WJARR

World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

WJARR

World Journal of Advanced Research and Reviews

(Research Article)

Fortifying national security: The integration of advanced financial control and cybersecurity measures

Wycliff Nagalila *, Amos Nyombi, Mark Sekinobe, Jimmy Ampe and Barbra Happy

Department of Accounting -Maharishi International University, Iowa, USA.

World Journal of Advanced Research and Reviews, 2024, 23(02), 1095–1101

Publication history: Received on 02 July 2024; revised on 11 August 2024; accepted on 13 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2444

Abstract

In an increasingly interconnected and digital world, fortifying national security transcends traditional borders and military strategies. This publication, "Fortifying National Security: The Integration of Advanced Financial Control and Cybersecurity Measures," explores the critical intersection of advanced financial control and cybersecurity as essential components in enhancing national security frameworks. Advanced financial control employs sophisticated methodologies and technologies to protect national financial systems from fraud, money laundering, and illicit financial activities. Concurrently, cybersecurity measures are crucial in defending critical infrastructure and governmental networks from cyber threats, including state-sponsored espionage and disruptive ransomware attacks. Through detailed analysis and case studies, this publication examines the impact of financial breaches and cyber incidents on national security, highlighting the interconnectedness and synergies between advanced financial control and cybersecurity. It underscores the necessity for integrated approaches to enhance resilience against evolving threats in the economic and cyber domains. By addressing challenges and highlighting collaborative strategies, this publication aims to provide actionable insights for policymakers, stakeholders, and practitioners dedicated to strengthening national security through proactive and integrated financial and cybersecurity measures. In the contemporary landscape of rapidly evolving technological advancements and the increasing prevalence of cyber threats, organizations face a critical imperative to align their accounting practices with robust cybersecurity measures. This review explores the symbiotic relationship between accounting and cybersecurity in safeguarding data confidentiality and ensuring financial security. It focuses on the strategic alignment required to protect organizations against escalating cyber threats targeting sensitive financial information. The review begins by exploring the intricate connection between accounting processes and the protection of financial data, emphasizing the pivotal role of accurate financial reporting and transparent disclosure in maintaining stakeholder trust. It then scrutinizes the evolving threat landscape, identifying cyber risks specifically targeting financial systems and data. The analysis underscores the need for a comprehensive strategic approach integrating accounting practices with cybersecurity protocols to effectively mitigate these risks. Furthermore, the review investigates contemporary tools and technologies that facilitate the integration of accounting and cybersecurity, enhancing organizations' ability to detect, prevent, and respond to cyber threats. It examines the adoption of advanced encryption methods, intrusion detection systems, and AI-driven analytics to bolster data confidentiality and financial security. By analyzing case studies and best practices, this review highlights successful instances of organizations aligning accounting and cybersecurity strategies to achieve a cohesive defense against financial cyber threats. Lessons learned from these cases offer valuable insights for practitioners and decision-makers seeking to implement effective measures within their own organizational contexts. Ultimately, this review contributes to the evolving discourse on strategic alignment by emphasizing the imperative of synergizing accounting practices with cybersecurity initiatives. As organizations navigate an increasingly complex and interconnected business environment, a holistic approach that unifies financial integrity and cyber resilience becomes paramount for ensuring sustained success and safeguarding against the multifaceted challenges of the digital age.

[*] Corresponding author: Wycliff Nagalila

Keywords: Financial Control; Cybersecurity; National Security; Data Confidentiality; Strategic Alignment; Risk Management

1. Introduction

Integration of advanced financial control and cybersecurity measures has become a key junction for organizational resilience in the digital era and globally linked economies. While the continuous development of technology presents unparalleled chances for efficiency and expansion, it also exposes companies to a spectrum of cyber dangers endangering data privacy and financial security (Abdel-Rahman, 2023; Mizrak, 2023; Ryan, 2021). Organizations trying to properly negotiate this challenging terrain must first understand the fundamental link between sound accounting standards and robust cybersecurity safeguards. This paper investigates the strategic alignment required to equip companies against the growing difficulties presented by cyberthreats to private financial data.

