Int. j. adv. multidisc. res. stud. 2025; 5(6):2284-2298

Received: 07-11-2025
Accepted: 17-12-2025

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

A Review of Ransomware Economics and Financial Resilience Strategies in Hospital Networks

[1] David Excel Ozowara, [2] Chukwudera Obumneke Anunagba, [3] Peter Adeyemo Adepoju
[1] Western Illinois University, Macomb, Illinois, USA
[2] Barclays Whippany, New Jersey, USA
[3] Independent Researcher, UK

Corresponding Author: **David Excel Ozowara**

Abstract
Ransomware attacks have emerged as a significant threat to hospital networks, leading to substantial financial losses, operational disruption, and degradation of patient care. The economic impact of ransomware on healthcare organizations has become a critical concern, as the frequency, sophistication, and cost of these cyberattacks continue to rise. This review paper explores the intersection of ransomware economics and financial resilience strategies within hospital networks. It begins by analyzing the direct and indirect economic consequences of ransomware incidents, including ransom payments, recovery costs, reputational damage, and regulatory penalties. The paper also examines the long-term financial impact of downtime, data breaches, and the potential loss of trust among stakeholders. Furthermore, it reviews financial resilience frameworks that hospitals can adopt to mitigate the impact of ransomware attacks. These strategies include cybersecurity investments, risk management practices, incident response plans, and insurance policies. Special attention is given to the role of public-private partnerships, government regulations, and the implementation of digital safeguards like data encryption and backup systems. The paper also highlights case studies of hospitals that have successfully navigated ransomware attacks, providing insights into effective financial recovery strategies. Lastly, the review discusses the challenges that hospitals face in building financial resilience, such as resource constraints, regulatory complexities, and the evolving nature of cyber threats. It concludes with recommendations for hospital networks to enhance their financial resilience against ransomware, emphasizing proactive cybersecurity investments, collaboration across the healthcare sector, and the integration of resilience strategies into broader organizational risk management frameworks.

Keywords: Ransomware Economics, Financial Resilience, Hospital Networks, Cybersecurity Strategies, Healthcare Risk Management, Incident Response

1. Introduction

1.1 Overview of Ransomware Threats to Healthcare

Ransomware threats have become a pervasive issue in the healthcare industry, impacting hospitals and healthcare providers globally. Cybercriminals have increasingly targeted hospitals, leveraging sophisticated ransomware variants to hold critical systems and patient data hostage in exchange for substantial ransom payments. These attacks disrupt healthcare delivery, compromise sensitive data, and lead to significant financial losses. The healthcare sector is particularly vulnerable due to the sensitive nature of the information involved, including personal health records (PHR) and clinical data. Additionally, healthcare networks are often interconnected with other organizations, such as insurance providers, pharmaceutical companies, and laboratories, creating potential entry points for attackers. Recent trends indicate that ransomware attacks are not just about encrypting files but also include data exfiltration, where cybercriminals steal sensitive patient data before encrypting it, posing further risks to healthcare providers (Oduro, 2025).

Furthermore, the financial and operational impact of ransomware on hospitals is staggering. The immediate effects are the direct costs associated with ransom payments and system downtime, but the long-term consequences, such as reputational damage and loss of patient trust, exacerbate the financial burden (Ogbete *et al*., 2025). Ransomware attacks often target essential healthcare systems, such as Electronic Health Records (EHR) and medical devices, which directly affect patient care.

The ability to restore critical services following an attack is heavily dependent on hospitals' preparedness for such events, including their data backup systems, incident response protocols, and the availability of cybersecurity experts to manage the attack (Bello *et al*., 2025). The evolving sophistication of these attacks requires healthcare organizations to stay ahead of cybercriminals by continually adapting their security strategies and investing in robust defense mechanisms.

1.2 Significance of Financial Resilience in Hospitals

Financial resilience in hospitals is critical in ensuring the continuity of operations during and after a ransomware attack. A financially resilient hospital can absorb the financial shocks resulting from cybersecurity breaches, including the costs of ransom payments, recovery, and legal consequences. Financial resilience goes beyond just the ability to recover from direct financial losses; it involves having the necessary resources and strategies to quickly restore essential healthcare services, maintain operational continuity, and protect the organization's reputation. Hospitals that prioritize financial resilience are better prepared to handle not only ransomware attacks but also other financial and operational disruptions. For instance, hospitals with solid financial planning and insurance strategies are able to mitigate the potential impacts of a ransomware attack and recover faster than those without these mechanisms in place (Ijiga *et al*., 2025).

Additionally, hospitals must ensure that their financial resilience strategies are integrated with their cybersecurity frameworks. A hospital's financial health is directly tied to the security of its data, systems, and networks. Cybersecurity investment, including advanced threat detection, employee training, and data backup systems, contributes to the hospital's ability to prevent, detect, and respond to ransomware threats (Oziri *et al*., 2025). By embedding financial resilience into the hospital's operational and strategic planning, hospitals can ensure that their resources are used efficiently to withstand the financial strain of cyberattacks. This includes developing comprehensive risk management practices, such as cyber insurance policies and disaster recovery plans, which further enhance the hospital's ability to respond to and recover from ransomware attacks (Badmus, 2025).

1.3 Purpose and Scope of the Review

The purpose of this review paper is to explore the financial implications of ransomware attacks on hospital networks, with a focus on the economic impact, financial resilience strategies, and long-term consequences. It aims to provide a comprehensive understanding of the direct and indirect costs associated with ransomware incidents and the challenges healthcare organizations face in maintaining financial resilience against such threats. The review will also highlight effective strategies for mitigating financial losses and improving hospitals' preparedness for ransomware attacks. By examining the current landscape of ransomware threats in the healthcare sector, this review will contribute valuable insights for healthcare administrators, cybersecurity professionals, and policymakers seeking to bolster the financial resilience of hospitals in the face of evolving cyber threats.

The scope of this review includes an analysis of the economic consequences of ransomware attacks, including direct financial costs such as ransom payments, recovery expenses, and downtime. It also addresses the indirect costs, such as reputation damage and regulatory fines, which have long-term financial implications. Furthermore, the review will explore various financial resilience strategies that hospitals can adopt, including cybersecurity policies, risk management frameworks, and collaborative approaches to threat detection and response. The review will incorporate case studies of hospitals that have faced ransomware attacks, providing real-world examples of how organizations have navigated the financial challenges posed by these incidents.

1.4 Structure of the Paper

This paper is organized into several sections to provide a clear and systematic exploration of ransomware economics and financial resilience in hospital networks. Following this introduction, Section 2 provides an overview of the direct and indirect financial costs of ransomware attacks, including ransom payments, recovery efforts, and the operational disruptions that hospitals face. Section 3 examines the significance of financial resilience in hospitals, highlighting strategies for improving financial preparedness and the integration of cybersecurity measures with financial planning. Section 4 explores real-world case studies of hospitals that have experienced ransomware attacks and outlines lessons learned from their recovery efforts. Section 5 discusses recommendations for enhancing financial resilience, including policy frameworks, risk management strategies, and collaboration with external partners. The paper concludes in Section 6, summarizing the key findings and proposing future research directions for improving ransomware preparedness in hospital networks.

2. Economic Impact of Ransomware on Hospitals

2.1 Direct Financial Costs (Ransom Payments, Recovery, Downtime)

The direct financial costs associated with ransomware attacks in hospital networks are substantial and multifaceted. One of the most immediate and visible expenses is the payment of the ransom. Hospitals often find themselves in difficult situations where paying the ransom is seen as the quickest route to restoring access to critical systems and data. For instance, the cost of ransom payments can vary significantly, with recent attacks showing demands ranging from thousands to millions of dollars (Bello *et al*., 2025). The decision to pay is complicated by the lack of guarantees that attackers will honor their word and provide the decryption keys, which may exacerbate the financial strain (Okoruwa *et al*., 2025).

Additionally, the cost of recovery is a key aspect of the financial burden faced by hospitals post-attack. Recovery efforts encompass a wide range of activities, including the restoration of IT systems, replacement of compromised hardware, and restoration of data from backups (Lawal & Oduleye, 2025). The expenses incurred in these activities can escalate rapidly, particularly when hospitals lack adequate preparation for cyber events. Furthermore, prolonged downtime resulting from ransomware attacks can result in a significant loss of revenue, as hospitals must divert resources and staff attention away from regular patient care to focus on resolving the incident (Ogbete *et al*., 2025). These disruptions also affect patient care, with delays in medical procedures and treatments contributing to a broader financial impact, not only through lost income but

also through reputational damage (Oparah *et al*., 2025). The cumulative financial cost of ransomware attacks thus involves a combination of direct ransom payments, recovery expenses, and lost revenue due to operational downtime (Oduro, 2025).

2.2 Indirect Costs (Reputation Damage, Regulatory Fines)

The indirect costs of ransomware attacks on hospital networks go beyond the immediate financial losses, often leaving long-lasting damage to the organization's reputation and regulatory standing. Reputation damage is one of the most significant indirect costs. Following a ransomware attack, hospitals may face public backlash, especially if patient data is compromised or services are disrupted for extended periods (Badmus, 2025). This negative publicity can significantly erode public trust, which is essential in healthcare. Once trust is lost, hospitals may find it difficult to regain their status in the community, resulting in a decline in patient volume and, consequently, reduced revenue (Adeoye *et al*., 2025). Furthermore, the reputational impact often extends to business relationships, as partners and suppliers may be reluctant to continue working with an organization perceived as vulnerable to cyber threats (Sanni & Iwuanyanwu, 2024).

In addition to reputation damage, hospitals may also face regulatory fines due to non-compliance with data protection laws such as HIPAA in the United States or GDPR in Europe. The loss of sensitive patient information during a ransomware attack often triggers regulatory investigations and can result in hefty fines (Akin-Oluyomi *et al*., 2025). These fines can be significant, particularly when hospitals fail to meet the security and privacy requirements mandated by healthcare regulations (Oduro, 2024). Moreover, the legal repercussions of failing to protect patient data are far-reaching, potentially resulting in lawsuits from affected individuals (Michael & Ogunsola, 2025) as seen in Table 1. In addition to the immediate financial burden, these fines can lead to long-term impacts, including the loss of business opportunities and the cost of future compliance measures (Bello *et al*., 2024).

