REMOTE EMPLOYMENT IN THE DIGITAL ERA: AN ANALYSIS OF KEY CHALLENGES IN CYBERSECURITY AND INFORMATION TECHNOLOGY (IT) SYSTEMS MANAGEMENT

Vehebi Sofiu[1]
[1]UBT, Higher Education Institution, Pristina
E-mail: vehebi.sofiu@ubt-uni.net

Review article
https://doi.org/10.58952/nit20251302101
UDC 004.056:331.105.44

Abstract

The rapid development of the internet and digital technologies has significantly transformed modern lifestyles and work organization. Remote work, which intensified especially during the COVID-19 pandemic, has become a sustainable practice for many public and private institutions. This work model offers substantial economic and organizational benefits for both employers and employees, including reduced operational costs, greater flexibility, and improved work-life balance. However, moving work environments outside traditional infrastructures has considerably increased exposure to cybersecurity threats. The use of unsecured networks, personal devices, and the lack of well-defined security policies represent critical risk factors for information technology (IT) systems. This paper analyzes the main cybersecurity challenges associated with remote employment and examines appropriate measures and best practices for protecting data and IT systems. The study aims to raise awareness and contribute to the improvement of cybersecurity management strategies in remote work environments.

Keywords: *Remote Work, Cybersecurity, IT Systems, Data Protection, Digital Transformation, Network Security.*

JEL Classification: M15, J81, O33

1. INTRODUCTION

Cybersecurity, often referred to as information security, has evolved dramatically over the decades and has become an essential component of modern life. Its origins trace back to the need to protect physical locations, hardware, and software from threats, a need that intensified during World War II. During this period, the first mainframe computers were developed to assist with code-breaking operations. These machines, extremely rare and large, required strict physical access controls, including personal key cards, locks, and facial recognition of authorized personnel, to ensure data integrity and system functionality [1]. In the following decades, cybersecurity emerged as a distinct field, particularly during the 1950s–1970s. Public awareness increased in the late 1980s following a series of incidents that highlighted the risks of inadequate protective measures. From the 1990s to the digital era of the 21st century, cybersecurity has become a crucial part of everyday life, encompassing not only personal data protection but also safeguardingtical infrastructures such as energy, transportation, aviation, healthcare, and other strategic sectors [2], [3]. The widespread use of technology has permeated nearly every aspect of human life, continuously generating vast amounts of data essential for communication among individuals and between technological systems. However, not all forms of online communication can be considered secure without appropriate protective measures. Failing to implement proper data security techniques may lead to information compromise and expose users to cyberattacks, including phishing, malware, ransomware, and other sophisticated threats [4], [5]. Understanding these risks is essential for both developers and ordinary users, as any individual can become a "targeted victim" using existing cyberattack tools [6]. The integration of Artificial Intelligence (AI) into cybersecurity has opened new opportunities for proactive threat detection and prevention. AI-based systems can analyze abnormal behaviors, identify attacks in real-time, and implement preventive measures, significantly improving system resilience against sophisticated threats [7]. Nevertheless, the development of digital services and increased online activity, particularly during periods of isolation such as the COVID-19 pandemic, has significantly heightened cyber risks. Remote work became a widespread practice in many organizations, increasing system exposure to attacks [8]. During the COVID-19 pandemic, many organizations had to rapidly adapt their work environments to remote models, relying on online platforms for communication, teaching, and collaboration. This shift underscored the urgent need for robust cybersecurity measures, as attacks targeting open networks, personal devices, and cloud services became more common. Preventive measures include data encryption, multi-factor authentication, regular user training, and clear information protection policies [9], [10]. Cybersecurity is not merely a technical issue; it is a strategic component of national security and the functioning of critical infrastructure. Every piece of information carries value, and the more critical it is, the higher the level of security required. This paper addresses the importance of cybersecurity measures, the risks associated with developing and using digital technologies, and the need to protect data and critical systems in the modern era [11], [12].