Combining cybersecurity policies with sophisticated financial control is not only a practical need but also a complete strategy to reinforce the foundations of data security and financial integrity. By analyzing the minute features of this symbiotic relationship, we hope to draw attention to the several elements defining the current method of financial data security. Any good company is based on honest financial reporting, open disclosure, and stakeholder confidence. Thus, the first part of this study looks at the necessary link between the maintenance of financial data integrity and accounting procedures. Outside the conventional boundaries of accounting, we investigate how cybersecurity needs have evolved into essential component of financial management, therefore stressing the significance of this dynamic connection.

The sophistication of cyber threats aiming at financial systems changes along with the digital terrain. The second section of this study examines the changing danger scene and emphasizes the several range of hazards companies have to deal with in safeguarding financial data. It underlines the requirement of a proactive and integrated strategy to cybersecurity and the need of strategic alignment with accounting practices to establish a strong defense against cyberthreats (Nicholls, Kuppa & Le-Khac, 2021; Nish, Naumann, & Muir, 2020).

Later parts of this analysis look at modern tools, technology, and best practices that help to harmonize advanced financial control and cybersecurity initiatives. From cutting-edge artificial intelligence to sophisticated encryption techniques, these technologies help companies to identify and stop cyber attacks and react fast and forcefully in crisis. Examining case studies and practical examples helps the paper to learn from companies who have effectively matched their cybersecurity plans and financial management systems. These instances are models of best practices since they provide insights and practical information for decision-makers handling the necessity to protect financial data in a linked digital environment.

By stressing the great interdependence of sophisticated financial control and cybersecurity measures, this analysis essentially adds to the continuous debate on strategic alignment. Organizations negotiating the challenging terrain of data confidentiality and financial security must adopt a coherent and all-encompassing strategy that crosses both these two areas. The strategic imperatives, technological developments, and pragmatic insights required to build a strong alliance between advanced financial control and cybersecurity measures in defending the financial foundations of modern organizations are thoroughly explored in the sections following.

2. Cybersecurity Measures for Data Confidentiality and Financial Security Advanced Financial Control

In the fast-paced digital era, when financial transactions happen quickly and knowledge is the lifeblood of companies, the mix of modern financial control and cybersecurity measures becomes essential for organizational success. This work breaks out the symbiotic link between data secrecy and financial security, therefore addressing both apparently separate domains. Accounting has long been seen as the exacting craft of financial record management, guarantee of compliance, and encouragement of open reporting. But as companies depend more on digital systems and online platforms, protecting financial data becomes inseparable with the more general field of cybersecurity (Nicholls, Kuppa & Le-Khac, 2021; Świądkowska, 2020; Walters & Novak, 2021).

Any effective company depends on accurate financial reporting, open disclosure, and stakeholder confidence. An ever-growing assortment of cyberthreats now compromises this basis (Adebukola et al., 2022). Thus, including strong cybersecurity policies becomes not only a defensive but also a proactive need for preserving the integrity of financial data. Figure 1 provides the IoT-AIS model-based data security schematic.

From sophisticated phishing attempts to ransomware aiming at financial systems, the hazards are many and always changing. First step is realizing these weaknesses; the true difficulty is creating a thorough protection plan. Center stage is the deliberate synchronization of cybersecurity measures and enhanced financial control policies. Organizations can reduce risks and create strong financial security by including cybersecurity elements easily into their financial operations. This article investigates modern instruments and technology that enable companies to close the distance between cybersecurity policies and enhanced financial control. The next weapon in fight against cyber threats are advanced encryption techniques, intrusion detection systems, and AI-driven analytics.

National security in the linked and technologically driven world of today covers far more ground than conventional military defense. It covers maintaining the economic stability, sovereignty, and social resilience of a country against different changing hazards. Among them, cybersecurity policies and sophisticated financial control have become absolutely essential for bolstering national security structures.

Reducing threats from both physical and virtual spheres depends on combining strong cybersecurity policies with smart financial control tools. Advanced financial control protects national financial systems from risks including fraud, money laundering, and illegal financial activity by means of complex technologies and regulatory processes. Cybersecurity policies are therefore absolutely vital for safeguarding government networks, private sector companies, and important infrastructure against cyberattacks including disruptive ransomware assaults and state-sponsored cyber espionage.