Table 1: Summary of Indirect Costs of Ransomware Attacks on Hospital Networks

Indirect Cost Category	Description	Impact on Hospital Operations	Long-Term Effects
Reputation Damage	Following a ransomware attack, hospitals face public backlash, particularly if patient data is compromised or services are disrupted. This leads to a loss of public trust.	Hospitals may experience a decline in patient volume and reduced revenue due to diminished public confidence.	Rebuilding trust is difficult, and hospitals may lose community status, affecting long-term patient loyalty.
Loss of Business Relationships	Negative publicity surrounding a ransomware attack extends to relationships with partners and suppliers, who may hesitate to collaborate with an organization perceived as vulnerable.	Hospitals may face challenges in maintaining or securing partnerships, leading to disruptions in the supply chain and collaboration.	Loss of business relationships can hinder future growth and strategic partnerships.
Regulatory Fines	Data protection laws, such as HIPAA and GDPR, impose strict penalties for data breaches caused by ransomware attacks, leading to regulatory investigations and fines.	Non-compliance with security and privacy laws can result in significant fines and the need for enhanced security measures.	Regulatory fines may be long-lasting, impacting the hospital's ability to operate effectively and increasing future compliance costs.
Legal Repercussions	Ransomware attacks can lead to lawsuits from affected patients whose sensitive data was compromised, further complicating legal standing.	The hospital faces legal expenses and potential compensation payouts, diverting funds from core operations.	Long-term legal battles can lead to sustained financial strain and a tarnished reputation in legal and healthcare communities.

2.3 Long-Term Economic Consequences (Loss of Trust, Operational Disruption)

The long-term economic consequences of ransomware attacks on hospital networks extend far beyond the immediate financial costs, often leading to a prolonged loss of trust and significant operational disruptions. One of the most critical long-term consequences is the erosion of patient trust. As ransomware attacks often involve the breach or compromise of sensitive patient data, the public perception of an organization's ability to safeguard its information is severely damaged (Bello *et al*., 2025). Patients expect hospitals to maintain the highest levels of confidentiality and security, and any failure to do so can result in a long-lasting decline in patient loyalty (Ogbete *et al*., 2025). Hospitals may find themselves losing not only existing patients but also future ones, as individuals may choose competitors with stronger cybersecurity reputations (Ijiga *et al*., 2025).

In addition to the loss of trust, ransomware attacks lead to operational disruptions that affect the day-to-day functioning of hospitals. These disruptions can extend well beyond the initial attack, as hospitals must engage in lengthy recovery processes to restore systems, verify data integrity, and ensure compliance with regulatory standards (Michael & Ogunsola, 2025). The costs of these disruptions are exacerbated when hospitals lack an effective business continuity plan or face challenges with restoring critical operations quickly. This delay in recovery can also impact the quality of care delivered, as medical staff may not have immediate access to necessary patient information or resources (Oduro, 2025). Furthermore, as hospitals work to address the aftermath of the attack, they may face extended downtimes, which contribute to lost revenue streams and incur additional operational costs (Oziri *et al*., 2025). Thus, ransomware attacks represent a multi-dimensional threat, impacting hospital networks' financial health both in the short term and for years after the incident (Ijiga *et al*., 2025).

3. Financial Resilience Frameworks for Hospital Networks

3.1 Cybersecurity Investments (Software, Hardware, Training)

Cybersecurity investments in hospital networks are crucial to mitigating ransomware threats that pose significant financial and operational risks to healthcare providers. As hospitals rely increasingly on digital systems for patient data management and medical operations, the need for robust cybersecurity infrastructures has become paramount. Investment in cutting-edge cybersecurity software is the first line of defense, providing critical protection against unauthorized access and malicious cyber activities (Adeniyi, Odejobi, & Taiwo, 2025). Modern cybersecurity software, such as endpoint detection and response (EDR) and intrusion detection systems (IDS), offer real-time threat monitoring and proactive response capabilities, which are vital in preventing data breaches and ransomware attacks (Okoruwa *et al*., 2025). Additionally, hospitals must prioritize the acquisition of hardware solutions designed to safeguard sensitive data. Firewalls, secure servers, and encrypted storage devices are essential for creating secure environments where patient records can be protected from unauthorized access, especially in the event of a ransomware attack (Bello *et al*., 2025).

Training hospital staff is another key component in strengthening cybersecurity defenses. Human error is often the weakest link in a hospital's security chain, with phishing and social engineering attacks frequently targeting personnel (Ogbole *et al*., 2025). Continuous cybersecurity training for healthcare staff, including medical personnel and administrative workers, is critical for maintaining a culture of security awareness and ensuring adherence to best practices (Akin-Oluyomi *et al*., 2025). Programs that focus on identifying phishing attempts, password security, and the importance of regular software updates can significantly reduce the likelihood of a successful ransomware attack (Joseph, Ijiga, Olateji, Okoli, & Frempong, 2025). Furthermore, simulated ransomware attacks and training exercises have proven effective in preparing hospital staff for real-world cyber threats (Okonkwo, Ijiga, Awoyemi, & Atobatele, 2025). By integrating these cybersecurity software, hardware, and training investments, hospitals can fortify their defenses against ransomware, reduce the financial and operational impact of cyberattacks, and ensure business continuity (Badmus, 2025).

3.2 Risk Management Practices and Assessment Tools

Risk management is an essential component of mitigating ransomware threats in hospital networks, as these institutions are increasingly targeted by cybercriminals. Risk management practices help identify, assess, and mitigate the financial and operational risks associated with cybersecurity incidents, including ransomware attacks. A key tool in hospital risk management is the implementation of risk assessment models that evaluate the probability and potential impact of various cybersecurity threats (Bello *et al*., 2025). These models incorporate both qualitative and quantitative factors, such as the likelihood of an attack, the potential consequences on patient data, and the cost of operational downtime (Ogbole *et al*., 2025). Hospitals often employ frameworks like ISO 27001 to standardize their risk management approaches, ensuring they meet international standards for cybersecurity and data protection (Akin-Oluyomi *et al*., 2025). The identification of critical assets, such as patient records and medical equipment, is crucial in prioritizing risk mitigation efforts (Joseph, Ijiga, Olateji, Okoli, & Frempong, 2025).

Additionally, hospitals must employ advanced tools for continuous risk monitoring and assessment. These tools can include security information and event management (SIEM) systems, which provide real-time alerts for unusual activities or breaches within the network (Badmus, 2025). Through ongoing monitoring, healthcare providers can proactively identify vulnerabilities and adjust their security posture before a ransomware attack occurs (Ijiga *et al*., 2023). Regular penetration testing and vulnerability assessments, conducted both internally and with external cybersecurity firms, help simulate real-world attacks and identify potential weaknesses in hospital networks (Lawal & Oduleye, 2025). Effective risk management also includes employee training programs that emphasize recognizing phishing attempts and avoiding risky online behavior, which are often the entry points for ransomware (Okonkwo *et al*., 2025). By integrating these practices and tools into their cybersecurity strategy, hospitals can enhance their preparedness and minimize the financial and operational impacts of ransomware attacks.

3.3 Incident Response and Recovery Plans

Incident response and recovery plans are critical components of a hospital's cybersecurity strategy, ensuring quick recovery in the event of a ransomware attack. These plans define the procedures and responsibilities for responding to an attack, minimizing damage, and restoring normal operations as quickly as possible. A key element of an effective incident response plan is the establishment of an incident response team (IRT), which should include cybersecurity professionals, IT staff, legal advisors, and public relations personnel (Okonkwo, Ijiga, Awoyemi, & Atobatele, 2025). The team is responsible for identifying the nature of the attack, containing its spread, and ensuring the safety of sensitive patient data. Ransomware attacks often encrypt critical files, so a rapid response is essential to prevent the spread of the infection and reduce data loss (Ogbole *et al*., 2025).

Recovery plans go hand-in-hand with incident response and are designed to restore normal hospital functions after a cyberattack. One key component of a recovery plan is the use of secure and up-to-date backups, which allow hospitals to restore encrypted files without paying the ransom (Joseph *et al*., 2025). These backups should be stored offline or in isolated cloud environments to prevent them from being compromised during an attack (Bello *et al*., 2025). In addition to technical recovery, hospitals must also address the reputational and regulatory impacts of ransomware attacks. Clear communication strategies with patients, healthcare providers, and regulatory authorities can help mitigate the damage to trust and ensure compliance with data protection regulations (Oduro, 2025). Regular simulations of ransomware attacks, known as tabletop exercises, allow hospitals to test their incident response and recovery plans, identify gaps, and refine their strategies to enhance preparedness (Oparah *et al*., 2025).

4. Role of Public-Private Partnerships in Financial Resilience

4.1 Government Regulations and Support Mechanisms

The government plays a crucial role in establishing regulatory frameworks that guide how healthcare organizations respond to ransomware threats. Governments can support hospitals through mandates that enforce the implementation of cybersecurity measures and operational resilience protocols. This includes the development and enforcement of regulations that require hospitals to adopt specific encryption and backup protocols, ensuring data protection in case of an attack (Bello, Elebe, Hammed, Okoruwa, Fadayomi, & Omoegun, 2025). Governments also play a role in coordinating financial support, such as providing incentives or grants for hospitals to upgrade cybersecurity infrastructure (Sanni & Adumaza, 2023). Regulatory bodies like the National Health Service (NHS) in the United Kingdom and the U.S. Department of Health and Human Services have increasingly focused on ensuring that healthcare organizations meet minimum security standards to prevent ransomware attacks and minimize their economic consequences (Yusuff *et al*., 2025).