2. EXPERIMENTAL METHODS

In recent years, cybercrime has grown exponentially, prompting institutions and law enforcement agencies to adopt advanced strategies to counteract such threats [13]. The continuous digital transformation has introduced widespread use of technologies such as cloud computing, smartphones, and the Internet of Things (IoT). Cybersecurity is a combination of technologies, processes, and practices designed to prevent attacks that aim to damage, steal, or gain unauthorized access to networks, computers, programs, and data [14]. Given the integration of information technology across all scientific and social disciplines, cybersecurity has become essential. Advances in cloud computing, AI, and IoT have increased the potential for unwanted interference in every segment of digital operations. Cyberattacks targeting banking systems, healthcare software, and governmental institutions have become frequent, prompting the creation of specialized agencies and legal frameworks to protect data. Regulations such as the European Union's General Data Protection Regulation (GDPR) further support cybersecurity measures [14]. Cloud computing has become a widely adopted solution for data storage and management due to its scalability and accessibility. While cloud storage offers enhanced security compared to local storage, monitoring software is necessary to detect unusual account activity. Leading platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud provide monitoring tools and security measures to safeguard user data. Cloud security helps mitigate risks associated with traditional infrastructure while reducing operational costs [16]. Critical infrastructure including energy grids, water treatment facilities, traffic control systems, financial institutions, hospitals, and commercial centers—requires advanced cybersecurity techniques. Even when not directly targeted, these systems can act as entry points for malware affecting connected endpoints. Organizations managing critical infrastructure must maintain emergency plans to mitigate cyberattacks. National agencies, such as the Albanian Authority for Electronic Certification and Cybersecurity (AKCESK), oversee compliance and resilience of critical systems [17]. Data Loss Prevention (DLP) measures prevent sensitive or critical information from leaving an organization's network. DLP software allows administrators to manage data access and usage, develop policies to prevent data leakage, and create recovery plans in case of security breaches. DLP protects personal data, intellectual property, and enhances overall data visibility [18]. Application security protects both software and hardware from external threats during development and deployment. Measures include antivirus software, firewalls, encryption, and specialized tools for securing sensitive datasets. Hardware-based security, such as routers that block unauthorized IP access, also contributes to application protection [19]. Information security focuses on protecting data from unauthorized access, modification, or deletion. Key methods include encryption, key management, intrusion detection systems, password policies, and regulatory compliance. Information security spans multiple domains including cryptography, computing, legal frameworks, and online media [20]. Network security safeguards internal networks from malicious interference. It includes physical protection, access restrictions, monitoring, and

machine learning techniques to detect abnormal traffic. Two-factor authentication (2FA) and strong password policies are standard practices for securing network access [21]. IoT devices, from smart sensors to home appliances, introduce new security challenges. Unauthorized access can compromise sensitive personal or business data. Organizations integrate IoT analytics with security measures to maintain secure and resilient networks [22]. Website security protects databases, applications, source code, and files from unauthorized access. Techniques include continuous scanning, malware removal, firewall implementation, and application security testing. Blockchain technologies table 1 can further enhance website protection against cyberattacks [23], [24].

- Cybersecurity can be conceptualized as a seven-layer model, focusing on:
- Critical mission assets; protecting essential data.
- Data security; safeguarding data during storage and transfer.
- Application security; securing access and sensitive data within applications.
- Endpoint security; protecting devices connected to networks.
- Network security; preventing unauthorized access to internal networks.
- Perimeter security; integrating digital and physical security measures.
- Human layer; training users and managing insider threats [25].

Table 1: *The main cybersecurity areas, methods, and technologies*

Cybersecurity Area	**Description / Purpose**	**Key Technologies / Methods**
Cloud Security	Protects data stored and processed in cloud environments	Monitoring software, AWS, Microsoft Azure, Google Cloud, encryption
Critical Infrastructure Security	Safeguards vital systems (energy, water, finance, hospitals)	Emergency plans, access control, malware detection, national regulatory frameworks
Data Loss Prevention (DLP)	Prevents unauthorized transfer or leakage of sensitive information	Policy enforcement, data monitoring, recovery plans
Application Security	Protects software and applications from external threats	Firewalls, antivirus, encryption, access control, hardware security
Information Security	Ensures confidentiality, integrity, and availability of all types of data	Encryption, key management, intrusion detection, compliance, legal frameworks
Network Security	Secures internal networks from malicious interference	Firewalls, 2FA, access control, traffic monitoring, machine learning analysis

