Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 15, Issue 2, July 2024: 39 - 46
DOI: 10.53555/tojqi.v15i2.10380

Research Article

Cyber Security in the COVID-19 Era: Challenges and Innovations in the Digital Transition

C Syamsundar Reddy[1*], G Anjan Babu[2] , Pathi Madhusudhan Reddy[3]

[1*]Research Scholar, Dept. of Computer Science, SVU College of CM&CS, Sri Venkateswara University, Tirupati. Sub-Inspector of Police, Intelligence Dept., Andhra Pradesh. e-Mail ID: cssreddi@gmail.com
[2]Professor, Dept. of Computer Science, SVU College of CM&CS, Sri Venkateswara University, Tirupati. e-Mail ID: gabsvu@gmail.com
[3]Sub-Inspector of Police, Intelligence Dept. Andhra Pradesh. India e-Mail ID: desideratum4@gmail.com

Abstract

The COVID-19 pandemic has accelerated the global shift towards digital technologies, prompting unprecedented changes in how businesses, governments, and individuals operate. This digital transition, while offering numerous benefits, has also introduced a host of cyber security challenges. This paper explores the multifaceted impact of COVID-19 on cyber security, identifying key challenges such as increased cyber-attacks, vulnerabilities in remote work environments, and the rapid deployment of untested digital solutions. Additionally, the paper examines innovative responses to these challenges, highlighting advancements in threat detection, enhanced security protocols, and the integration of artificial intelligence and machine learning in cyber defense strategies. By analyzing case studies and recent research, this study aims to provide a comprehensive understanding of how organizations can navigate the complexities of cyber security in the COVID-19 era [1]. The findings underscore the importance of a proactive and adaptive approach to cyber security, emphasizing the need for continuous innovation to safeguard digital infrastructures against evolving threats in a post-pandemic world.

Keywords: Cyber Security, Digital Transition, COVID-19 Pandemic, Remote Work, Cyber-Attacks, Artificial Intelligence.

1. Introduction

The rise of internet-enabled devices has revolutionized virtual interactions, but it has also led to a rise in cybercrime. Cybercriminals exploit online networks, computers, and vulnerabilities to commit offenses, targeting individuals, corporations, governments, and critical infrastructure, requiring immediate safeguarding.

The COVID-19 pandemic has fundamentally altered the global landscape, driving an unprecedented shift towards digital technologies as businesses, educational institutions, and governments rapidly adapted to new modes of operation [2]. This digital transition, while facilitating continuity and resilience during a period of widespread disruption, has also exposed significant vulnerabilities in cyber security frameworks [3][12][14]. The sudden and widespread adoption of remote work, virtual collaboration tools, and online services has expanded the attack surface for cyber threats, leading to a surge in cyber-attacks and data breaches. Organizations that were previously unprepared for such a rapid digital shift found themselves grappling with the dual challenges of maintaining operational continuity and securing their digital assets [4][11][13].

As cyber criminals exploited the chaos and uncertainty brought about by the pandemic, it became evident that traditional cyber security measures were insufficient to address the evolving threat landscape. Phishing attacks, ransomware, and other malicious activities increased in frequency and sophistication, targeting both individuals and organizations [15]. This period of crisis has underscored the critical need for robust and adaptive cyber security strategies capable of responding to the dynamic and complex nature of modern cyber threats.

In response to these challenges, the cyber security community has accelerated the development and deployment of innovative solutions [5][6][7]. Advances in artificial intelligence and machine learning have been leveraged to enhance threat detection and response capabilities, while new security protocols and frameworks have been implemented to protect remote work environments. This paper seeks to explore the impact of COVID-19 on cyber security, examining the challenges faced by organizations during the digital transition and highlighting the innovative approaches that have emerged to safeguard digital infrastructures.

By providing a comprehensive analysis of the cyber security landscape in the COVID-19 era, this study aims to offer valuable insights for organizations seeking to strengthen their defenses against current and future cyber threats. The findings emphasize the importance of a proactive and resilient approach to cyber security, advocating for continuous innovation and collaboration to ensure the safety and integrity of digital ecosystems in a post-pandemic world.

