19 related cyber - attack, attacks steadily became much more prevalent to the point that on some days, 3 or 4 unique cyber - attacks were being reported. The analysis proceeds to utilise the UK as a case study to demonstrate how cyber - criminals leveraged key events and governmental announcements to carefully craft and design cyber - crime campaigns.

This study Chowdhury et al. (2020) examines the potential effects of cybersecurity on individuals. It outlines some of the most popular techniques for tricking people into disclosing information that might lead to financial loss or theft and/or intellectual property theft. It also outlines some standard precautions that may be performed to eliminate a lot of the hazards. Overall, with particular supporting evidence, this study has attempted to identify the majority of the possible hazards on the digital platform. The article also focusses on some efficient ways to deal with these important problems, particularly in light of the COVID - 19 pandemic [41].

This study Bokan and Santos, (2021) explains a novel threat - based method for assessing cybersecurity architectures that enables businesses to see their cybersecurity defences from the perspective of an opponent. The plan is based on a technique that the Department of Homeland Security improved upon after it was developed by the Department of Defence. The threat - based method uses a cyber threat framework to catalogue all known threat actions and ranks safeguards (cybersecurity architectural capabilities) based on their ability to: a) detect, b) prevent, and c) assist in recovering from the threat action [42].

In order to make a framework of recommendations for the implementation of cybersecurity strategies that guarantee an acceptable level of information security, this research program Elkhannoubi and Belaissaoui, (2016) aims to identify the essential components of an effective cybersecurity strategy that can be addressed to organisations (administration or enterprise). Our primary goal is to create an effective cybersecurity strategy platform by building on prior cybersecurity strategy successes and reviving international standards and reference materials like ITIL and ISO27002 [43].

This study Himdi, Ishaque and Ahmed, (2021) focuses on the Cybersecurity challenges faced by smart cities in the awaken of the COVID - 19 disease. With the pandemic still there, cybercriminals and state - sponsored groups have taken advantage of attacking intelligent cities worldwide. This research primarily focuses on a correspondence between the increase in the attacks on different cyber - sectors in smart cities and the ongoing pandemic [44].

This study Tanna, Sridaran and Dobariya, (2019) intends to analyse the various mitigation strategies for security issues that may arise in various cloud computing settings in order to help cloud consumers, researchers, and service providers. The cloud computing concept is integrated for the current study and its implications and risks are identified in terms of security [45].

In order to assist software developers in creating safe applications, this effort Romero M and Haddad, (2009) looks into security flaws and mitigation techniques. Examining the software from various perspectives, such as the external environment that supplies the data needed for processing, the data stored and retrieved internally, the algorithms and computations run on the data, the results, and finally, the software's extensibility and mobile capabilities, the study identifies common vulnerabilities and relevant mitigation strategies. The secret to comprehending the challenge of creating safe software applications is to look at software security from these perspectives [46].

Table 1: Summary of literature review in the field of cyber security threats and mitigation strategies pandemic

Reference	Focus Area	Proposed solution	Key Features	Application domain	Challenges addressed
[41]	Cybersecurity impact on individuals	Raising awareness and educating users to prevent manipulation and theft	Highlighting manipulation method, common risks, and protective measures	Individuals, digital platforms	Social engineering, phishing, data theft
[42]	Threat–based state evaluation of cybersecurity architectures	Use of a cyber threat framework to evaluate and score architecture protections	Threat detection, protection, and recovery evaluation	Organisational cybersecurity	Adversarial threats, evaluation of protection systems
[43]	Cybersecurity strategies of organizations.	Development of cybersecurity strategy based on standards like ISO27002 and ITIL.	Framework for information security strategies, focusing on global standards.	Enterprises, administrative bodies	Implementation of effective cyber security strategies