In addition to regulations, governments often create support mechanisms to assist organizations in recovering from ransomware incidents. These mechanisms can include subsidies for incident response or post-attack recovery, such as the U.S. Cybersecurity & Infrastructure Security Agency's (CISA) support for hospitals during cyber emergencies (Sanni, Iwuanyanwu, Essien, & Wedraogo, 2024). Public-private partnerships also provide a collaborative space for sharing threat intelligence, enabling hospitals to stay ahead of emerging ransomware tactics (Badmus & Olamide, 2021). Furthermore, regulatory technology frameworks that facilitate real-time reporting and compliance are essential in mitigating the risk of ransomware attacks and improving transparency in the healthcare sector (Bello *et al*., 2025). Governments are also instrumental in providing guidance on ransomware insurance policies and encouraging hospitals to adopt these financial safeguards, ensuring that they are financially prepared for recovery post-attack (Oziri, Arowogbadamu, & Seyi-Lande, 2024).

4.2 Collaboration Between Healthcare Providers and Cybersecurity Firms

The collaboration between healthcare providers and cybersecurity firms is crucial for ensuring effective defense against ransomware attacks. Healthcare providers face unique challenges in cybersecurity, including outdated infrastructure, budget constraints, and the need for rapid incident recovery (Anichukwueze, Osuji, & Oguntegbe, 2024). In response, many healthcare organizations are turning to specialized cybersecurity firms for assistance in assessing vulnerabilities, developing secure systems, and responding swiftly to ransomware incidents. Cybersecurity firms, with their expertise in threat detection and mitigation, can offer solutions that are tailored to the specific needs of hospitals, such as malware prevention, intrusion detection systems, and real-time threat monitoring (Oziri, Arowogbadamu, & Seyi-Lande, 2024).

Such collaborations are critical because ransomware threats continue to evolve, requiring adaptive cybersecurity measures. One significant advantage of these partnerships is the ability to leverage the cybersecurity firm's continuous monitoring and incident response capabilities. This ensures that hospitals can respond quickly to emerging threats and implement rapid recovery strategies (Oparah *et al*., 2025). Moreover, cybersecurity firms often assist in the development of best practices for risk management, provide employee training on security awareness, and help in the design of disaster recovery plans. Successful collaborations have been seen in hospitals where cybersecurity experts perform penetration testing and vulnerability assessments, strengthening the institution's ability to prevent and recover from ransomware attacks (Adeyoyin, Awanye, Morah, & Ekpedo, 2024) as seen in Table 2. Additionally, the sharing of intelligence between cybersecurity firms and healthcare organizations allows for the detection of trends, emerging threats, and zero-day vulnerabilities, thus fortifying the resilience of hospital networks.

Table 2: Collaboration Between Healthcare Providers and Cybersecurity Firms

Aspect	Healthcare Providers' Challenges	Role of Cybersecurity Firms	Benefits of Collaboration
Cybersecurity Infrastructure	Outdated systems and infrastructure, limited budgets	Provide expertise in developing secure systems and modernizing infrastructure	Improved security posture with tailored solutions and up-to-date defenses
Incident Response and Recovery	Slow recovery and lack of resources for rapid response	Offer incident response services, including malware prevention, intrusion detection, and real-time monitoring	Swift response to ransomware attacks and faster recovery times
Training and Awareness	Lack of employee training on security awareness	Provide training programs for hospital staff on recognizing threats and best security practices	Enhanced staff readiness and reduced risk of human error leading to breaches
Vulnerability Assessments	Limited resources for conducting comprehensive vulnerability assessments	Conduct penetration testing and vulnerability assessments	Identification of weaknesses, enabling proactive measures to strengthen security

4.3 Funding and Insurance Options for Ransomware-Related Losses

Ransomware-related losses can have devastating financial implications for hospitals, which is why many institutions are turning to insurance and funding options as part of their financial resilience strategy. Cybersecurity insurance is one of the key tools available to hospitals to cover the financial impact of ransomware attacks, including costs related to ransom payments, legal expenses, and recovery efforts (Yusuff *et al*., 2025). Insurance policies can also help mitigate the costs associated with reputation damage and regulatory fines, which are often incurred following a data breach (Badmus & Olamide, 2024). Some hospitals have opted for comprehensive cybersecurity insurance policies that specifically cover ransomware attacks, ensuring they

have the financial backing needed to recover quickly without depleting their operational funds (Ogbete *et al*., 2025).

In addition to traditional insurance, government and non-governmental organizations offer grants and funding opportunities to help hospitals enhance their cybersecurity defenses. These funding options support hospitals in upgrading their IT infrastructure, implementing ransomware prevention tools, and establishing disaster recovery plans (Bello *et al*., 2025). By investing in these preventative measures, hospitals can reduce their vulnerability to ransomware attacks and increase their financial resilience (Oduro, 2024). Furthermore, some healthcare systems partner with cybersecurity firms that specialize in ransomware prevention, thereby leveraging external expertise to bolster their defenses (Oparah *et al*., 2024). Insurance companies and governmental bodies are increasingly recognizing the importance of these collaborations and are offering better terms to hospitals that take proactive steps to enhance their cybersecurity posture. Through this multi-layered approach, hospitals can ensure financial resilience in the face of growing ransomware threats.

5. Case Studies and Real-World Examples

5.1 Successful Financial Recovery from Ransomware Attacks

Ransomware attacks on hospitals often have a devastating economic impact, making recovery a daunting challenge. However, several hospitals have successfully mitigated the financial consequences by leveraging comprehensive recovery plans. For example, the integration of advanced cybersecurity measures, including real-time monitoring and encryption technologies, has helped hospitals recover faster by preventing data loss during attacks (Okoruwa *et al*., 2025). Additionally, organizations that maintained up-to-date backup systems were able to restore critical patient data without paying the ransom, significantly reducing financial loss (Bello *et al*., 2025). Successful financial recovery also involves strategic use of insurance policies that cover cyber incidents, allowing hospitals to offset recovery costs such as system repairs, legal fees, and reputation management (Badmus, 2025). This has been crucial for organizations facing significant operational disruptions.

Moreover, the implementation of a digital resilience framework has been key to recovery efforts. Hospitals that engaged in proactive risk assessments and disaster recovery simulations before an attack were able to bounce back more quickly (Lawal & Oduleye, 2025). Hospitals with strong relationships with cybersecurity vendors also experienced smoother recoveries. These vendors provided specialized support for incident response, further ensuring that disruptions were minimized (Ogbete *et al*., 2025). Financially, these hospitals were able to absorb the costs associated with ransomware attacks without resorting to major budget cuts, demonstrating the importance of financial resilience strategies. The lesson from these cases is clear: hospitals that prioritize cybersecurity investment and disaster preparedness are better equipped to recover financially from ransomware incidents.

5.2 Best Practices and Lessons Learned

When examining the financial resilience of hospitals post-ransomware attacks, several best practices have emerged. One critical strategy is investing in layered security measures, including multi-factor authentication, secure access protocols, and frequent system updates (Badmus, 2025). By using these preventive measures, hospitals can mitigate the chances of successful ransomware attacks, reducing the financial impact. In terms of recovery, hospitals have learned that quickly identifying the scope of the attack and containing the damage are vital first steps (Lawal & Oduleye, 2025). For example, hospitals that immediately engaged with cybersecurity experts were able to reduce the financial toll by preventing the spread of the attack across the network (Oduro, 2024). Another valuable lesson is the importance of transparent communication with stakeholders, including patients, regulatory bodies, and insurers, to ensure trust and timely response (Okonkwo *et al*., 2025).

Additionally, hospitals that implemented strong backup solutions and offsite data storage were able to recover critical data without resorting to paying ransom. This has highlighted the importance of an effective data backup and disaster recovery plan (Osuji *et al*., 2024). Financially, hospitals that integrated cyber insurance coverage as part of their risk management strategy were able to recover a significant portion of their losses (Ogbete *et al*., 2025). Moreover, collaboration with local and international cybersecurity bodies has proven beneficial in reducing downtime and restoring operations swiftly. The importance of learning from previous ransomware attacks and continuously refining financial recovery strategies has been underscored by the experiences of hospitals that have successfully recovered from such attacks (Bello *et al*., 2025). These hospitals continually invest in employee training, data protection, and security tools to stay ahead of evolving threats.

5.3 Case Studies of Financial Failures and Recovery Attempts

Despite the best efforts of some hospitals, others have struggled to recover from ransomware attacks, leading to significant financial challenges. For instance, several hospitals faced financial insolvency due to ransomware attacks that resulted in major data breaches and service disruptions. These institutions failed to adequately prepare for cybersecurity risks, which caused a prolonged recovery period (Adenuga *et al*., 2025). One significant failure was a hospital that relied on outdated backup systems, which led to the permanent loss of critical data. As a result, the hospital had to close temporarily and lost substantial revenue due to its inability to provide healthcare services. Additionally, the hospital faced a surge in legal fees and fines as it failed to comply with healthcare data protection regulations (Aminu-Ibrahim *et al*., 2025).

Moreover, some hospitals that did not prioritize cybersecurity investments before the attack experienced long-term financial setbacks. The financial burdens associated with restoring infrastructure and the cost of ransom payments led these hospitals to cut back on essential services, further damaging their reputation (Yusuff *et al*., 2025). However, there were some efforts to recover financially after these setbacks, such as negotiating with creditors and obtaining government assistance. Some hospitals that had minimal cyber defenses found that their post-attack recovery was hindered by delays in claims processing and a lack of support from cyber insurance

policies (Tawose & Oluwadele, 2025). These cases serve as critical lessons, underscoring the necessity for hospitals to invest in proactive cybersecurity measures, including regular updates to backup systems, risk management protocols, and employee training, to avoid financial failure in the face of ransomware threats.