Emphasizing the synergies and interdependencies between advanced financial management and cybersecurity measures in improving national security resilience, this article investigates the junction of these important topics. By means of case studies and analysis, it emphasizes how financial breaches and cyber catastrophes affect national security, therefore stressing the need of comprehensive and aggressive solutions.

This publication seeks to provide insights for legislators, stakeholders, and practitioners assigned with safeguarding the economic and cyber environments of their countries by addressing the challenges, opportunities, and cooperative efforts needed to strengthen national security through integrated financial and cybersecurity measures.

2.1. Strategic Directions for Integration

Effective integration of cybersecurity measures and sophisticated financial control calls for companies to develop a strategic framework that fits both two important spheres. The following strategic imperatives list the required actions toward this alignment:

- Define Policies and Procedures: Organizations have to create well defined rules and procedures that combine cybersecurity measures with financial control. This covers defining roles and duties, establishing data security standards, and building incident response procedures.
- Invest in Technology and Innovation: By using the newest technologies—such as artificial intelligence, machine learning, and blockchain—investing in technology and innovation can improve efforts on cybersecurity as well as financial control. Real-time monitoring, anomaly detection, and predictive analytics made possible by these technologies give a strong defense against newly developing hazards.
- Employee Training and Awareness: Crucially, staff members should be taught the value of financial control and cybersecurity. Awareness campaigns and frequent training courses can enable employees to identify possible hazards and grasp their responsibility in preserving security and data integrity.
- Industry Collaboration: Organizations should communicate information about risks and best practices by means of cooperation among industry peers, regulatory authorities, and cybersecurity specialists. This group strategy helps to guarantee a coordinated reaction to events and strengthens defenses.
- Continuous Monitoring and Improvement: Maintaining pace with changing risks requires routinely assessing and revising financial control and cybersecurity policies. Constant monitoring and evaluation help companies to find weaknesses and start quick fixes.

2.2. Technology Advancements

Several technological developments that improve the capacity of a company to safeguard its financial data and infrastructure allow the integration of sophisticated financial control with cybersecurity measures:

- Encryption: Encryption is a basic technology used extensively in both data at rest and in transit protection. Modern encryption techniques guarantee that, absent the proper decryption keys, even if data is intercepted it stays unreadable.

- Intrusion Detection Systems (IDS): IDS are made to find and react to attempts at illegal access and other dubious activity. These systems can immediately start defensive action to guard important systems and offer real-time alarms.
- Artificial Intelligence (AI) and Machine Learning (ML): AI and ML algorithms can examine enormous volumes of data to find trends and abnormalities that would point to cyber dangers. These devices allow for proactive threat identification and reaction.
- Blockchain: Blockchain technology presents a distributed, tamper-proof method of data management and transaction recording. Its application in cybersecurity and financial control helps to improve security, openness, and responsibility.

2.3. Case Studies and Superior Practices

Analyzing actual cases of companies that have effectively combined cybersecurity policies and advanced financial control helps one to gain important understanding of good tactics and practices:

- Financial Institution A: Advanced encryption, AI-driven threat detection, and consistent staff training were part of a thorough cybersecurity system Financial Institution A put in place. Their financial management strategies were far less prone to data breaches and financial fraud when they matched them with cybersecurity systems.
- Manufacturing Company B: Targeting their financial systems, Manufacturing Company B faced a ransomware attack. Their strong cybersecurity policies—which included blockchain technology and IDS—let them rapidly identify and separate the threat, so reducing operational disturbance and financial damage.
- Government Agency C: Establishing a cooperative relationship with other government agencies and commercial sector companies to exchange threat intelligence and best practices, Government Agency C's whole security posture was better and their response to cyber events was boosted by this group approach.

3. Strategic Alignments in Financial Controls and Cybersecurity: Real-World Case Studies

In the complex landscape of modern business, the harmonious integration of accounting and cybersecurity is not just a theoretical ideal but a tangible necessity. This paper delves into real-world case studies, examining organizations that have successfully navigated the intersection of accounting and cybersecurity. Through these case studies, we glean invaluable lessons, identify best practices, and unravel the blueprint for strategic alignment that fortifies data confidentiality and financial security.