[44]	Cybersecurity challenges in smart cities during COVID - 19	Real - time cybersecurity protocols to counter increased cyberattacks on smart cities.	Focus on correlation between pandemic and rising cyberattacks state - sponsored threats.	Smart cities, urban infrastructure	COVID - 19 exacerbated cyberattacks on smart infrastructure
[45]	Security threats in cloud computing	Development of threat models and cloud security frameworks for service providers	Security threat analysis, mitigation strategies for cloud computing	Cloud computing	Cloud security, unauthorized access, data breaches
[46]	Security vulnerabilities in software development	Secure software development through mitigation strategies for identified vulnerabilities	Focus on input validation, secure algorithms, and protection at various stages of software	Software development, mobile apps	Software vulnerabilities, insecure algorithms, data management

8. Conclusion

The COVID - 19 pandemic has irrevocably altered the workplace dynamic, ushering in an era of remote work that presents both opportunities and vulnerabilities. With the new normal, organizations have surely entered the era of robust cybersecurity measures. The same global scenario brought a massive change to the face of cybersecurity, forcing organizations to adapt without any delay to remote working amidst rampant cyber threats. The risks of remote working, including insecure networks, unprotected devices, and lack of awareness among employees about cybersecurity, could pose perilous threats to the assets of an organization and sensitive information. These have to be met by extensive security measures, including endpoint protection that is strong, user training proactive, and adoption of advanced authentications, thus making the organisations better positioned to live with the complexity of the digital environment and minimize the risks caused by changing cyber threats. In the future, it will be very important for organizations to update their cybersecurity strategy on constant learning of emerging threats and new types to develop their resilience and security in this highly connected world.

References

[1] L. Atstāja, D. Rūtītis, S. Deruma, and E. Aksjoņenko, “Cyber Security Risks And Challenges In Remote Work Under The Covid - 19 Pandemic, ” 2021. doi: 10.15405/epsbs.2021.12.04.2.

[2] S. Pandey, “Leveraging Workday For Effective Covid - 19 Vaccination Tracking: Integrating Custom Objects And Security Features In Human Capital Management Systems, ” *Int. J. Bus. Quant. Econ. Appl. Manag. reseacrh*, vol.7, no.1, pp.56–63, 2021.

[3] S. Saiful Amin, “Online Purchase Intention and Cyber Frauds during COVID - 19, ” *Trends J. Sci. Res.*, 2021, doi: 10.31586/ujfe.2021.113.

[4] L. Wang and C. A. Alexander, “Cyber security during the COVID - 19 pandemic, ” *AIMS Electronics and Electrical Engineering*.2021. doi: 10.3934/ELECTRENG.2021008.

[5] S. Pandey, “TRANSFORMING PERFORMANCE MANAGEMENT THROUGH AI: ADVANCED FEEDBACK MECHANISMS, PREDICTIVE ANALYTICS, AND BIAS MITIGATION IN THE AGE OF WORKFORCE OPTIMIZATION, ” *Int. J. Bus. Quant. Econ. Appl. Manag. reseacrh*, vol.6, no.7, pp.1–10, 2020.

[6] J. Sabin, “The future of security in a remote - work environment, ” *Netw. Secur.*, 2021, doi: 10.1016/S1353 - 4858 (21) 00118 - 5.

[7] I. Coman and I. Mihai, “The Impact of COVID - 19 on Cybercrime and Cyberthreats, ” *CEPOL Eur. Union Agency Law Enforc. Train.*, 2021.

[8] V. V Kumar, M. Tripathi, M. K. Pandey, and M. K. Tiwari, “Physical programming and conjoint analysis - based redundancy allocation in multistate systems: A Taguchi embedded algorithm selection and control (TAS& C) approach, ” *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol.223, no.3, pp.215–232, Sep.2009, doi: 10.1243/1748006XJRR210.

[9] Delloite, “COVID - 19’s Impact on Cybersecurity, ” *Deloitte*, 2020.

[10] Sahu K, Rajshree, and Kumar R, “Risk Management Perspective in SDLC, ” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2014.