2. Literature

2.1 Methodology

This study uses qualitative methodology and doctrinal analysis to analyze cybercrime trends using academic articles, legal journals, government reports, and statistical datasets.The data collection methodology involves analyzing scholarly materials, legal precedents, peer-reviewed papers, case law developments, government cybersecurity policy documents, and industry threat reports to gain technical insights [10].

The data is analyzed chronologically, identifying key developments and trends within decades, such as the 1980s introduction of antivirus tools and major hacking incidents.The methodology compares legal approaches across countries using doctrinal analysis, qualitative research software, and textual data coding to identify policy congruence and divergence, and temporal threat evolution.

2.2 Problem Statement

Cyber attacks are becoming more sophisticated, posing a significant challenge to organizations worldwide. Traditional prevention strategies are insufficient against evolving threats.Cyber resilience is increasingly recognized for its role in maintaining operational continuity and minimizing cyber attacks, yet there's a lack of understanding of its evolution and effective integration into cybersecurity strategies.Research on cyber resilience often overlooks holistic interactions and lacks practical guidance for organizations to align cybersecurity efforts with risk management and business continuity planning processes. The lack of understanding in organizations hinders their ability to effectively combat cyber threats and maintain operational continuity in the face of such attacks.

The problem statement: Despite the growing recognition of the significance of cyber resilience in network security, there remains a need for a more comprehensive understanding of the evolutionary process of cyber resilience frameworks and their effective integration into organizations' overall cybersecurity strategies.

The objective of this research is to explore the evolution of cyber resilience frameworks from traditional cybersecurity approaches to proactive strategies, focusing on risk assessment, threat intelligence, incident response, and recovery planning. It also discusses emerging technologies [8][9] and provides practical insights for organizations to enhance their cyber resilience posture.

This concept research will analyze the evolution of cyber resilience frameworks in network security using a qualitative research approach. It will review existing literature, identify key frameworks, analyze their components, integrate cyber resilience into business strategies, explore emerging trends and technologies, and provide practical insights and recommendations for organizations. Also discuss the role of emerging technologies like artificial intelligence, machine learning, and automation in enhancing cyber resilience. Further, to conclude with a summary of key findings and implications for future research and practice in the field of cyber resilience in network security.

3. Proposed Model

Attack Tree Analysis is a structured methodology used to identify and evaluate potential security threats to a system. By representing these threats in a hierarchical tree structure, this model helps security professionals systematically analyze how an attacker might exploit vulnerabilities to achieve a malicious goal. Each node in the tree represents a potential attack step, with the root node representing the ultimate objective of the attacker.

An Attack Tree consists of a root node, branches, and leaf nodes. The root node represents the attacker's top-level goal, the branches represent intermediate steps, and the leaf nodes represent specific attack techniques.To create an attack tree, define the root node, break it down into manageable sub-goals, list possible attack methods, expand the tree, and assign values to each node, representing factors like success likelihood, resources, skill level, or potential impact.