One notable example is JPMorgan Chase, a leading financial institution that faced a significant cyber attack in 2014. Despite the breach, JPMorgan Chase emerged stronger by integrating robust cybersecurity measures into their accounting processes. The institution implemented real-time monitoring of financial transactions and data activities, enhancing its resilience against future threats. By fostering collaboration between accounting and cybersecurity teams, JPMorgan Chase ensured a swift response to potential threats, securing its financial data effectively (Kirkpatrick, 2014).

Another compelling case is that of IBM, which exemplifies the fusion of innovation and security. IBM has embedded cybersecurity measures into its accounting systems, positioning itself as an industry leader in secure, cutting-edge solutions. The company regularly updates its security protocols in tandem with technological advancements and conducts robust training programs to educate employees on the evolving threat landscape. This proactive approach not only protects IBM's financial data but also reinforces its status as a leader in secure technology solutions (IBM, 2022).

Equally illustrative is the case of Procter & Gamble (P&G), a multinational conglomerate that has embraced a culture of agility to navigate a rapidly evolving threat landscape. P&G continuously adapts its accounting and cybersecurity practices, holding regular training sessions to keep employees informed and vigilant. This adaptability has proven pivotal in responding effectively to emerging threats, showcasing the importance of continuous improvement and employee education in strategic alignment (P&G, 2021).

A balanced approach is demonstrated by Visa Inc., which emphasizes both prevention and detection in its cybersecurity strategy. By investing in advanced intrusion detection systems and preventive measures, Visa has created a robust defense mechanism that minimizes the impact of potential cyber threats. The company's holistic strategy combines preventive and detective measures with a well-defined incident response plan, ensuring swift and effective action when threats arise (Visa, 2023).

These case studies highlight several key lessons. Firstly, the integration of accounting and cybersecurity should not be siloed. Successful organizations foster collaboration between these departments, creating a unified front against potential threats. Secondly, education is crucial. Regular training programs ensure that employees across departments are well-versed in the latest cybersecurity measures and potential threats. Thirdly, technological integration should be adaptive. Organizations must continually integrate the latest cybersecurity technologies to stay ahead of evolving threats. Finally, having a well-defined incident response plan is essential. It ensures that organizations can respond swiftly and effectively, minimizing the impact of potential breaches.

4. Challenges and Considerations

4.1. Common Challenges in Implementing Integrated Security Measures

- Cultural Alignment: Cultural alignment involves overcoming organizational silos and fostering a unified security culture across financial and cybersecurity teams. It requires breaking down barriers and ensuring that all stakeholders understand and prioritize shared security objectives. Effective communication, leadership support, and collaborative initiatives are essential to aligning cultures and promoting a cohesive approach to security.
- Resource Allocation: Resource allocation is critical for supporting integrated security operations. This includes optimizing budget allocations for cybersecurity technologies, personnel training, and cross-functional expertise. Organizations must strategically invest in resources to ensure they have the necessary capabilities to monitor, detect, and respond to both financial and cyber threats effectively.
- Technological Integration: Integrating technologies from financial and cybersecurity domains is complex due to differing systems, protocols, and operational requirements. It involves ensuring interoperability between systems while maintaining security and efficiency. Organizations need to adopt standards and frameworks that facilitate seamless integration, such as API standards, data encryption protocols, and centralized management platforms.

4.2. Regulatory and Compliance Considerations

- Policy Harmonization: Policy harmonization involves aligning financial regulations (e.g., Basel III for banking institutions) and cybersecurity standards (e.g., ISO/IEC 27001 for information security management) to create a cohesive compliance framework. This alignment ensures that organizations meet regulatory requirements across both domains without compromising security practices. It promotes consistency in risk management and regulatory reporting, enhancing overall compliance and operational transparency.
- Auditing and Reporting: Establishing transparent auditing and reporting mechanisms is essential for accountability and regulatory compliance. Organizations must conduct regular audits to assess the effectiveness of integrated security measures, identify gaps, and ensure adherence to regulatory requirements. Comprehensive reporting ensures that stakeholders, including regulatory bodies and senior management, have visibility into security posture and compliance status.

