Overcoming Consequences of COVID-19 on Cyber Security: The Emergence of Blockchain Apps

Blockchain apps, rising amidst COVID-19 challenges, resiliently fortify cybersecurity with decentralized strength, serving as a defence and a transformative safeguard against evolving threats. The COVID-19 pandemic has triggered a profound reshaping of the global landscape, and one sector that has undergone significant transformation is cybersecurity. The swift transition to remote work and an escalating reliance on digital technologies have created a fertile ground for a surge in cyber threats. The boundaries between personal and professional digital spaces have blurred, amplifying the vulnerabilities of traditional cybersecurity measures. The escalating frequency and sophistication of cyberattacks, ranging from phishing schemes to ransomware attacks, have necessitated a paradigm shift in defence strategies.

An Investigation of Cyberbullying and Its Impact on Adolescents' Mental Health in the UK

Innovative solutions have emerged as crucial tools in fortifying cybersecurity in response to these formidable challenges. Among these, blockchain applications have become a robust defence mechanism against the evolving landscape of cyber threats. Blockchain technology's decentralized and tamper-resistant nature provides a fundamentally different approach to securing digital assets. As organizations worldwide grapple with the intricacies of safeguarding sensitive data in an era of heightened digital connectivity, blockchain applications offer a promising avenue for bolstering resilience and enhancing the overall security posture.

Introduction

In the investigations conducted by Agyepong et al. (2020) and Khan, Brohi, and Zaman (2020), it is evident that cybersecurity plays a crucial role in safeguarding confidential information within organizations. Tashea's research in 2018 underscored the protective capabilities of blockchain technology in countering cyber threats. By eliminating centralized control over network and data flow, blockchain minimizes the vulnerability to hacker infiltration. Singh and Singh (2016) further

elaborate that blockchain technology serves as an additional layer of security, fortifying organizations against potential cyber-attacks on their devices and systems.

Find Out Latest Cyber Security Dissertation Topics For 2024

Furthermore, Bordoff, Chen, and Yan (2019) and Okereafor and Adebola (2020) highlighted the impact of the global COVID-19 pandemic, which prompted widespread adoption of remote working practices. This shift created opportunities for cyber fraud, posing a threat to the cyber security of numerous firms. Ahram et al. (2017) emphasized the tamper-resistant nature of blockchain technology, distributing key data across various nodes to create a resilient record. This decentralized structure makes it challenging for hackers to compromise the integrity of the blockchain, providing robust protection against cyber threats for organizations.

Problem Statement

Ahmad (2020), Khan, Brohi, and Zaman (2020), and Wangila (2020) collectively affirm that the global COVID-19 crisis has significantly impacted organizations worldwide. These studies suggest that organizations have been compelled to embrace remote working practices while ensuring the uninterrupted regulation of critical business operations (Ahmad, 2020; Khan, Brohi, and Zaman, 2020; Wangila, 2020). However, Wirth (2020), Okereafor, and Adebola (2020) argue that the COVID-19 pandemic has presented substantial challenges for organizations regarding cyber security. According to Bordoff, Chen, and Yan (2019), Kour (2020), and Agyepong et al. (2020), the primary cyber security threats faced by organizations during this period include phishing, malicious spam, and ransomware.

Okereafor and Adebola's (2020) report reveals that hackers exploited COVID-19 to deceive organizations and the general public. They did so by encouraging the download of specific applications or software under the guise of providing updates on the global pandemic. However, upon downloading these applications, hackers gained access to sensitive information, posing a significant threat to the compromised cyber security of organizations. Consequently, the present research explores blockchain technology as an emerging solution to mitigate the cyber security threats posed to organizations during the COVID-19 pandemic.

- # Aim and Objectives

The research seeks to elucidate the efficacy of blockchain applications in mitigating the repercussions of COVID-19 on cyber security.

To scrutinize the theoretical framework outlining the impact of COVID-19 on cyber security.

To evaluate the obstacles and impediments to cyber security arising from the worldwide COVID-19 pandemic.

To pinpoint the essential components inherent in blockchain applications that can address the repercussions of COVID-19 on cyber security.

To proffer recommendations for mitigating the consequences of COVID-19 on cyber security.

Literature Review

The study by Ahram et al. (2017) highlighted the significance of blockchain technology as a prominent tool across various markets for fortifying organizations against cyber-attacks. Agyepong et al. (2020) underscored the utility of blockchain applications in preventing data theft and fraud and safeguarding organizations' reputations. Additionally, Khan, Brohi, and Zaman's (2020) research emphasized the widespread use of blockchain technology in the banking sector, particularly for securing online financial transactions that demand an additional layer of security. Kour's (2020) study asserted that the COVID-19 pandemic created opportunities for hackers to exploit organizations through phishing and spam. Nevertheless, the banking sector responded by introducing new trading platforms adhering to blockchain protocols, thereby reducing intermediaries and enhancing transaction security (Bordoff, Chen, and Yan, 2019).

Explore the National Cyber Security Policy and Strategy of Ghana

According to Agyepong et al. (2020), blockchain technology has played a crucial role in addressing the cybersecurity challenges faced by banks during the COVID-19 pandemic. However, a report from Www2.deloitte.com. (2020) argued that COVID-19 heightened security risks as organizations embraced remote working practices. The report specifically pointed out the risks associated with the misconfiguration of virtual private networks (VPN) and the occurrence of Denial of Service (DoS) attacks, exposing sensitive information online (Www2.deloitte.com. 2020). Furthermore, Bordoff, Chen, and Yan's (2019) study asserted that the pandemic has led to delays in detecting and responding to cyber-attacks within banks and corporations. This delay is attributed to the slower response time of employees compared to the IT department, providing hackers with a greater window to compromise crucial data.