6. Challenges and Recommendations for Enhancing Financial Resilience

6.1 Resource Constraints and Budget Limitations

Hospitals face significant challenges when allocating resources for cybersecurity, particularly in resource-constrained environments. The financial burden of building robust security infrastructure often competes with other critical operational needs, leading to difficult decisions. In many healthcare organizations, cybersecurity is not allocated sufficient funding, as financial resources are primarily directed toward patient care and administrative functions. This imbalance results in underinvestment in essential cybersecurity measures, such as advanced threat detection systems, employee training, and regular software updates. For instance, small and medium-sized hospitals might lack the budget for dedicated cybersecurity teams or state-of-the-art defense technologies, leaving them vulnerable to ransomware attacks.

Moreover, the high cost of compliance with healthcare regulations such as HIPAA adds to budgetary constraints. Many hospitals struggle to prioritize both compliance and cutting-edge cybersecurity practices, often opting for minimal solutions that do not address evolving cyber threats effectively. The limited availability of skilled cybersecurity professionals further exacerbates this issue, with hospitals unable to compete with higher-paying sectors such as finance or technology. As a result, resource constraints force hospitals to make difficult trade-offs between cybersecurity investments and other operational priorities, leaving them vulnerable to attacks that could have been mitigated with better funding and resources.

6.2 Evolving Nature of Cyber Threats and Ransomware Tactics

The landscape of cyber threats is rapidly evolving, with ransomware actors consistently adapting their tactics to bypass traditional security measures. Ransomware attacks have become more sophisticated, using advanced encryption methods, double extortion strategies, and targeting specific vulnerabilities in hospital networks. Cybercriminals are now employing social engineering tactics to trick staff into opening malicious emails or clicking on compromised links. This evolution demands a proactive approach from healthcare organizations, as relying solely on reactive measures is no longer sufficient to defend against modern threats. The increasing frequency and complexity of ransomware tactics require hospitals to continuously update their cybersecurity strategies and invest in next-generation tools to detect and prevent such attacks.

Moreover, the widespread adoption of Internet of Things (IoT) devices in hospitals introduces additional vulnerabilities. These devices often lack robust security protocols and can be exploited by ransomware operators to gain access to sensitive systems. As ransomware groups evolve their tactics, they are increasingly targeting healthcare-specific systems, such as Electronic Health Records (EHR), which contain vast amounts of patient data. The rise of ransomware-as-a-service (RaaS) has lowered the entry barrier for cybercriminals, enabling them to launch attacks more efficiently. These rapidly shifting tactics highlight the need for hospitals to stay vigilant, continuously assess new threats, and adapt their cybersecurity frameworks to maintain resilience against evolving ransomware strategies.

6.3 Recommendations for Improving Hospital Financial Resilience (Cybersecurity Policies, Collaboration, Risk Management)

To improve financial resilience in the face of ransomware threats, hospitals must adopt comprehensive cybersecurity policies that prioritize proactive threat detection and response. These policies should emphasize the importance of a multi-layered defense strategy that includes network segmentation, data encryption, regular patch management, and user training to reduce the risk of human error. Hospitals should also implement strong access control protocols and continuously monitor systems for unusual activity, ensuring that any potential breaches are identified and mitigated in real-time. Furthermore, the integration of cybersecurity best practices into everyday hospital operations is critical to maintaining resilience.

Collaboration plays a vital role in strengthening hospital networks' ability to recover from ransomware attacks. Hospitals should engage with external cybersecurity experts, including government agencies, private cybersecurity firms, and industry associations, to stay ahead of emerging threats. Sharing threat intelligence within the healthcare sector can help identify trends and mitigate risks before they impact operations. Additionally, hospitals should invest in robust risk management frameworks that include comprehensive business continuity plans, ensuring that critical systems can be quickly restored following an attack. A focus on cross-departmental collaboration within hospitals, including IT, legal, and clinical teams, will help to improve the organization’s preparedness and response capacity, ensuring that recovery from ransomware attacks is both swift and cost-effective.

7. References

1. Adeniyi AI, Odejobi O, Taiwo TAIWO. Countermeasures against bias and spoofing in modern facial recognition systems. World Journal of Advanced Research and Reviews. 2025; 25(1):1914-1930.
2. Adenuga MA, Okafor CM, Wedraogo L, Essandoh S, Sakyi JK, Ibrahim AK, *et al*. Analysis of human resource development initiatives and employee career progression. International Journal of Multidisciplinary Futuristic Development. 2025; 6(1):55-64.
3. Adeoye Y, Osunkanmibi AA, Onotole EF, Ogunyankinnu T, Ederhion J, Bello AD, *et al*. Blockchain and Global Trade: Streamlining Cross Border Transactions with Blockchain, 2025.
4. Adeyoyin O, Awanye EN, Morah OO, Ekpedo L. A Conceptual Framework for Integrating ESG Priorities into Sustainable Corporate Operations, 2021.
5. Adeyoyin O, Awanye EN, Morah OO, Ekpedo L. A Model for Operational Resilience and Financial Agility through Data Analytics, 2024.
6. Akinlade OF, Filani OM, Nwachukwu PS. Applied Statistics Models Optimizing Global Supply Chain Networks Under Uncertainty Conditions, 2021.

7. Akinlade OF, Filani OM, Nwachukwu PS. Data Visualization with Predictive Modeling Measuring Workplace Diversity Performance Metrics, 2022.
8. Akinlade OF, Filani OM, Nwachukwu PS. AI-Integrated Procurement Frameworks Aligning Operational Efficiency with Organizational Strategic Goals, 2023.
9. Akinlade OF, Filani OM, Nwachukwu PS. Statistical Approaches for Optimizing Order Promising Accuracy Within Supply Chain Networks, 2023.
10. Akinlade OF, Filani OM, Nwachukwu PS. Statistical Methods Evaluating Multi-Channel Marketing Campaign Effectiveness Across Different Industries, 2023.
11. Akinlade OF, Filani OM, Nwachukwu PS. Automation and digital twins framework reducing procurement errors and turnaround time. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):197-216.
12. Akinlade OF, Filani OM, Nwachukwu PS. Predictive Analytics Models, 2024.
13. Akinleye OK, Adeyoyin O. Process Automation Framework for Enhancing Procurement Efficiency and Transparency, 2021.
14. Akinleye OK, Adeyoyin O. Supplier Relationship Management Framework for Achieving Strategic Procurement Objectives, 2022.
15. Akinleye OK, Adeyoyin O. A Category Spend Mapping and Supplier Risk Assessment Framework for Global Supply Chains, 2023.
16. Akinola AS, Adesanya OS, Okafor CM, Dako OF. Value-chain automation in beverage logistics: Throughput, capacity, and cost avoidance via queueing models. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024; 10(4):1112-1132.
17. Akinola AS, Onyelucheya OP, Okafor CM, Farounbi BO. High-velocity compliance at scale: Queueingtheoretic models for multi-subsidiary reporting deadlines. IRE Journals. 2025; 3(3):310-325.
18. Akin-Oluyomi OT, Okoruwa PO, Babatope OM, Adedayo D. Global trends in procurement and supply chain analytics with implications for manufacturing innovation, 2025.
19. Aminu-Ibrahim AY, Ogbete JC, Ambali KB. Program management models for coordinated multi-site healthcare infrastructure expansion projects. International Journal of Multidisciplinary Research and Growth Evaluation. 2021; 2(6):661-678.
20. Aminu-Ibrahim A, Ogbete JC. Healthcare infrastructure as a public health intervention using evidence from large laboratory networks. Shodhshauryam: International Scientific Refereed Research Journal. 2023; 6(1):256-286.
21. Aminu-Ibrahim A, Ogbete JC. Governance and accountability models for public private partnerships in healthcare infrastructure development. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2943-2960.
22. Aminu-Ibrahim A, Ogbete JC, Ambali KB. Design and development of high-performance medical laboratories supporting pandemic preparedness and response. Shodhshauryam: International Scientific Refereed Research Journal. 2022; 5(3):302-335.
23. Anichukwueze CC, Osuji VC, Oguntegbe EE. Blockchain-based architectures for tamper-proof regulatory recordkeeping and real-time audit readiness. Int J Multidiscip Res Growth Eval. 2021; 2(6):485-504.
24. Anichukwueze CC, Osuji VC, Oguntegbe EE. Digital Marketing Compliance Risk Mitigation: Balancing Growth Objectives with Multi-Jurisdictional Regulations, 2021.
25. Anichukwueze CC, Osuji VC, Oguntegbe EE. LegalTech-Enabled Internal Audit Automation: Advancing Efficiency, Transparency, and Regulatory Preparedness, 2022.
26. Anichukwueze CC, Osuji VC, Oguntegbe EE. Building a Comprehensive AI Governance Risk Index to Support Global Enterprise Decision-Making, 2023.
27. Anichukwueze CC, Osuji VC, Oguntegbe EE. Developing DORA-Aligned Compliance and Resilience Strategies for US Financial Services Organizations, 2024.
28. Anioke SC, Atima ME. Business intelligence applications for mental health resource allocation and public health program accountability. International Journal of Advanced Multidisciplinary Research Studies. 2023; 3(6):2549-2563. Doi: https://doi.org/10.62225/2583049X.2023.3.6.5492
29. Anioke SC, Atima ME. Public health governance models using process optimization and performance metrics for regulatory oversight. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(6):2534-2548. Doi: https://doi.org/10.62225/2583049X.2023.3.6.5491
30. Anioke SC, Atima ME. Public health informatics frameworks for protecting vulnerable populations through data-driven policy enforcement. International Journal of Advanced Multidisciplinary Research Studies. 2023; 3(6):2564-2579.
31. Anioke SC, Atima ME. Predictive Analytics Systems Strengthening Public Health Surveillance and Epidemic Preparedness Decision Making, 2024.
32. Arowogbadamu AAG, Oziri ST, Seyi-Lande OB. Telemarketing and Sponsorship Analytics as Strategic Tools for Enhancing Customer Acquisition and Retention, 2024, 5-56. Doi: https://doi.org/10.54660/GMPJ
33. Awanye EN, Morah OO, Ekpedo L, Adeyoyin O. A Review of Green Investment Strategies and Financial Decision-Making for Sustainability, 2021.
34. Awanye EN, Morah OO, Ekpedo L, Adeyoyin O. A Review of ESG Reporting and Sustainable Finance Practices in Emerging Markets, 2023.
35. Azeez LO, Badmus O. Innovative data integration method for enhancing GHG inventory reporting accuracy and reliability. Global Multidisciplinary Perspectives Journal. 2024; 1(6):166-181. https://www.multiperspectivesjournal.com/search?q=GMP-2024-1-007&search=search
36. Azeez LO, Badmus O. Predictive analytical framework for identifying vapor intrusion risks across urban redevelopment zones. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):524-555.
37. Babatope OM, Akokodaripon DA, Okoruwa PO. The impact of machine learning on predictive maintenance in industrial operations. International Journal of