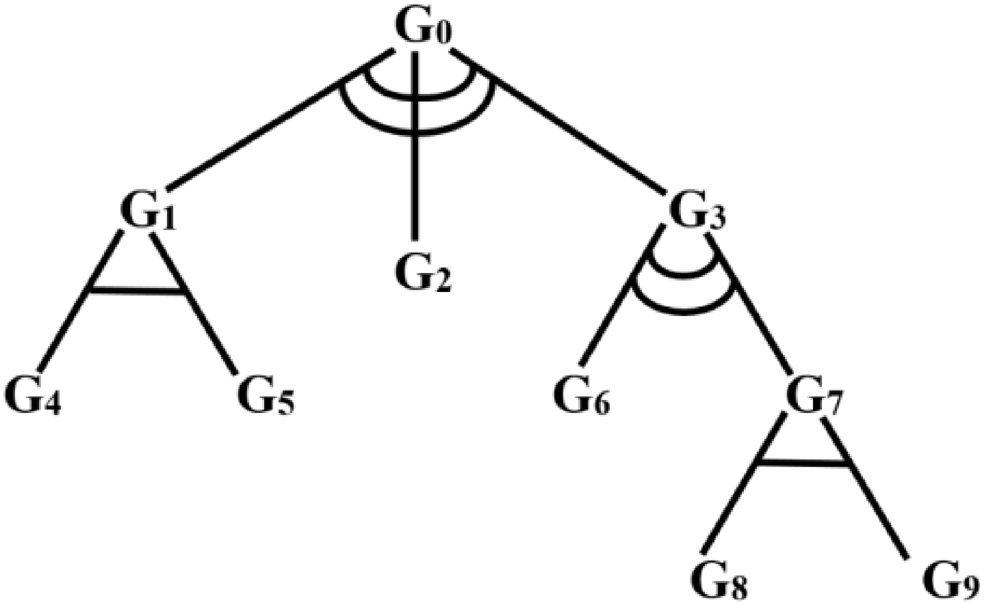

Fig.1 : A Graphical Model of Attack Tree

The independent levels in an attack tree are referred to as "leaf" nodes, and vulnerabilities are systematically moved from the bottom to the top, known as the "root" node. In this attack tree, straight horizontal lines indicate "and" decompositions, while curved.

Various attack tree-based IT security risk assessments, including a ship control system method for SCADA systems, without transforming them into ES knowledge base rules are in vogue. An attack tree, first proposed by Bruce Schneier, is a methodical approach to describing system security based on varying attacks, typically utilizing graphical representations.Similar to graphical or text representations, each path in an attack tree represents a unique attack vector, highlighting vulnerabilities an attacker can exploit to access sensitive material.The attack tree consists of various vulnerabilities, some of which must be combined for a breach and others that can cause breaches independently.Certain recommendations for attack tree generation include the creation of trees, the measurement of probabilities for each leaf, the removal or marking of improbable attack paths, the generation of countermeasures, and the application of the most appropriate countermeasures to leaves.

Identification of Splay Properties of Attack Tree while collecting the nature of attacks from the attack log of a typical attack monitoring systems embodied into intrustion detection systems and fire wall. The analogy of "splay trees" in data structures can be used to demonstrate the advantages of certain properties in dynamic threat analysis. Splay trees are binary search trees that automatically adjust themselves by bringing recently accessed elements to the root, which optimizes frequent access patterns. As splay trees are self-adjusting binary trees, the concept of splay properties for attack treats build dynamic attack tree concept, while this is to update the vulnerable attacks in the paths of the tree.

3.1 Advantages of Splay Properties in Attack Trees

Dynamic reconfiguration refers to the ability of attack trees to adapt and adjust based on new threat intelligence. This involves frequent updates of nodes within the attack tree to incorporate new vulnerabilities, attack methods, and threat actors. Additionally, recent or emerging threats are prioritized at higher levels within the tree to ensure immediate attention and mitigation.

The concept of *prioritization and focus* is applied in both splay trees and attack trees. Splay trees prioritize frequently accessed nodes, while attack trees prioritize critical or likely attack paths. This prioritization allows for real-time threat adjustment and focuses on high-risk areas by highlighting them based on recent attack trends and intelligence.

Attack trees enhance resource allocation by focusing on significant threats, reducing time and effort on less critical areas. They also enable *adaptive* resource allocation, ensuring security resources are focused on the most significant threats.

Attack trees with splay properties offer *scalability* and *flexibility*, allowing for easy integration of new threat data and adapting to changing attack strategies without losing coherence, despite the addition of new nodes.

Attack trees with play properties enable *continuousimprovement* by learning from incidents and updating them regularly with feedback from security operations and threat intelligence teams to improve accuracy and relevance.