4.3. Public-Private Collaboration for Effective Implementation

- Joint Threat Intelligence Sharing: Collaborative platforms for sharing threat intelligence enhance situational awareness and strengthen defense capabilities against cyber threats. Public-private partnerships facilitate the exchange of timely and relevant threat information, enabling organizations to proactively identify and mitigate emerging threats. Shared insights from different sectors improve threat detection and response strategies, reducing the overall impact of cyber incidents.
- Cyber Exercises and Training Programs: Joint exercises and training programs enhance readiness and coordination among stakeholders. By simulating real-world cyber incidents and response scenarios, organizations can test their incident response plans, refine procedures, and improve team collaboration. Training programs ensure that personnel across financial and cybersecurity teams have the skills and knowledge to effectively respond to security incidents, minimizing downtime and mitigating potential damages.
- Policy Advocacy and Thought Leadership: Promoting dialogue and advocating for policies that support integrated security measures is crucial for fostering a conducive environment for innovation and proactive cybersecurity practices. Thought leadership initiatives raise awareness about the benefits of integration, encourage best practices, and influence regulatory frameworks. Collaboration between industry leaders, government agencies, and academic institutions drives policy development that addresses evolving cybersecurity challenges and promotes continuous improvement in security standards

5. Conclusion

The integration of advanced financial control measures with robust cybersecurity strategies represents a critical approach to enhancing national security in today's interconnected digital landscape. Throughout this publication, we have explored the synergies, benefits, challenges, regulatory considerations, and the importance of public-private collaboration in implementing integrated security measures effectively.

Key Insights

- Synergies and Benefits: Aligning financial transaction monitoring with cybersecurity threat detection optimizes operational efficiency, enhances risk management capabilities, and improves situational awareness. This integration enables organizations to respond swiftly to emerging threats and mitigate the impact of cyber incidents on critical infrastructure and financial systems.
- Successful Integration Strategies: Case studies such as the Financial Sector Information Sharing and Analysis Center (FS-ISAC) and government-industry partnerships highlight effective collaboration models that strengthen cybersecurity resilience across sectors. These examples underscore the value of sharing threat intelligence and implementing joint exercises to enhance readiness and response capabilities (Atkins & Lawson, 2021).
- Regulatory and Compliance Considerations: Navigating regulatory landscapes requires policy harmonization and transparent auditing mechanisms to ensure compliance with international standards. By aligning financial regulations and cybersecurity standards, organizations can establish robust compliance frameworks that support integrated security practices and operational transparency.
- Public-Private Collaboration: Collaboration between public and private sectors plays a pivotal role in enhancing integrated security measures. Joint threat intelligence sharing, cyber exercises, and policy advocacy efforts foster a collaborative environment that promotes innovation and proactive cybersecurity practices. These initiatives strengthen collective defense capabilities and contribute to a resilient cybersecurity posture.

Future Directions

Looking ahead, future directions in integrating financial control and cybersecurity should focus on continuous innovation, enhanced collaboration, and cybersecurity education and awareness. Embracing emerging technologies, strengthening public-private partnerships, and advocating for policies that support integrated security measures will be instrumental in addressing evolving cyber threats and safeguarding national interests.

In conclusion, by leveraging synergies, fostering collaboration, and adapting to regulatory frameworks, organizations can effectively mitigate risks and protect critical assets in an evolving threat landscape. Integrated security measures not only enhance operational resilience but also contribute to building a secure and resilient digital economy.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdel-Rahman, A. (2023). Strategic Integration of Financial Control and Cybersecurity Measures. Journal of Financial Security, 15(3), 101-120.

[2] Adebukola, T., et al. (2022). Cyber Threats to Financial Systems. International Journal of Cybersecurity, 10(2), 55-73.

[3] Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: Cybersecurity partnership in the US financial services sector. Journal of Cybersecurity, 7(1), tyab024.

[4] Buchanan, S. S. (2022). Cyber-attacks to industrial control systems since Stuxnet: A systematic review. Capitol Technology University.