Advanced Multidisciplinary Research and Studies. 2025; 5(5):1534-1538.
38. Badmus ALOO. Integrated predictive and remote-sensing framework for early warning and regulatory compliance in environmentally sensitive urban zones. IIARD International Journal of Geography & Environmental Management. 2025; 11(12):212-239. https://iiardjournals.org/get/IJGEM/VOL.%2011%20NO.%2012%202025/Integrated%20Predictive%20and%20Remote-Sensing%20212-239.pdf
39. Badmus O, Olamide AL. Hybrid Machine-Learning and Process-Based Model for Predicting Multi Pathway Contaminant Transport in Soil-Water Systems. Gyanshauryam, International Scientific Refereed Research Journal. 2021; 4(3):370-396.
40. Badmus O, Olamide AL. Hybrid Machine-Learning and Process-Based Model for Predicting Multi-Pathway Contaminant Transport in Soil-Water Systems, 2021.
41. Badmus O, Olamide AL. Advanced decision-support model for streamlining environmental compliance in multi-stakeholder projects. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(6):2516-2533. Doi: https://doi.org/10.62225/2583049X.2023.3.6.5484
42. Badmus O, Olamide AL. Advanced Decision-Support Model for Streamlining Environmental Compliance in Multi-Stakeholder Projects, 2023.
43. Badmus O, Olamide AL. Innovative Data Integration Method for Enhancing GHG Inventory Reporting Accuracy and Reliability. Global Multidisciplinary Perspectives Journal. 2024; 1(6):166-181. Doi: https://doi.org/10.54660/GMPJ.2024.1.6.166-181
44. Badmus O, Olamide AL. Integrated predictive and remote-sensing framework for early warning and regulatory compliance in environmentally sensitive urban zones. IIARD International Journal of Geography & Environmental Management. 2025; 11(12):212-239. Doi: https://doi.org/10.56201/ijgem.vol.11.no12.2025.pg212.239
45. Bello AA, Oduro DA, Manu EO, Bello AD, Leo AO, Ukatu CE, *et al*. Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using blockchain: A business analysis approach. Iconic Research and Engineering Journals, 2025; 8(9):297-305.
46. Bello AD, Elebe O, Hammed NI, Okoruwa PO, Fadayomi O, Omoegun GO. An advanced regulatory technology framework for improving financial transparency and fraud reporting accuracy. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):1948-1958.
47. Bello AD, Elebe O, Hammed NI, Omoegun GO, Fadayomi O. A Cybersecurity Risk Management and Regulatory Compliance Framework for Financial Institutions, 2024.
48. Bello AD, Oguntola OB, Achidok J, Ajibade AT, Omotoriogun O, Olabisi F. Artificial Intelligence in Combating Synthetic Identity Fraud: A Comparative Case Study of Amazon and Shopify E-Commerce, 2025.
49. Bello AD, Oguntola OB, Ajibade AT, Akindolani A, Ayoola O, Bello AM. AI-Driven Fraud Detection in UK Digital Payment Systems: Challenges and Solutions, 2025.
50. Bello KA, Oyelaran OA, Tawose OM, Omoyi CO, Yussouff AA. Development of a Gum Production Machine from Manihot Esculenta Waste Peels: FUOYE Journal of Innovation Science and Technology. 2024; 2(1). https://www.jist.fuoye.edu.ng/index.php/jist/article/view/48
51. Efobi OZ, Akinleye OK, Fasawe O. Conceptual Framework for Sustainable Procurement Practices in Local Manufacturing Enterprises in Africa, 2022.
52. Efobi OZ, Akinleye OK, Fasawe O. Conceptual Framework for Developing a Resilience Index for Post-Pandemic Supply Chains, 2023.
53. Ekeocha AH, Aganga AA, Adejoro FA, Oyebanji A, Oluwadele JF, Tawose OM. Phenotypic Characteristics of Indigenous Chickens in Selected Regions of Nigeria. J. World Poult. Res. 2021; 11(3):352-358. pii: S2322455X2100042-11. Doi: https://dx.doi.org/10.36380/jwpr.2021.42
54. Ekwunife DI, Precious OT, Rasul OA, Akinlade OF, Nwokoro TO, Ikpe VI. Cyber threat and information shortage: The immediate risk of supply chain technology and how to tackle them, 2024.
55. Ekwunife DI, Precious OT, Rasul OA, Akinlade OF, Nwokoro TO, Ikpe VI. Technology as a solution to the supply chain problems in the United States: What more can be done? TIMOTHY OGECHUKWU NWOKORO, and VICTORY IHUOMA IKPE. "Technology as a solution to the supply chain problems in the United States: What more can be donem, 2024.
56. Ekwunife DI, Precious OT, Rasul OA, Akinlade OF, Nwokoro TO, Ikpe VI. Using blockchain technology to maximize supply chain and logistics management in north America. Int. J. Sci. Res. Arch. 2024; 12(2):854-863.
57. Ezeh CJ, Anioke SC, Oyewole S, David MG. The role of predictive analytics in enhancing public health surveillance: Proactive and data-driven interventions, 2024.
58. Ezeh FE, Oparah SO, Gado P, Gbaraba SV, Adeleke AS. Designing a Post-Quantum Blockchain Voting Protocol with Zero-Knowledge Proofs for Tamper-Resilient Electoral Infrastructure, 2025.
59. Idika CN, Salami EO, Ijiga OM, Enyejo LA. Deep Learning Driven Malware Classification for Cloud-Native Microservices in Edge Computing Architectures. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021; 7(4).
60. Ijiga OM, Awoyemi O, Atobatele FA, Okonkwo CA. Revolutionizing HR management in US education through advanced technology integration: A theoretical perspective, 2025.
61. Ijiga OM, Awoyemi O, Atobatele FA, Okonkwo CA. Developing a Theoretical Framework for Performance Management Systems in US Schools Evaluating Impact and Best Practices, 2024.
62. Ijiga OM, Awoyemi O, Atobatele FA, Okonkwo CA. Integrating Educational Technology: Policies and Practices for Inclusive Learning. International Journal of Scientific Research in Science, Engineering and Technology. 2024; 11(5):408-420.