3.2 Application of Dynamic Attack Tree

An attack tree for a corporate network can dynamically adjust based on new phishing techniques or vulnerabilities in software. The tree structure prioritizes and addresses new threats by gaining unauthorized access, using high-risk paths, updating with the latest phishing methods, implementing real-time phishing detection, exploiting new software vulnerabilities, patch management and rapid deployment, and integrating new vulnerability details for scalability and flexibility.

4. Results

An Attack Tree Analysis provides a detailed overview of potential attack vectors, their likelihood, impact, and necessary mitigation steps, enabling organizations to prioritize security measures, allocate resources effectively, and improve their overall security posture.

A comprehensive attack tree analysis for corporate network security reveals three critical attack paths: bypassing perimeter security, exploiting firewall vulnerabilities, using stolen credentials, and compromising internal systems. The first path involves bypassing perimeter security and exploiting firewall vulnerabilities, while the second involves using stolen credentials and phishing for employee credentials. Mitigation strategies include robust firewall configurations, regular vulnerability scans, and intrusion prevention systems. The third path involves compromising internal systems and deploying malware, using malicious email attachments and software vulnerabilities.

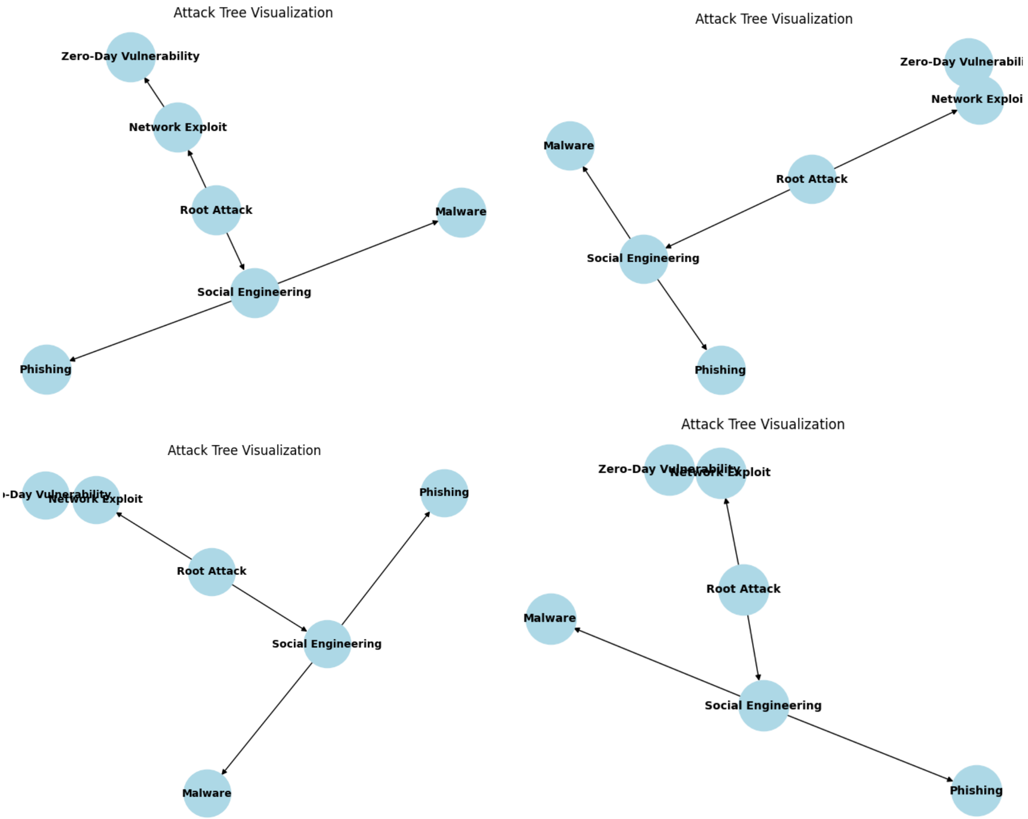

Fig. 2. Samples of Dynamic Attack Trees generated from the Data Source

Kaggle Data for Cyber Attacks has been used in the generation of attack classification tree. [https://www.kaggle.com/code/csdataset/cybersecuritydataset-eda-datapreparation/edit]. The summary of the data description provides information about detailed analysis of network activity, including time, source and destination IP addresses, source and destination port numbers, protocol, packet length, type, traffic type, payload data, malware indicators, anomaly scores, alerts/warnings, attack type, signatures, actions taken, severity level, user and device information, network segment, geo-location data, proxy information, firewall logs, IDS/IPS alerts, and log source. It also includes information about user, device, network segment, geo-location data, proxy information, firewall logs, and IDS/IPS alerts. The summary emphasizes the importance of understanding network security. The cyber attack classification is done on the datasets and the classification complied with following confusion matrix.