[11] P. Deo, G. Raj, and R. Perumal, “How Covid - 19 is Dramatically Changing Cybersecurity, ” *Tata Consult. Serv. Ltd.*, 2020.

[12] M. Baz, H. Alhakami, A. Agrawal, A. Baz, and R. A. Khan, “Impact of covid - 19 pandemic: A cybersecurity perspective, ” *Intell. Autom. Soft Comput.*, 2021, doi: 10.32604/IASC.2021.015845.

[13] A. Shimura, K. Yokoi, Y. Ishibashi, Y. Akatsuka, and T. Inoue, “Remote Work Decreases Psychological and Physical Stress Responses, but Full - Remote Work Increases Presenteeism, ” *Front. Psychol.*, vol.12, Sep.2021, doi: 10.3389/fpsyg.2021.730969.

[14] S. C. R. Vennapusa, T. Fadziso, K. Sachani, V. K. Yarlagadda, and S. K. R. Anumandla, “Cryptocurrency - Based Loyalty Programs for Enhanced Customer Engagement, ” *Technol. Manag. Rev.*, vol.3, no.1, pp.46–62, 2018.

[15] J. Xu, J. Lv, H. T. Yang, and Y. L. Li, “Video conferencing software selection based on hybrid MCDM and cumulative prospect theory under a major epidemic, ” *J. Intell. Fuzzy Syst.*, 2021, doi: 10.3233/JIFS - 211054.

[16] Z. Ma, D. Zhang, and J. Li, “A dedicated collaboration platform for Integrated Project Delivery, ” *Autom. Constr.*, 2018, doi: 10.1016/j. autcon.2017.10.024.

[17] H. Chung, J. Park, S. Lee, and C. Kang, “Digital forensic investigation of cloud storage services, ” *Digit. Investig.*, 2012, doi: 10.1016/j. diin.2012.05.015.

[18] R. Angelo, “SECURE PROTOCOLS AND VIRTUAL PRIVATE NETWORKS: AN EVALUATION, ” *Issues Inf. Syst.*, 2019, doi: 10.48009/3_iis_2019_37 - 46.

[19] M. D. Santos *et al.*, “A Real - Time Wearable System for Monitoring Vital Signs of COVID - 19 Patients in a Hospital Setting, ” *Front. Digit. Heal.*, 2021, doi: 10.3389/fdgth.2021.630273.

[20] R. Goyal, “The Role Of Business Analysts In Information Management Projects, ” *Int. J. Core Eng.*