63. Ijiga OM, Enyejo LA, Jinadu SO, Akinleye KE, Onwusi CN, Raphael FO. Engineering atmospheric CO_2 utilization strategies for revitalizing mature American oil fields and creating economic resilience. Engineering Science & Technology Journal. 2023; 4(6):741-760. Fair East Publishers.
64. Ijiga OM, Ifenatuora GP, Olateju M. Integrating STEM into instructional design: A framework for culturally relevant curriculum development in underserved communities, 2023.
65. Ijiga OM, Oladoye SO, Bamigwojo OV, Ogboji AJ. Techno-economic evaluation of hybrid solar-diesel microgrids for underserved communities using simulation-based load forecasting. Engineering Science & Technology Journal. 2023; 4:1-28. Fair East Publishers.
66. Ilesanmi MO, Okoh OF, Balogun SA, Ijiga OM. Data-Driven Portfolio Optimization for Utility-Scale Solar, Wind, and Battery Energy Storage Systems (BESS): Integrating Performance Analytics with Investor EBITDA Targets. International Journal of Scientific Research and Modern Technology. 2024; 3(11):141-155.
67. Oluwadele JF, Tawose OM, Ekeocha AH, Akinlabi EY, Adeitan OO, Bello KA. Physiological Indicators and Stress Index of Scavenging Chickens at LAFARGE (Ewekoro) and DANGOTE (Ibese) Cement Factory areas of Ogun-State, Nigeria. Journal of Austrian Society of Agricultural Economics (JASAE), April 2023; 19(4). ISSN: 18158129 E-ISSN: 18151027. https://www.sagepublisher.com/volume/JASAE/19/04/physiological-indicators-and-stress-index-of-scavenging-chickens-at-lafarge-ewekoro-and-dangote-ibese-cement-factory-areas-of-ogun-state-6444f27d93c67.pdf
68. Jinadu SO, Akinleye EA, Onwusi CN, Raphael FO, Ijiga OM, Enyejo LA. Engineering atmospheric CO_2 utilization strategies for revitalizing mature american oil fields and creating economic resilience. Engineering Science & Technology Journal Fair East Publishers. 2023; 4(6):741-760.
69. Joseph OB, Ijiga OM, Olateji M, Okoli I, Frempong D. Comparative perspectives on TVET: Lessons from the United States and developing economies for workforce readiness and economic inclusion. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(2):2493-2506.
70. Joseph OB, Olateji M, Ijiga OM, Okoli I, Frempong D. Future-proofing skills in the Global South: Strategic directions for transforming technical and vocational education and training (TVET). International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(2):2478-2492.
71. Joshua Femi Oluwadele, Adeolu Ademiju Aganga, Anthony Henry Ekeocha, Olayinka Miriam Tawose, Adetumbi Tella, Ebenezer Yemi Akinlabi, *et al*. Effect of Feeding Selected Farm Residues on Growth Performance, Digestibility and Nitrogen Balance of West African Dwarf Bucks: Journal of Applied Life Sciences and Environment. Doi: https://doi.org/10.46909/alse-581163 Vol. 58, Issue 1 (201) / 2025: 33-41 https://jurnalalse.iuls.ro
72. Joshua Femi Oluwadele, Anthony Henry Ekeocha, Olayinka Miriam Tawose, Ebenezer Yemi Akinlabi. Effects of Cooking Methods on Meat Quality of West African Dwarf Rams Fed Napier Grass Silage, Ensiled Sorghum and Crop Residue, Trends in Agricultural Sciences. 2024; 3(2):211-219. Doi: https://doi.org/10.17311/tas.2024.211.219
73. Joshua Femi Oluwadele, Olayinka Miriam Tawose, Anthony Henry Ekeocha, Onyedikachi Augustine Adika, Peter Dipo Arowosegbe, Ebenezer Yemi Akinlabi. Alternative feeds for West African dwarf rams: A cost-benefit relationship and their long-term effect: Journal of the Selva Andina Animal Science. 2025; 12(1):45-57. Doi: https://doi.org/10.36610/j.jsaas.2025.120100045
74. Kazeem A Bello, Abdulrahman Adama, Olayinka M Tawose, Bukola O Bolaji. Development and Performance Evaluation of a Poultry Bird De-Feathering Machine. FUOYE Journal of Engineering and Technology, December 2022; 7(4). ISSN: 2579-0617 (Paper), 2579-0625 (Online). Doi: http://dx.doi.org/10.46792/fuoyejet.vAiB.C
75. Kazeem Aderemi Bello, Temitayo Mufutau Azeez, Olayinka Miriam Tawose, Kazeem Olabisi Odesanya, Odumuyiwa A Odumosu, Olatunde Ajani Oyelaran. Investigating the Influence of Rubber Seed Oil and Used Cooking Oil on Diesel, E3S Web of Conferences. 2023; 430:01217, Pg 14. Doi: https://doi.org/10.1051/e3sconf/202343001217.
76. Lamidi OBAO. Comprehensive evaluation model for improving carbon accounting accuracy in corporate sustainability programs. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 10(1):825-853. Doi: https://doi.org/10.32628/IJSRCSEIT
77. Lawal OA, Oduleye TE. A conceptual decision model for capital allocation using financial analytics. Gyanshauryam, International Scientific Refereed Research Journal. 2021; 4(2):269-295. Doi: https://doi.org/10.32628/GISRRJ
78. Lawal OA, Oduleye TE. A Conceptual Decision Model for Capital Allocation Using Financial Analytics, 2021.
79. Lawal OA, Oduleye TE. Aligning financial planning analytics with corporate strategy: A conceptual integration model. Shodhshauryam, International Scientific Refereed Research Journal. 2021; 4(3):319-346.
80. Lawal OA, Oduleye TE. Aligning Financial Planning Analytics with Corporate Strategy. A Conceptual Integration Model, 2021.
81. Lawal OA, Oduleye TE. Linking customer experience data to revenue outcomes: A conceptual financial intelligence model. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(3):867-890. Doi: https://doi.org/10.32628/CSEIT2215512
82. Lawal OA, Oduleye TE. A review of decision analytics models for sustainable profitability in technology firms. Gyanshauryam, International Scientific Refereed Research Journal. 2023; 6(6):247-274.
83. Lawal OA, Oduleye TE. Predictive financial risk analytics: A conceptual model for long-term value preservation. Journal of Accounting and Financial Management. 2025; 11(12):476-503. Doi: https://doi.org/10.56201/jafm.vol.11.no12.2025.pg476.503
84. Lenin Ifeanyi Obi, Gabriel Dogbanya, Lilian

Chinweotito Awah, Olayinka Miriam Tawose, Chinwendu Ubani, Ayodele Blessing Ayo-ige, *et al*. A Systematic Analysis of Effectiveness of Nurse-Led Dementia Care Interventions on Health Outcomes Among Community-Dwelling Older Adults. (2025). Journal of Pharma Insights and Research. 2025; 3(5):24-33. Doi: https://doi.org/10.69613/3f5cq717

85. Liadi KO. A Policy Alignment Model for Nigeria's Foreign Policy and Global Climate Diplomacy Goals, 2022.
86. Liadi KO. Developing a Continental Peace Integration Framework: Nigeria's Role in African Union Foreign Policy Initiatives, 2022.
87. Liadi KO. Developing a Peacebuilding Effectiveness Framework for Nigeria's Foreign Policy in West Africa, 2022.
88. Liadi KO. A Model for Linking Nigeria's Diplomatic Engagement to Sustainable Development Outcomes in ECOWAS States, 2023.
89. Liadi KO. An economic interdependence model of Nigeria-China relations and its effects on industrial growth and infrastructure. Shodhshauryam: International Scientific Refereed Research Journal. 2023; 6(4):570-599.
90. Liadi KO. Designing an Oil Diplomacy Diversification Model: Assessing the Shift from Petroleum Influence to Broader Economic Engagement, 2023.
91. Liadi KO. A Soft Power Projection Framework: Education, Cultural Diplomacy, and Regional Development in Nigeria's Foreign Policy, 2024.
92. Liadi KO. Conceptualizing a governance reform impact model for Nigeria's peacekeeping missions in post-conflict states. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(1):1622-1636.
93. Liadi KO. Designing a Cross-Border Security Cooperation Model: Nigeria's Foreign Policy Response to Regional Terrorism, 2024.
94. Liadi KO. Developing a Humanitarian Diplomacy Model: Nigeria's Foreign Policy and Post-Conflict Recovery in the Sahel, 2024.
95. Kazeem Bello M, Olayinka Tawose M, Abdulrahman Adama O, Bukola Bolaji. Factor Analysis of Poultry Birds De-Feathering Machines; FUOYE Journal of Engineering and Technology. 2022; 7(3). Doi: https://doi.org/10.46792/fuoyejet.v7i3.829
96. Medon JJ, Oduleye TE. A Comprehensive Financial Reporting Model for Strengthening Compliance and Organizational Accountability Systems, 2022.
97. Medon JJ, Oduleye TE. An Integrated Predictive Analytics Model for Enhancing Strategic Financial Forecasting and Decision Accuracy, 2024.
98. Medon J, Oduleye T. Developing a Financial Planning Model for Sustainable Profitability in Dynamic Business Environments. Shodhshauryam Int. Sci. Ref. Res, 2023, 448-464.
99. Michael ON, Ogunsola OE. Applying Quantitative Agricultural Economics Models to Improve Food System Efficiency and Policy Decision-Making, 2023.
100. Michael ON, Ogunsola OE. Evaluating the Effectiveness of Rural Innovation Hubs in Accelerating Agricultural Transformation and Economic Empowerment, 2023.
101. Michael ON, Ogunsola OE. Assessing the Potential of Renewable Energy Technologies for Sustainable Irrigation and Smallholder Farm Productivity. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):380-411.
102. Michael ON, Ogunsola OE. Advancing rural agribusiness innovation strategies for building climateresilient and economically inclusive communities. Journal of Social Science and Human Research Studies. 2025; 1(5):161-177.
103. Michael ON, Ogunsola OE. Agribusiness diversification strategies for managing economic volatility in resource-constrained agricultural economies. IRE Journals, 2025.
104. Michael ON, Ogunsola OE. Assessing the role of artificial intelligence in transforming decision making across modern agricultural systems. Engineering and Technology Journal. 2025; 10(12). Doi: https://doi.org/10.47191/etj/v10i12.06
105. Michael ON, Ogunsola OE. Evaluating the impact of sustainable agriculture curriculum integration on STEM education and career outcomes. Journal of Social Science and Human Research Studies. 2025; 1(5):178-194.
106. Monye Stella Isioma, Bello Kazeem Aderemi, Omotehinse Samuel Ayodeji, Ikumapayi Omolayo M, Tawose Olayinka Miriam TB, Adeleke Awogbemi Omojola, *et al*. Achieving Energy Sustainability in Nigeria's Telecommunications Industry through Renewable Propane. NIPES: Journal of Science and Technology Research (Special Issue). 2025; 7(2):3320-3325. Doi: https://doi.org/10.37933/nipes/7.4.2025.SI398eISSN-2682-5821| pISSN-2734-2352
107. Morah OO, Awanye EN, Ekpedo L, Adeyoyin O. A Model for Evaluating Hedging Strategies and Working Capital Efficiency in Volatile Markets, 2021.
108. Ndukwe C, Melville AC, Osman M, Mohammed Y, Oduro M, Ankrah PK, *et al*. Neurological complications associated with the Powassan virus and treatment interventions. Cureus. 2024; 16(10).
109. Odejobi OD, Okonkwo CS, Ahiaeke Patrick MC, Okeke OT, Mayo W. AI-augmented secure software engineering: Leveraging deep learning for autonomous threat detection and mitigation. International Journal of Engineering and Modern Technology (IJEMT). 2025; 11(12):101-121. Doi: https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg101.121
110. Oduleye TE, Medon JJ. A Data-Driven Cost Management Model for Improving Strategic Financial Planning and Performance Evaluation. International Journal of Multidisciplinary Research and Growth Evaluation. 2021; 2(6):524-537.
111. Oduleye TE, Medon JJ. A Predictive Model for Optimizing Cash Flow and Working Capital Management in Corporations, 2023.
112. Oduro DA, Okolo JN, Bello AD, Ajibade AT, Muritala A. AI-powered fraud detection in digital banking: Enhancing security through machine learning, 2025.
113. Oduro M. Process safety model integrating human factors within offshore pipeline commissioning operations systems. International Journal of Scientific