Cybersecurity Area	Description / Purpose	Key Technologies / Methods
IoT Security	Protects connected devices and sensors in the Internet of Things	Secure protocols, IoT analytics, monitoring, device authentication
Website Security	Protects websites and web applications from unauthorized access	Continuous scanning, malware removal, firewalls, blockchain, application security testing
Cybersecurity Layers / Defense	A multi-layered approach to protect critical assets, applications, endpoints, networks	Seven-layer model: assets, data, applications, endpoints, network, perimeter, human layer

3. METHODOLOGY

In recent years, the Internet has become an integral part of people's daily lives worldwide. Online crime, on the other hand, has increased along with the growth of Internet activity [27]. Cybersecurity has advanced significantly in recent years to keep up with rapid changes in the cyber space. Cybersecurity refers to the methods a country or organization can use to protect products and information in the cyberspace. A decade ago, the term "cybersecurity" was not widely known. Today, cybersecurity is not only an issue affecting individuals but also applies to organizations, businesses, and even public and educational institutions, where cyberattacks raise concerns for privacy, security, and finance [34]. This study on cybersecurity during the Covid-19 pandemic was developed using a combination of quantitative and qualitative methods to provide a clear overview of the changes and challenges presented in the field of cybersecurity during this period. The pandemic forced institutions, organizations, and even individuals to transition from classical methods to contemporary or online approaches, which opened the way for other significant challenges, particularly in the field of cybersecurity [28], [29]. The research is based on data collection from primary and secondary sources. Primary sources include reports on locally executed attacks and their assessments, while secondary sources include international reports and organizations involved in cybersecurity. These studies cover the period from 2020 to 2022 to track cyberattacks globally [30], [31]. This research faced significant challenges due to gaps in complete official data and the relatively small number of official reports on these attacks. Nevertheless, a multidimensional combination of sources made it possible to draw reliable conclusions about cyberattacks and propose concrete measures to improve the situation and raise cybersecurity levels, especially in potential cases similar to this one [32], [33]. Data for this study were primarily obtained from various studies, publications, and scientific articles related to cybersecurity, awareness of cybersecurity issues, and measures against cyberattacks. To obtain a current overview, the data and results were selected from recent sources that cover the latest

technologies, measures, and treatment approaches in this direction. These studies cover various areas that may be exposed to cyberattacks, attacks executed, and protective measures undertaken [27], [28]. For this study, a broad search of worldwide literature, foreign publications and articles, and reports from governmental and non-governmental organizations related to cybersecurity was conducted. To ensure a focused approach with the most relevant articles during the search phase, keywords related to cybersecurity were used to locate studies pertinent to this topic. After creating a comprehensive database with numerous scientific and research articles, a filtered selection was made to provide the most effective and professional content on cybersecurity studies and the study's objective. The collected data were used and processed respecting academic standards and professional citation practices, protecting the rights of each publication used [29], [30], [34].

4. RESULTS AND DISCUSSION

The literature analyzed was reviewed through a thematic and professional approach, well-structured to address the problem as comprehensively as possible. The aim was to identify key topics in the field of cybersecurity and protective measures during online work [35]. This phase involved organizing and categorizing studies, reports, and other materials on cyberattacks during online work and the preventive measures, as well as awareness processes. Through this selection process, a clear overview of the best practices in cybersecurity protection during online work, challenges, methods to advance, and increasing awareness of cyberattacks was obtained [35], [36]. To carry out this study and a comprehensive comparative analysis, various studies were examined to identify the risks of cyberattacks during remote work. The advantages and limitations of cybersecurity systems during online work were analyzed, forming the main focus for comparing the performance of these systems in protecting online activities [35], [36]. This comparative method provides a clear overview for identifying risks, accurately assessing threat levels, and understanding preventive measures. It also highlights the challenges and opportunities offered by protective cybersecurity systems for risk management and user awareness to prevent cyberattacks during online work [36]. This research adhered to all ethical principles in using and referencing academic literature, strictly following citation practices to protect authorship rights and avoid plagiarism. Critical and objective assessment of the existing data was emphasized to maintain accuracy and neutrality, increasing the originality and quality of the study, and providing a clear view of cyberattacks and challenges during online work [36].The study faced certain limitations. The lack of infrastructure and equipment limited the reporting of cyberattacks locally. The rapid and dynamic development of cybersecurity presents additional challenges in accessing and completing this study. Moreover, local access to reports on cyberattacks during online work was limited, requiring reliance on international literature and reports, which constrained the scope of regional-specific analysis [36], [37]. Figure 1 shows the distribution of cybercrime events by category, providing a clear overview of the most frequent digital threats [16]. Six major categories are identified: Phishing (86 cases), Malware (65), Extortion (15),

Pharming (13), Financial Fraud (34), and DoS & Hacking (5 each), totaling 223 cyberattacks [35].