Manag., vol.6, no.9, pp.76–86, 2020.
[21] A. Moallem, "Endpoint Protection, " in *Understanding Cybersecurity Technologies*, 2021. doi: 10.1201/9781003038429 - 8.
[22] A. Schrimpf, A. Drechsler, and K. Dagianis, "Assessing Identity and Access Management Process Maturity: First Insights from the German Financial Sector, " *Inf. Syst. Manag.*, 2021, doi: 10.1080/10580530.2020.1738601.
[23] S. G. Kumud Dixit, Priya Pathak, "Secure Location Selection Using Trusted Authority Or Rsu In Aodv Based Vanet, " *IJCCER*, vol.4, no.1, pp.10–14, 2016.
[24] S. G. Priya Pathak, Akansha Shrivastava, "A survey on various security issues in delay tolerant networks, " *J Adv Shell Program.*, vol.2, no.2, pp.12–18, 2015.
[25] R. Goyal, "The Role Of Requirement Gathering In Agile Software Development: Strategies For Success And Challenges, " *Int. J. Core Eng. Manag.*, vol.6, no.12, pp.142–152, 2021.
[26] R. Neware, U. Shrawankar, P. Mangulkar, and S. Khune, "Review on Multi - Factor Authentication (MFA) Sources and Operation Challenges, " *Int. J. Smart Secur. Technol.*, 2020, doi: 10.4018/ijsst.2020070104.
[27] S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation, " *Technol. \& Manag. Rev.*, vol.5, no.1, pp.45–65, 2020.
[28] S. G. Jubin Thomas, Kirti Vinod Vedi, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains, " *Int. J. Res. Anal. Rev.*, vol.8, no.3, pp.874–879, 2021.
[29] V. K. Yarlagadda, "Harnessing Biomedical Signals: A Modern Fusion of Hadoop Infrastructure, AI, and Fuzzy Logic in Healthcare, " *Malaysian J. Med. Biol. Res.*, vol.2, no.2, pp.85–92, 2021.
[30] K. Mullangi, N. D. Vamsi Krishna Yarlagadda, and M. Rodriguez, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision - Making, " *Int. J. Reciprocal Symmetry Theor. Phys.*, vol.5, no.1, pp.42–52, 2018.
[31] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi - agent framework, " in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.
[32] V. V. Kumar, A. Sahoo, and F. W. Liou, "Cyber - enabled product lifecycle management: A multi - agent framework, " in *Procedia Manufacturing*, 2019. doi: 10.1016/j. promfg.2020.01.247.
[33] K. Mohsin, "Cybersecurity in Corona Virus (COVID - 19) Age, " *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3669810.
[34] K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges, " *Int. J. Creat. Res. Thoughts*, vol.9, no.12, pp. f573–f578, 2021.
[35] R. Yadav, "Cyber Security Threats During Covid - 19 Pandemic, " *Int. Trans. J. Eng.*, vol.12, no.3, pp.1–7, 2021, doi: 10.14456/ITJEMAST.2021.59.
[36] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role - Based Access Control in SAS Programming: Enhancing Security and Authorization, " *Int. J. Reciprocal Symmetry Theor. Phys.*, vol.6, no.1, pp.31–42, 2019.
[37] R. P. Vamsi Krishna Yarlagadda, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity, " *Eng. Int.*, vol.6, no.2, pp.211–222, 2018.
[38] J. F. Broder and E. Tucker, "Mitigation and Preparedness, " in *Risk Analysis and the Security Survey*, 2012. doi: 10.1016/b978 - 0 - 12 - 382233 - 8.00013 - 3.
[39] E. Beaunoyer, S. Dupéré, and M. J. Guitton, "COVID - 19 and digital inequalities: Reciprocal impacts and mitigation strategies, " *Comput. Human Behav.*, vol.111, p.106424, Oct.2020, doi: 10.1016/j. chb.2020.106424.
[40] B. Pranggono and A. Arabo, "COVID - 19 pandemic cybersecurity issues, " *Internet Technol. Lett.*, vol.4, no.2, pp.4–9, 2021, doi: 10.1002/itl2.247.
[41] S. Chowdhury, S. Mukherjee, S. N. Roy, R. Mehdi, and R. Banerjee, "An overview of cybersecurity risks during the COVID - 19 pandemic period. " 2020.
[42] B. Bokan and J. Santos, "Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures, " in *2021 IEEE Systems and Information Engineering Design Symposium, SIEDS 2021*, 2021. doi: 10.1109/SIEDS52267.2021.9483736.
[43] H. Elkhannoubi and M. Belaissaoui, "Fundamental pillars for an effective cybersecurity strategy, " in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2016. doi: 10.1109/AICCSA.2015.7507241.
[44] T. Himdi, M. Ishaque, and J. Ahmed, "Cybersecurity challenges during pandemic in smart cities, " in *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, 2021. doi: 10.1109/INDIACom51348.2021.00079.
[45] M. Tanna, R. Sridaran, and A. Dobariya, "A study on security mitigation models in cloud computing, " in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development, INDIACom 2019*, 2019.
[46] B. D. Romero M and H. M. Haddad, "Security vulnerabilities and mitigation strategies for application development, " in *ITNG 2009 - 6th International Conference on Information Technology: New Generations*, 2009. doi: 10.1109/ITNG.2009.151.