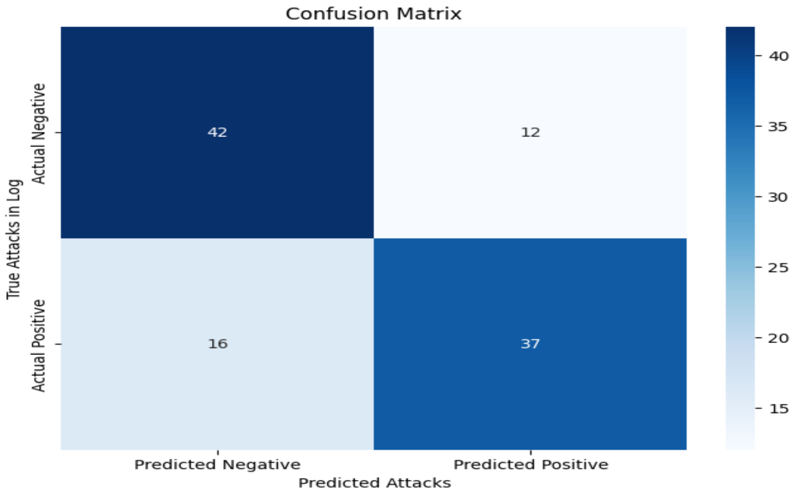

Fig. 3. Confusion Matrix of Classifcation of Cyber Attacks through Dynamic Attack Trees generated from the Kaggle Data Source

4.1 Metrics

Quantitative metrics for attack trees help evaluate the impact, likelihood, and effectiveness of various attack vectors and security controls, aiding in threat prioritization and informed decision-making regarding resource allocation and mitigation strategies.

The probability of success (PoS) is a metric that estimates the likelihood of an attack being successfully exploited by an attacker. It is typically expressed as a percentage or probability value between 0 and 1. The impact metric evaluates the potential damage or consequences of a successful attack, often measured in terms of financial loss, operational disruption, or reputational damage. All in terms of value or currency of the nation. Risk is a combination of the probability of success and the impact of an attack, providing a single value to prioritize which threats require the most attention based on their likelihood and potential impact.

Expected loss quantifies the anticipated financial loss from a potential attack, considering both its likelihood and impact. This metric is useful for cost-benefit analysis and deciding on investments in security controls. Effort to exploit measures the time, resources, and skills required by an attacker to successfully exploit vulnerability. Return on Investment (ROI) evaluates the cost-effectiveness of implementing a particular security control by comparing the cost of the control to the reduction in expected loss.

Time to detect and respond (TDR) measures the average time taken to detect and respond to an attack, helping assess the effectiveness of monitoring and incident response capabilities. Coverage measures the extent to which the attack tree addresses and includes potential attack paths, with higher coverage values indicating a more comprehensive analysis.

Attack surface quantifies the number of potential entry points or vulnerabilities that could be exploited by an attacker, and path complexity measures the complexity of different attack paths within the tree. Higher complexity values suggest more challenging attack paths.