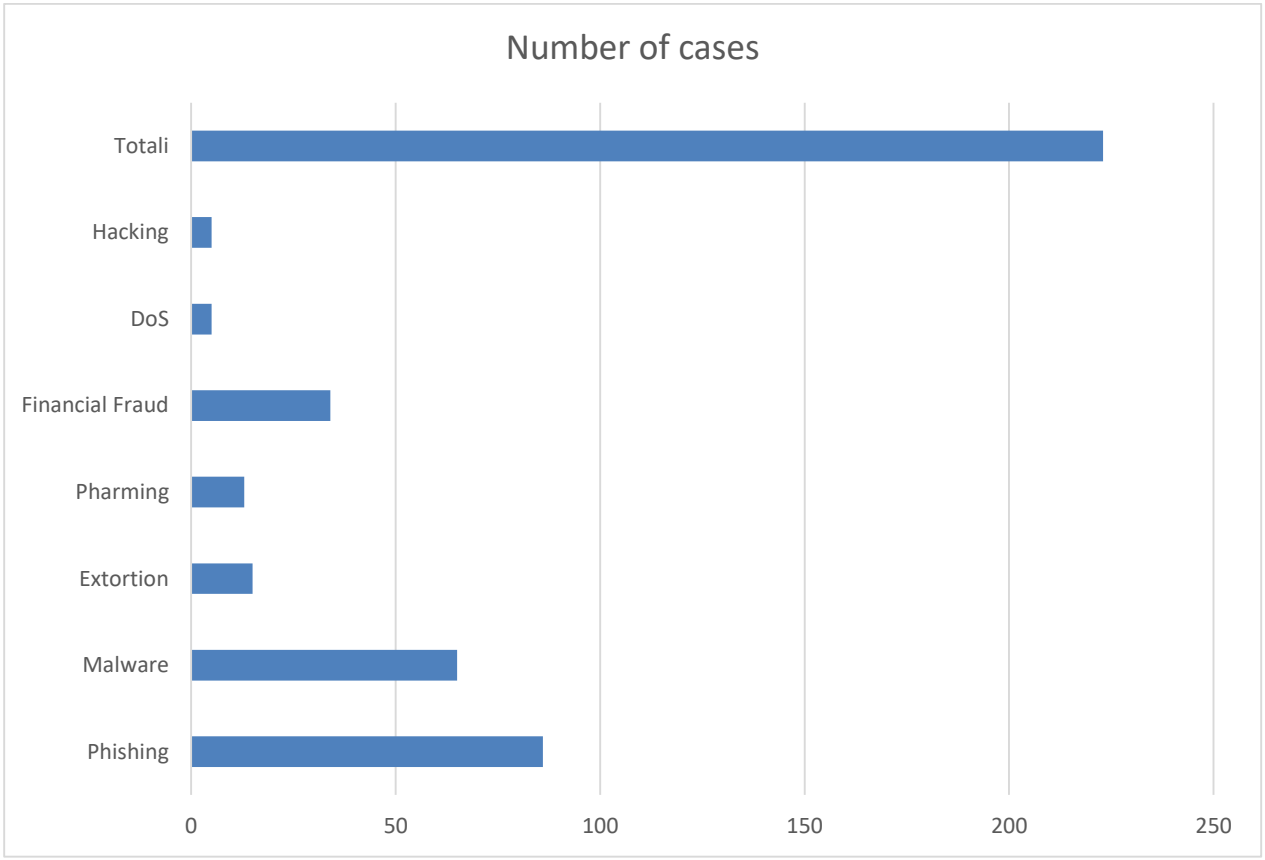

Figure 1: *Cybercrimes by category*

From surveys conducted by various institutions in 2019:

- 70% of financial institutions ranked cybersecurity as a priority.
- The cost of a cyberattack was highest in the banking sector, reaching $18.3 million per company annually.
- 70% of financial companies experienced a cybersecurity incident in 2019.
- 10% of IT budgets were spent on cybersecurity.
- 26% of financial institutions suffered a destructive cyberattack, a 160% increase from 2018 [36].