A Brief Methodology

In crafting a brief methodology, the research approach involved meticulously analysing existing literature to establish a foundational understanding of the subject. The subsequent phase comprised a targeted survey, capturing diverse perspectives. Finally, qualitative interviews were conducted with industry experts to glean nuanced insights and validate the findings from the literature review.

- ## Research Approach and Method

According to Flick (2015) and Jonker and Pennink (2010), the research methodology encompasses three primary approaches: abductive, inductive, and deductive. This study adopts a deductive approach to rigorously test existing theories by formulating hypotheses and employing statistical analyses to either validate or refute these hypotheses. The focus is on examining the effectiveness of blockchain applications in mitigating the consequences of COVID-19 on the cybersecurity of banks and the corporate sector in the UK.

The research methodologies explored by Anderson, Adey, and Bevan (2010), Mackey and Gass (2015), and Kumar (2019) include mixed methods, quantitative methods, and qualitative methods. Opting for a quantitative approach aligns with the goals of the current research. This method utilizes statistical analyses, presenting factual information supported by logical reasoning to convey findings (Mackey and Gass, 2015). The quantitative approach is chosen to objectively present insights into overcoming the consequences of COVID-19 on the cybersecurity of banks and the corporate sector in the UK through blockchain technology.

- ## Data Collection Method

As outlined in Anderson, Adey, and Bevan's study (2010), data collection methods encompass two primary avenues: primary and secondary sources. In this research, a reliance on secondary data is chosen, drawing insights from existing literature to articulate key arguments regarding blockchain technology and the impact of COVID-19 on the cybersecurity landscape of banks and the corporate sector in the UK. Additionally, primary data will be gathered through a survey questionnaire, with 100 IT managers from the UK's banking and corporate sectors participating to provide firsthand perspectives.

- ## Data Analysis

The present study will employ statistical analyses, including regression, frequency, and coefficient analysis, utilizing SPSS to examine data gathered through a survey questionnaire.

Gantt Chart

A Gantt Chart is a visual project management tool that illustrates tasks, durations, and dependencies over a timeline. It provides a comprehensive overview of project progress, aiding in efficient planning and tracking of tasks.

Task	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9
Topic Research									
Proposal									
Chapter 1: Introduction									
Chapter 2: Literature Review									
Chapter 3: Research Methodology									
Chapter 4: Data analysis									

Chapter 5: Conclusion and Recommendation									

Conclusion

This research highlights cybersecurity's pivotal role, accentuating blockchain technology's protective capacity in the global COVID-19 pandemic. Focused on the UK's banking and corporate sectors, the study recognizes the transformative impact of the pandemic on organizational dynamics and the increased susceptibility to cyber threats.

The research adopts a deductive approach with quantitative methodologies, including regression and SPSS analysis, to systematically evaluate existing theories and offer objective insights. Integrating both secondary data from the literature and primary data from a survey of IT managers enhances the comprehensiveness of our findings. As organizations confront evolving challenges in cybersecurity during the pandemic, the proactive incorporation of blockchain applications emerges as a strategic solution, addressing current issues and providing recommendations for a resilient and secure cybersecurity framework in the post-pandemic landscape.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P. and Burnap, P., 2020. Cyber Security Operations Centre Concepts and Implementation. In Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 88-104). IGI Global.

Ahmad, T., 2020. Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Available at SSRN 3568830.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B., 2017, June. Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (pp. 137-141). IEEE.

Anderson, J., Adey, P. and Bevan, P., 2010. Positioning place: polylogic approaches to research methodology. Qualitative Research, 10(5), pp.589-604.

Bordoff, S., Chen, Q. and Yan, Z., 2019. Cyber attacks, contributing factors, and tackling strategies: the current status of cybersecurity science. In Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 20-37). IGI Global.

Www2.deloitte.com. 2020. [online] Available at: <https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf> [Accessed 4 June 2020].

Flick, U., 2015. Introducing research methodology: A beginner's guide to doing a research project. Sage.

Jonker, J. and Pennink, B., 2010. The essence of research methodology: A concise guide for master and PhD students in management science. Springer Science & Business Media.

Khan, N.A., Brohi, S.N. and Zaman, N., 2020. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.

Kour, R., 2020. Cybersecurity Issues and Challenges in Industry 4.0. In Applications and Challenges of Maintenance and Safety Engineering in Industry 4.0 (pp. 84-101). IGI Global.

Kumar, R., 2019. Research methodology: A step-by-step guide for beginners. Sage Publications Limited.

Mackey, A. and Gass, S.M., 2015. Second language research: Methodology and design. Routledge.

Okereafor, K. and Adebola, O., 2020. Tackling The Cybersecurity Impacts Of The Coronavirus Outbreak As A Challenge To Internet Safety. Journal Homepage: Http://Ijmr. Net. In, 8(2).

Singh, S. and Singh, N., 2016, December. Blockchain: Future of financial and cyber security. In 2016, the 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 463-467). IEEE.

Tashea, J., 2018. What do AI, blockchain and GDPR mean for cybersecurity? ABA Journal, 104, p.12.

Wangila, F., 2020. Organizational Cyber-Security Measures During COVID-19 Epidemic.

Wirth, A., 2020. Cyberinsights: COVID-19 and What It Means for Cybersecurity. Biomedical Instrumentation & Technology, 54(3), pp.216-219.