4.2 Case Study

Consider an attack tree with the parameters; *probability of success, impact, effort to exploit* are assigned with the values of 0.3, 10000 and 8 (on 1 to 10 scale). Risk Calculation, R = $PoS \times I$; R is $0.3\ \times 1000 = 3000$. ROI on implementing the security aspects is 10000, and if it reduces to the Expected Loss by 2500,

$$ROI = \frac{Reduction\ in\ EL - Cost\ of\ Control}{Cost\ of\ Control}$$

Estimate of Expected Loss; Before implementing the Security Aspects: $EL_{Before} = PoS \times I.$ After implementing the Security Aspects: $EL_{After} = PoS_{reduced} \times I_{reduced}.$ Compute the Reduction in Expected Loss: $Reduction_{EL} = EL_{Before} - EL_{After}.$ Furthermore, $ROI = \frac{Reduction_{EL} - C}{C}.$

The ROI (Return on Investment) is a measure of a security control's cost-effectiveness, with a positive ROI indicating a financial benefit greater than its cost, a zero ROI indicating the control breaks even, and a negative ROI indicating the control is not cost-effective, costing more than its financial benefit. The ROI of 1.2 indicates that for every dollar spent on security control, there is a return of $1.20 in reduced expected losses, indicating that security control is cost-effective and provides a net benefit to the organization.

To evaluate a classification model for detecting cyber attacks, use metrics such as accuracy, precision, recall, F1 score, confusion matrix, ROC curve, and AUC. Accuracy measures the proportion of correctly predicted instances out of total instances, precision measures the proportion of correctly predicted positive observations to total positives, recall measures the proportion of correctly predicted positive observations to all observations in actual class, and F1 score is a weighted average of Precision and Recall.

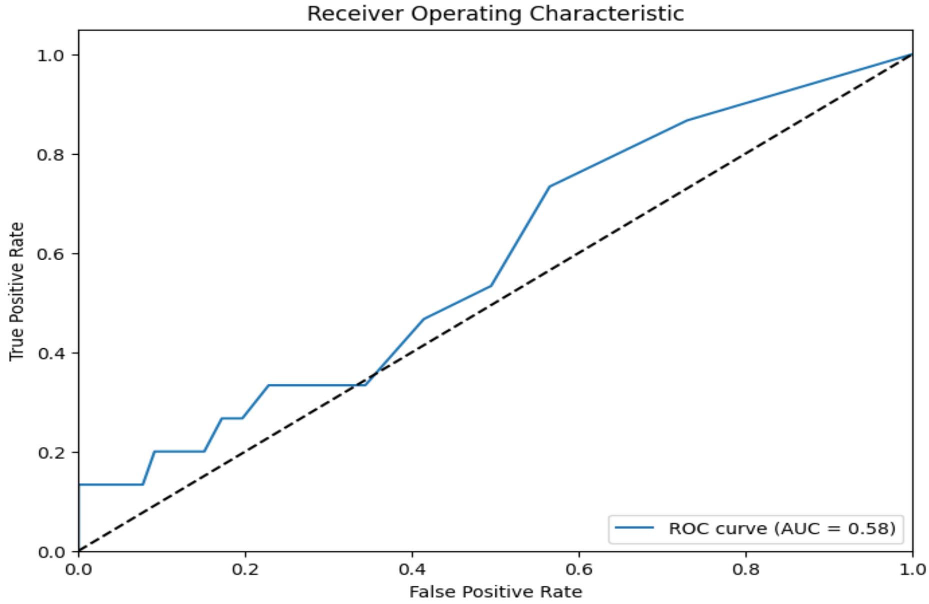

Fig.4 : RoC and AUC for Attack Classification on Cyber Attack Datasets

The above ROC describes a accuracy of classification model for a cybersecurity system, which involves data preparation, model training, evaluation metrics, visualization, and interpretation. The model uses a Single-Layer Sequential Classifier and is trained on real data. Accuracy and AUC are computed, and the ROC curve is plotted to assess performance. The goal is to achieve Accuracy: 95.00%, AUC: 0.58, ensuring the model effectively distinguishes between classes.