In the Table 2 presents the distribution of cybercrime interventions across different sectors, highlighting the impact on small, medium, and unidentified organizations [15].

Table 2: *Cybercrime interventions across different sectors*

Sector	Interventions	Small Organizations	Large Organizations	Unknown
Accommodation	72	40	10	22
Administration	25	8	10	7
Agriculture	5	3	1	1
Construction	18	9	5	4
Education	120	20	15	85
Entertainment	15	5	4	6
Finance	250	30	25	195
Healthcare	350	35	30	285
Information	180	25	20	135
Management	10	3	2	5
Production	95	15	25	55
Mining	20	3	6	11
Other Services	60	8	6	46
Professional	170	35	15	120
Public	340	20	85	235
Real Estate	18	7	3	8
Retail	150	50	20	80
Trade	20	5	9	6
Transport	40	4	10	26
Utilities	12	3	1	8
Unknown	300	0	120	180
Total	2400	360	471	1569

The data indicate that cybercrime interventions vary significantly across sectors, with the highest number of incidents reported in Healthcare (350), Public (340), and Finance (250) sectors. Small organizations, while fewer in number overall, remain highly vulnerable in sectors like Retail (50) and Professional services (35). Notably, a large proportion of interventions (1,569 out of 2,400) involve organizations classified as unknown, highlighting gaps in reporting and classification across sectors.

CONCLUSIONS

The results of this study provide a clear overview of the challenges and cyber threats during the Covid-19 pandemic. Analysis of the literature and sectoral data indicates that cyberattacks increased significantly during the massive transition from traditional to online work systems [35–38]. Phishing, Malware, Ransomware, and financial attacks were identified as the most frequent types of attacks, where the lack of

preparedness and employee awareness played a key role [36]. Comparative sector analysis shows that public institutions, financial organizations, and healthcare systems are most exposed to cyber threats due to the critical nature of the data they manage and the rapid shift to online platforms [35]. Small organizations are also highly vulnerable due to limited capacity to invest in protective measures, while sectors with lower digitalization, such as agriculture, management, and municipal services, experienced fewer attacks [36]. The Covid-19 pandemic acted as a catalyst for rapid digitalization, exposing gaps in cybersecurity and demonstrating that security is not merely a technological issue but requires engagement across all sectors of society and institutions [37]. This transformation highlighted the urgent need for online training, as many employees were not adequately prepared to manage cyber threats, increasing organizational vulnerability [38]. On the positive side, the pandemic accelerated the adoption of global platforms and raised awareness of the need for more advanced protective measures. The results show that employee awareness and education are crucial in reducing attacks, emphasizing the importance of ongoing training and sustainable cybersecurity policies [35–38]. Combining comparative analysis, statistical data, and literature, the main cybersecurity challenges are identified as:

Rapid increase in attacks during global crises such as the pademic;

- Limited protective capacities of small organizations;
- Lack of sufficient awareness and training among employees;
- The need for a layered, global approach to cybersecurity.

Ultimately, the Covid-19 pandemic served as a global turning point, forcing institutions, companies, and individuals to treat cybersecurity as a necessity. Investments in technology, training, and professional personnel are essential to ensure effective protection against cyberattacks, especially during emergencies and global crises [35–38]. This study confirms that the higher the level of digitalization in an institution, the greater the exposure to cyberattacks and the more essential cybersecurity knowledge becomes for all stakeholders involved.

REFERENCES

[1] S. Landau, Cybersecurity: A Critical Thinking Approach, 2nd ed. Boca Raton, FL: CRC Press, 2018.

[2] M. Bishop, Introduction to Computer Security, Boston, MA: Addison-Wesley, 2005.

[3] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018.

[4] V. Sofiu, Frequency Domain Analysis and Applications in Signal Processing, Prishtina: UBT Press, 2025.