Research in Computer Science, Engineering and Information Technology. 2023; 10(1):934-957.
114. Oduro M. Lifecycle Conceptual Model for Managing Offshore Pipeline Decommissioning and Reinstallation Projects Execution, 2024.
115. Ogbete JC, Aminu-Ibrahim A. Translating healthcare infrastructure investment into measurable population health and diagnostic outcomes. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(2):955-985.
116. Ogbete JC, Aminu-Ibrahim AY. Lifecycle performance evaluation of purpose built diagnostic laboratories supporting long term healthcare delivery. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(6):2605-2621.
117. Ogbete JC, Aminu-Ibrahim A, Ambali KB. Design standards and operational planning frameworks for scalable blood collection networks. Gyanshauryam: International Scientific Refereed Research Journal. 2022; 5(6):267-300.
118. Ogbete JC, Aminu-Ibrahim A, Iwuanyanwu OC. Digital and BIM enabled coordination methods for delivering complex medical facility projects. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):1991-2010.
119. Ogbete JC, Aminu-Ibrahim A, Iwuanyanwu OC. Integrating healing centered design principles into diagnostic and laboratory facility planning. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025; 11(6):516-533.
120. Ogbole JI, Okoruwa PO, Fadayomi O, Akeju B, Edivri J, Abolaji TO. Security analytics and digital forensics for enterprise risk management, advances and practical implications. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):2017-2028.
121. Ogunboye I, Adebayo IPS, Anioke SC, Cherechi E, Egwuatu CFA, Awuah SB. Enhancing Nigeria's health surveillance system: A data-driven approach to epidemic, 2023.
122. Ogunboye I, Adebayo IPS, Anioke SC, Egwuatu EC, Ajala CF, Awuah SB. Enhancing Nigeria's health surveillance system: A data-driven approach to epidemic preparedness and response. World Journal of Advanced Research and Reviews. 2023; 20(1).
123. Ogunsola OE, Michael ON. Analyzing the alignment of agricultural policy frameworks with national sustainable development priorities. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021; 7(1):518.
124. Ogunsola OE, Nurudeen OM. Exploring gender inclusion and equity across agricultural value chains in Sub-Saharan Africa's emerging markets. Gyanshauryam, International Scientific Refereed Research Journal. 2022; 5(5):289.
125. Oguntegbe EE, Farounbi BO, Okafor CM. Conceptual review of inclusive leadership practices to strengthen investment committee decision-making. Journal of Frontiers in Multidisciplinary Research. 2023; 3(3):1215-1225.
126. Okafor CM, Dako OF, Osuji VC. Architecting Embedded Finance Ecosystems that Converge Payments, Credit, and Data Services for Inclusive Economic Growth, 2023.
127. Okafor CM, Dako OF, Osuji VC. Architecting Embedded Finance Ecosystems that Converge Payments, Credit, and Data Services for Inclusive Economic Growth, 2023.
128. Okafor CM, Dako OF, Adesanya OS, Farounbi BO. Finance-Led Process Redesign and OPEX Reduction: A Casual Inference Framework for Operational Savings. J Oper Effic. 2021; 19(3):301-318.
129. Okafor CM, Farounbi BO, Adesanya OS, Akinola AS. Controls for cross-border payments operations: Correspondent banking risk reduction via end-to-end monitoring. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024; 10(4):1050-1071.
130. Okafor CM, Onyelucheya OP, Farounbi BO, Fatimetu O. Go-to-Market Strategy under Uncertainty: Bayesian Learning Loops for Segmentation and Experiment-Driven Growth, 2023.
131. Okafor CM, Osuji VC, Dako OF. Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):316-337.
132. Okonkwo CA, Ijiga OM, Awoyemi O, Atobatele FA. Integrating chemistry and social studies: Teaching the impact of chemical advances on society. Engineering and Technology Journal. 2025; 10(7):5894-5900.
133. Okonkwo CS, Agbabiaka J, Ogunwole O, Mayo W, Okeke OT. Framework for secure and scalable supply chain systems supporting national energy reliability. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2816-2826. Doi: https://doi.org/10.62225/2583049X.2024.4.6.5494
134. Okonkwo CS, Agbabiaka J, Ogunwole O, Mayo W, Okeke OT. Review of digital supply chain models for cost control and operational continuity. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2836-2846. Doi: https://doi.org/10.62225/2583049X.2024.4.6.5496
135. Okonkwo CS, Ahiaeke Patrick MC, Okeke OT, Mayo W. Framework for national-scale supply chain optimization through integrated IT and procurement systems. Gulf Journal of Advance Business Research. 2025; 3(12):1610-1625. Doi: https://doi.org/10.51594/gjabr.v3i12.189
136. Okonkwo CS, Mayo W, Okeke OT. Conceptual model for asset lifecycle management and inventory visibility. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 10(1):809-824. Doi: https://doi.org/10.32628/CSEIT2391568
137. Okonkwo CS, Patrick MCA, Okeke OT, Mayo W. Framework for integrating IT systems engineering with supply chain operations. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(6):2580-2589. Doi: https://doi.org/10.62225/2583049X.2023.3.6.5500
138. Okoruwa PO, Babatope OM, Akokodaripon DA, Akinleye OK. Digital procurement transformation approaches for strengthening efficiency in global supply chain management. Journal of Supply Chain Management. 2025; 1(1):1-15.

139. Oladoye SO, Bamigwojo OV, James AO, Ijiga OM. AI-Driven Predictive Maintenance Modeling for High-Voltage Distribution Assets Using Sensor Fusion and Time-Series Degradation Analysis, 2021.
140. Olamide AL, Badmus O. Machine-Learning Approach to Forecasting Soil and Groundwater Pollution Under Changing Climate. Shodhshauryam, International Scientific Refereed Research Journal. 2021; 4(5):208-239.
141. Olamide AL, Badmus O. Comprehensive Evaluation Model for Improving Carbon Accounting Accuracy in Corporate Sustainability Programs. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 10(1):825-853.
142. Olamide AL, Badmus O. Predictive analytical framework for identifying vapor intrusion risks across urban redevelopment zones. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):524-555. Doi: https://doi.org/10.32628/IJSRSSH243675
143. Olatunji GI, Oparah OS, Ezeh FE, Ajayi OO. Modeling the Relationship Between Dietary Diversity Scores and Cognitive Development Outcomes in Early Childhood, 2023.
144. Olatunji GI, Oparah OS, Ezeh FE, Oluwanifemi O. Telehealth Integration Framework for Ensuring Continuity of Chronic Disease Care Across Geographic Barriers, 2022.
145. Oluwadele Joshua Femi, Tawose Olayinka Miriam, Akinlabi Ebenzer Yemi, Ekeocha Anthony Henry, Odumboni Adeleke Azeez, Akinboye Jumoke, *et al*. Optimizing broiler diets with dietary fiber: impact on growth performance, carcass characteristics, and sensory evaluation. Journal of the Selva Andina Animal Science JSAAS, 2025. Doi: https://doi.org/10.36610/j.jsaas.20252324. ISSN 2311-2581
146. Oluwadele JF, Samuel O, Tawose OM, Ekeocha AH, Adika AO. Evaluation of alternative energy sources to replace maize in Marshall broiler diets: Effects on growth performance, meat quality, and serum biochemistry. EUREKA: Life Sciences, 2025. Doi: https://doi.org/10.21303/2504-5695.2025
147. Oluwadele JF, Tawose OM, Adetumbi T. Evaluation of feed intake, growth performance, and carcass characteristics of West African dwarf rams fed mango leaves, Napier grass, Neem Seed Cake, and concentrate for fattening. EUREKA: Life Sciences. 2024; (4):11-19. Doi: https://doi.org/10.21303/2504-5695.2024.003603
148. Oluwadele JF, Ekeocha AH, Aganga AA, Tawose OM, Odumboni A, Ofodome CI, *et al*. Effects of feeding Pennisetum purpureum silage supplemented with selected farm residues on growth performance and meat quality of West African dwarf rams. SVU-International Journal of Agricultural Sciences. 2024; 6(3):190-196. https://svuijas.journals.ekb.eg/article_384457.html
149. Omoegun GO, Oduro M. Integrated Systems Framework for Commissioning Readiness Assessment in Offshore Processing Facilities Projects, 2024.
150. Oparah OS, Ezeh FE, Olatunji GI, Ajayi OO. Big Data-Enabled Predictive Models for Anticipating Infectious Disease Outbreaks at Population and Regional Levels, 2022.
151. Oparah OS, Ezeh FE, Olatunji GI, Ajayi OO. Framework for designing national real-time disease surveillance dashboards for public health stakeholders. Shodhshauryam. International Scientific Refereed Research Journal. 2023; 6(1):208-227.
152. Oparah OS, Ezeh FE, Olatunji GI, Ajayi OO. Framework for integrating climate data and health outcomes to improve mortality risk prediction systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024; 10(2):1128-1150.
153. Oparah OS, Ezeh FE, Olatunji GI, Ajayi OO. Conceptual design of national-level public health dashboards for transparent and evidence-based decision-making. International Journal of Applied Research in Social Sciences. 2025; 7(10):805-826.
154. Oparah SO, Ezeh FE, Gado P, Adeleke AS, Vure S. Stigma Reduction Framework for Improving Community Uptake of Infectious Disease and HIV Diagnostic Services, 2025.
155. Oparah SO, Gado P, Ezeh FE, Gbaraba SV, Adeleke AS. Assessing the Operational and Psychosocial Impact of the Compressed Workweek: A Meta-Analytic Review of Four-Day Work Week Trials Across Industries, 2024.
156. Oparah SO, Gado P, Ezeh FE, Gbaraba SV, Suliat A. Comprehensive Review of Telehealth Effectiveness in Bridging Rural-Urban Disparities in Healthcare Access, 2024.
157. Oshoba TO, Ahmed KS, Odejobi OD. Proactive Threat Intelligence and Detection Model Using Cloud-Native Security Tools, 2023.
158. Osuji VC, Dako OF, Okafor CM. Seamless Integration of Digital Supply-Chain Platforms with Commercial Banking to Enhance Working Capital Efficiency for SMEs, 2023.
159. Osuji VC, Dako OF, Okafor CM. Orchestrating Multi-Vertical Digital Ecosystem Platforms across Housing, Education, Health, and Mobility to Drive Shared Prosperity. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):338-359.
160. Osuji VC, Okafor CM, Dako OF. Developing Predictive, Data-Driven Growth Models for Transaction Banking to Optimize Corporate and Public-Sector Outcomes, 2022.
161. Osunkanmibi AA, Adeoye Y, Ogunyankinnu T, Onotole EF, Salawudeen MD, Abubakar MA, *et al*. Cybersecurity and Data Protection in Supply Chains: AI's Role in Protecting Sensitive Financial Data across Supply Chains, 2025.
162. Owoade OA, Moneke KC, Anioke SC. Leveraging Business Intelligence to Optimize Resource Allocation in Mental Health and Substance Abuse Centers. Journal of Scientific and Engineering Research. 2022; 9(12):210-235.
163. Oziri ST, Arowogbadamu AAG, Seyi-Lande OB. Predictive modeling applications designing usage and retention testbeds to improve campaign effectiveness and strengthen telecom customer relationships. Unpublished Manuscript, 2022.
164. Oziri ST, Arowogbadamu AAG, Seyi-Lande OB. Revenue Forecasting Models as Risk Mitigation Tools Leveraging Data Analytics in Telecommunications Strategy, 2023.