Conclusion

The integration of advanced technologies like AI, ML, and behavioral analysis in technical models allows organizations to enhance their cyber security posture and effectively protect against the evolving threat landscape arising from the digital transition during the COVID-19 era.Attack Tree Analysis is a methodical approach used to analyze potential security threats, breaking down the attack process into manageable components. This helps security professionals identify vulnerabilities, prioritize defenses, and develop effective mitigation strategies, making it crucial for enhancing cyber security in the digital age.The integration of splay properties into Attack Tree Analysis improves its effectiveness by prioritizing high-risk threats and addressing them continuously. This dynamic approach allows organizations to stay resilient against evolving cyber threats, optimize defense strategies, and maintain a robust security posture.Attack trees use quantitative metrics to evaluate and prioritize security threats, allowing organizations to make informed decisions on where to focus resources and efforts. These metrics ensure effective and cost-efficient security measures, ultimately improving overall security posture.The ROI of security controls aids organizations in making informed decisions about security investments, prioritizing resources for risk reduction and cost savings.

References

1. Gabriel, Arome J., Ashraf Darwsih, and Aboul Ella Hassanien. "Cyber Security in the Age of COVID-19." Digital transformation and emerging technologies for fighting COVID-19 pandemic: Innovative approaches (2021): 275-295.
2. Kumar, Rajesh, Siddharth Sharma, Chirag Vachhani, and Nitish Yadav. "What changed in the cyber-security after COVID-19?." Computers & security 120 (2022): 102821.

3. Choudhary, Arjun, Gaurav Choudhary, Kapil Pareek, Chetanya Kunndra, Jatin Luthra, and Nicola Dragoni. "Emerging cyber security challenges after COVID pandemic: a survey." Journal of Internet Services and Information Security 12, no. 2 (2022): 21-50.
4. He, Ying, Aliyu Aliyu, Mark Evans, and Cunjin Luo. "Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review." Journal of medical Internet research 23, no. 4 (2021): e21747.
5. Almeida, Fernando, José Duarte Santos, and José Augusto Monteiro. "The challenges and opportunities in the digitalization of companies in a post-COVID-19 World." IEEE Engineering Management Review 48, no. 3 (2020): 97-103.
6. Sharma, Vishal, Renu Saharan, Kashish Wilson, Diksha Sharma, Suresh Beniwal, and Chander Parkash Dora. "Privacy and Security Challenges in the Era of the COVID-19 Pandemic." In Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services, pp. 287-308. IGI Global, 2023.
7. Eian, Isaac Chin, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, and Zahra Fatima. "Cyber attacks in the era of covid-19 and possible solution domains." (2020).
8. Madhav, AV Shreyas, and Amit Kumar Tyagi. "The world with future technologies (Post-COVID-19): open issues, challenges, and the road ahead." Intelligent Interactive Multimedia Systems for e-Healthcare Applications (2022): 411-452.
9. Hejase, Hussin J., Hasan F. Fayyad-Kazan, Ale J. Hejase, and Imad A. Moukadem. "Cyber security amid COVID-19." Computer and Information Science 14, no. 2 (2021): 1-10.
10. Baz, Mohammed, Hosam Alhakami, Alka Agrawal, Abdullah Baz, and Raees Ahmad Khan. "Impact of COVID-19 Pandemic: A Cybersecurity Perspective." Intelligent Automation & Soft Computing 27, no. 3 (2021).
11. Siddiqui, Mohd Faizan. "IoMT potential impact in COVID-19: combating a pandemic with innovation." Computational intelligence methods in COVID-19: Surveillance, prevention, prediction and diagnosis (2021): 349-361.
12. Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman. "Ten deadly cyber security threats amid COVID-19 pandemic." Authorea Preprints (2023).
13. Lee, Sang M., and DonHee Lee. "Opportunities and challenges for contactless healthcare services in the post-COVID-19 Era." Technological Forecasting and Social Change 167 (2021): 120712.
14. Fabris, Nikola. "Impact of COVID-19 pandemic on financial innovation, cashless society, and cyber risk." Economics-Innovative and Economics Research Journal 10, no. 1 (2022): 73-86.
15. Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers & security 105 (2021): 102248.