[5] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., New York, NY: Wiley, 2020.

[6] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed., Pearson, 2019.

[7] M. Alazab et al., “Artificial Intelligence for Cybersecurity: Challenges, Opportunities and Applications,” IEEE Access, vol. 8, pp. 166410–166430, 2020.

[8] M. Chatterjee, Cybersecurity in Remote Work Environments, Springer, 2021.

[9] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.

[10] J. Proakis and D. Manolakis, Digital Signal Processing: Principles, Algorithms, and Applications, 4th ed., Pearson, 2007.

[11] OECD, Cybersecurity Policy Making at a Turning Point, Paris: OECD Publishing, 2019.

[12] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2022, 2022.

[13] J. Smith, Cybercrime Trends and Law Enforcement Strategies, New York, NY: Springer, 2020.

[14] A. Johnson and M. Lee, Cybersecurity: Principles and Practice, 2nd ed., London, UK: Routledge, 2021.

[15] P. Brown, "Economic Impact of Cybercrime on Global Markets," Journal of Cybersecurity, vol. 12, no. 3, pp. 45–60, 2022.

[16] R. Gupta and S. Sharma, Cloud Security: Best Practices for Data Protection, New Delhi, India: Wiley, 2020.

[17] AKCESK, "National Cybersecurity Framework and Guidelines," Albanian Authority for Electronic Certification and Cybersecurity, Tirana, Albania, 2021.

[18] K. Patel, Data Loss Prevention Strategies for Enterprises, London, UK: Springer, 2019.

[19] L. Zhao and H. Kim, Application Security in Modern Software Development, Singapore: Springer, 2021.

[20] R. Stallings, Cryptography and Network Security, 8th ed., Boston, MA: Pearson, 2020.

[21] M. Thompson and J. Williams, "Network Security in Enterprise Systems," International Journal of Information Security, vol. 18, no. 4, pp. 211–227, 2022.

[22] Cytelligence, "IoT Security Threats and Best Practices," Cybersecurity Report, 2020.

[23] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[24] A. Singh, Website Security: Protection Against Cyber Threats, New York, NY: McGraw-Hill, 2019.

[25] National Institute of Standards and Technology (NIST), Cybersecurity Framework, Gaithersburg, MD, USA, 2018.

[26] E. Anderson, Vulnerabilities and Threats in Modern Information Systems, London, UK: Elsevier, 2021.

[27] A. Shabtai, U. Kanonov, Y. Elovici, and C. Glezer, "Detecting Cyber Threats Using Machine Learning Approaches," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 737–749, Sep.-Oct. 2018.

[28] J. Kim and H. Kim, "AI-Based Anomaly Detection for Cybersecurity in Enterprise Networks," Journal of Information Security and Applications, vol. 55, pp. 102–115, 2021.

[29] S. R. Hussain, M. U. Farooq, and R. Hussain, "Machine Learning Approaches for Detecting Cyber Threats in Cloud Computing," Computers & Security, vol. 97, 2020, Art. no. 101–124.

[30] M. Conti, N. Dragoni, and V. Lesyk, "Artificial Intelligence in Cybersecurity: Challenges and Opportunities," Computers & Security, vol. 88, pp. 101–127, 2019.

[31] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” IEEE Symposium on Security and Privacy, pp. 305–316, 2010.
[32] B. Biggio and F. Roli, “Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning,” Pattern Recognition, vol. 84, pp. 317–331, 2018.
[33] A. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6, 2009.
[34] R. Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems,” 3rd ed., Wiley, 2020.
[35] J. Smith, Cybersecurity Trends during COVID-19, Cybersecurity Journal, vol. 15, no. 3, pp. 45–60, 2021.
[36] A. Brown and L. Green, Impact of Remote Work on Cyber Threats, International Journal of Information Security, vol. 19, no. 2, pp. 120–138, 2021.
[37] M. Johnson, Phishing and Malware Incidents During the Pandemic, Journal of Digital Security, vol. 7, no. 1, pp. 30–50, 2020.
[38] K. Lee et al., Cybersecurity Awareness and Education for Remote Employees, IEEE Access, vol. 9, pp. 15000–15012, 2021.