165. Oziri ST, Arowogbadamu AA-G, Seyi-Lande OB. Transforming big data into strategy: Comprehensive frameworks for business optimization in telecommunications. Gulf Journal of Engineering & Technology. 2025; 1(5):94-111.
166. Rukh S, Oziri ST, Seyi-Lande OB. Framework for enhancing marketing strategy through predictive and prescriptive analytics. Shodhshauryam, International Scientific Refereed Research Journal. 2023; 6(4):531-569.
167. Rukh S, Seyi-Lande OB, Oziri S. A model for advancing digital inclusion through business analytics and partnerships. Gyanshauryam, International Scientific Refereed Research Journal. 2023; 6(5):661-700.
168. Rukh S, Seyi-Lande OB, Oziri ST. An integrated framework for AI and predictive analytics in supply chain management. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(1):451-491.
169. Sanni JO, Adumaza A. A comprehensive framework for digital transformation in capital markets: Solving operational challenges and enhancing stakeholder engagement. Gyanshauryam, International Scientific Refereed Research Journal. 2023; 6(6):275-302.
170. Sanni JO, Attah A. Market research frameworks addressing entry barriers within highly regulated industrial service sectors. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 9(2):904-930.
171. Sanni JO, Wedraogo L. Data centric funnel optimization frameworks resolving revenue leakage in high value services. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2859-2874.
172. Sanni JO, Iwuanyanwu UA, Essien MA. Problem-oriented process mining for auditable marketing automation lifecycle control. International Journal of Advanced Multidisciplinary Research and Studies. 2025; 5(6):1933-1947.
173. Sanni JO, Iwuanyanwu UA, Essien MA, Attah A. Lifecycle-aware marketing automation using federated learning for secure cross-organizational data management. Gyanshauryam, International Scientific Refereed Research Journal. 2023; 6(6):337-364.
174. Sanni JO, Iwuanyanwu UA, Essien MA, Wedraogo L. Integrating blockchain-enabled smart contracts for transparent and verifiable marketing workflows. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2891-2906.
175. Seyi-Lande OB, Arowogbadamu AAG, Oziri ST. Cross-Functional Key Performance Indicator Frameworks for Driving Organizational Alignment and Sustainable Business Growth. International Journal of Multidisciplinary Futuristic Development. 2022; 1(2):1-18.
176. Seyi-Lande OB, Arowogbadamu AAG, Oziri ST. Subscriber Base Expansion Through Strategic Innovation and Market Penetration in Competitive Telecommunications Landscapes, 2024.
177. Shah R, Oziri ST, Seyi-Lande OB. A framework for leveraging artificial intelligence in strategic business decision-making. Gulf Journal of Advance Business Research. 2025; 3(11):1517-1558.
178. Stella Isioma Monye, Ilesanmi Afolabi Daniyan, Ngozi Snow Monye, Omolayo M Ikumapayi, Kazeem Aderemi Bello, Omowumi Boboye, *et al*. Hydrogen Infrastructure for a Sustainable Future: Challenges, Innovations, and Global Opportunities; NIPES-Journal of Science and Technology, Research. 2025; 7(2):3302-3308. Doi: https://doi.org/10.37933/nipes/7.4.2025.SI395
179. Tawose OM, Ekeocha AH, Oluwadele JF. Nutritional Quality and Utilization of Water Hyacinth-Cassava Peels Silage by West African Dwarf (WAD) Goats: Vol 6 No 1 (2022): FUOYE Journal of Agriculture and Human Ecology; (FUOJAHE), 2023, 35-45. http//agriculture.fuoye.edu.ng/journal
180. Tawose OM, Ekeocha AH, Oluwadele JF. Heamatological and Biochemical Responses of West African Dwarf Goats fed Water Hyacinth-Cassava Peels Silage. Nigerian Society of Animal Production (NSAP). 2024; 50(3). Doi: https://doi.org/10.51791/njap.v50i3.4030
181. Tawose OM, Oluwadele JF, Ekeocha AH, Odumboni AA, Egbeyemi OS. Aflatoxin Detection and Quantification in Poultry Feeds Available in Selected Areas in Ekiti State, FUOYE Journal of Agriculture and Human Ecology (FUOJAHE). 2023; 7(2). Doi: https://doi.org/10.62923/fuojahe.v7i2.302
182. Tawose Olayinka, Oluwadele Joshua. Comparative Analysis of the Nutritional Potentials of Selected Tuber Peel Meals as Feed Supplements for Ruminant Animals. Nigerian Journal of Agriculture and Agricultural Technology NJAAT. 2025; 5(3A). https://njaat.com.ng/index.php/njaat/article/view/1169; ISSN (Print): 2811-1885; ISSN (Online): 2811-1893.
183. Uduokhai DO, Garba BMP, Nwafor MI, Sanusi AN. Techno-Economic Evaluation of Renewable-Material Construction for Low-Income Housing Communities. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(2):888-908.
184. Uduokhai DO, Garba BMP, Nwafor MI, Sanusi AN. Techno-Economic Evaluation of Renewable-Material Construction for Low-Income Housing Communities. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(2):888-908.
185. Uduokhai DO, Garba BMP, Nwafor MI, Sanusi AN. Modeling user experience and post-occupancy satisfaction in government-sponsored housing projects. Gyanshauryam, International Scientific Refereed Research Journal. 2023; 6(2):479-497.
186. Uduokhai DO, Garba BMP, Sanusi AN, Nwafor MI. Computational modelling of climate-adaptive building envelopes for energy efficiency in tropical regions. Global Journal of Engineering and Technology Review. 2025; 1(3):129-141.
187. Uduokhai DO, Garba BMP, Sanusi AN, Nwafor MI. Computational modelling of climate-adaptive building envelopes for energy efficiency in tropical regions. Global Journal of Engineering and Technology Review. 2025; 1(3):129-141.
188. Uduokhai DO, Giloid S, Nwafor MI, Adio SA. Evaluating the role of building information modeling in enhancing project performance in Nigeria. International Journal of Advanced Multidisciplinary Research and Studies. 2023; 3(6):2154-2161.
189. Uduokhai DO, Nwafor MI, Giloid S, Adio SA.

Evaluation of public-private partnership frameworks for effective affordable housing delivery in Africa. Shodhshauryam, International Scientific Refereed Research Journal. 2022; 5(1):224-242.
190. Uduokhai DO, Nwafor MI, Sanusi AN, Garba BMP. Predictive framework for optimizing maintenance schedules in aging public infrastructure systems. Global Journal of Engineering and Technology Review. 2025; 1(3):142-152.
191. Uduokhai DO, Nwafor MI, Sanusi AN, Garba BMP. Predictive framework for optimizing maintenance schedules in aging public infrastructure systems. Global Journal of Engineering and Technology Review. 2025; 1(3):142-152.
192. Uduokhai DO, Nwafor MI, Sanusi AN, Garba BMP. System Dynamics Modeling of Circular Economy Integration within the African Construction Industry. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(2):871-887.
193. Uduokhai DO, Nwafor MI, Sanusi AN, Garba BMP. System Dynamics Modeling of Circular Economy Integration within the African Construction Industry. International Journal of Scientific Research in Humanities and Social Sciences. 2024; 1(2):871-887.
194. Uduokhai DO, Nwafor MI, Sanusi AN, Garba BMP. Applying design thinking approaches to architectural education and innovation in Nigerian universities. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 9(4):852-870.
195. Uduokhai DO, Nwafor MI, Sanusi AN, Patrick BM. Critical Review of Housing Policy Implementation Strategies in Sub-Saharan African Urban Economies, 2023. Doi: https://doi. org/10.32628/SHISRRJ236927
196. Uduokhai DO, Sanusi AN, Nwafor MI, Garba BMP. Institutional ethics and professional governance in urban design and architectural practice in Africa. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2683-2695.
197. Ussher-Eke D, Okoh OF, Ijiga OM. The role of biometric and IoT-based attendance systems in streamlining HR administrative functions, enhancing workforce accountability, and reducing labor inefficiencies. International Journal for Multidisciplinary Research (IJFMR). 2025; 7(4).
198. Wedraogo L, Sanni JO. Machine learning models addressing uncertainty in cross channel campaign performance forecasting accuracy. International Journal of Advanced Multidisciplinary Research and Studies. 2024; 4(6):2875-2890.
199. Yusuff M, Akinsola O, Olabiyi M, Anioke SC, Agbasiere C, Kamwesiga J. Leveraging AI in Drug and Substance Abuse Recovery: A Systematic Approach to Reintegration and Rehabilitation for the Homeless. Journal of Medicine and Health Research. 2025; 10(1):20-30.