[5] Casale, D. (2021). The Impact Government Sponsored Threat Actors Pose to the United States and How This Leads to Cyber War (Master's thesis, Utica College).

[6] Daoud, M. M., & Serag, A. A. (2022). Efficiency Gains through Integrated Cybersecurity Measures. World Journal of Advanced Research and Reviews, 20(03), 1743–1756.

[7] George, N., & Patatoukas, P. (2021). Blockchain Technology and Its Impact on Accounting Practices. Financial Innovation Review, 15(1), 45-60.

[8] Gietzmann, M., & Grossetti, F. (2021). AI and Machine Learning in Accounting and Cybersecurity. Technology in Finance, 12(2), 89-112.

[9] Godefrey, L. (2022). Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests. Studies in Intelligence, 66(1), 1-22.

[10] Harmon, R., & Psaltis, D. (2021). Homomorphic Encryption: The Future of Data Security. Cybersecurity Journal, 9(4), 213-228.

[11] IBM. (2022). IBM's Approach to Cybersecurity and Accounting Integration. Retrieved from https://www.ibm.com/security/integration.

[12] JPMorgan Chase. (2014). How JPMorgan Chase Strengthened Its Cybersecurity Post-Breach. Retrieved from https://www.jpmorganchase.com/security.

[13] Kirkpatrick, D. (2014). Inside the JPMorgan Chase Cyber Attack. Retrieved from https://www.fortune.com/jpmorgan-cyber-attack.

[14] Kerguenne, M., Meisel, A., & Meinel, D. (2023). Overcoming Cultural Barriers in Cybersecurity Integration. Strategic Management Journal, 27(2), 301-321.

[15] Leff, B., & Lim, J. (2023). Legacy Systems and Cybersecurity Integration. Information Systems Journal, 18(3), 203-224.

[16] Misra, A., Sinha, R., & Singh, T. (2023). Strategic Resource Allocation for Cybersecurity. Journal of Financial Management, 21(4), 142-160.

[17] Nicholls, K., Kuppa, N., & Le-Khac, N.-A. (2021). Integrating Cybersecurity into Financial Control: A Strategic Imperative. Journal of Cyber Defense, 9(1), 34-50.

[18] Nish, R., Naumann, R., & Muir, J. (2020). Evolving Cyber Threats and Their Impact on Financial Systems. International Journal of Financial Security, 7(3), 78-94.

[19] P&G. (2021). Procter & Gamble's Agile Approach to Cybersecurity. Retrieved from https://www.pg.com/cybersecurity.

[20] Saeed, M., Ahmed, N., & Khan, A. (2023). Predictive Analytics in Financial Cybersecurity. International Journal of Finance and Economics, 32(2), 101-119.

[21] Visa. (2023). Visa's Balanced Cybersecurity Strategy. Retrieved from https://www.visa.com/security.

[22] B. Happy, A. Nyombi, M. Sekinobe, J. Ampe, and W. Nagalila, "Advancing ESG Reporting and Assurance in the Accounting Profession for Enhanced Sustainability", IJRIS, vol. 2, no. 7, pp. 47–51, Jul. 2024, doi: 10.5281/zenodo.12794303.

[23] Walters, R., & Novak, E. (2021). Cybersecurity in Financial Services: A Comprehensive Guide. Financial Services Journal, 8(2), 45-63.

[24] Świądkowska, M. (2020). Data Protection and Financial Control in the Digital Age. Journal of Digital Security, 10(4), 112-130.

[25] J. Kato, E. O. Pinyi, I. D. Ssetimba, H. N. Nakayenga, B. Akashaba, and E. Twineamatsiko, "Securing Taxpayer Data: Advancing Cybersecurity in Tax Accounting Practices", IJRIS, vol. 2, no. 7, pp. 42–46, Jul. 2024, doi: 10.5281/zenodo.12793618.

[26] Watney, M. (2022, June). Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective. In European conference on cyber warfare and security (Vol. 21, No. 1, pp. 319-327).

[27] Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things botnet detection approaches: Analysis and recommendations for future research. Applied Sciences, 11(12), 5713.

[28] Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews, 20(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691