Int. j. adv. multidisc. res. stud. 2025; 5(6):2269-2283

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

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

A Review of Zero Trust Security Models and Cost Effectiveness in Healthcare Infrastructure

[1] Abolaji Adebayo, [2] Chukwudera Obumneke Anunagba, [3] David Excel Ozowara
[1] East Tennessee State University, USA
[2] Barclays Whippany, New Jersey, USA
[3] Western Illinois University, Macomb, Illinois, USA

DOI: https://doi.org/10.62225/2583049X.2025.5.6.6051
Corresponding Author: **Abolaji Adebayo**

Abstract
Zero Trust Security Models (ZTSMs) have emerged as a robust cybersecurity framework in response to the increasingly sophisticated threat landscape, particularly within healthcare infrastructure. With the continuous rise in cyberattacks targeting sensitive health data, healthcare organizations are increasingly adopting Zero Trust models to mitigate risks and ensure data protection. This review paper examines the principles of Zero Trust security models, focusing on their application within healthcare systems, highlighting their effectiveness in safeguarding critical infrastructure, patient data, and medical devices. The paper explores various components of Zero Trust frameworks, such as continuous verification, least-privilege access, and micro-segmentation, providing a comprehensive understanding of how these principles function in healthcare settings. Additionally, the paper evaluates the cost-effectiveness of implementing Zero Trust architectures in healthcare, considering factors like operational expenses, system integration, and long-term security benefits. Challenges in adoption, including resistance to change and high initial setup costs, are addressed, alongside recommendations for overcoming these barriers. The analysis also includes a comparative overview of Zero Trust models versus traditional perimeter-based security systems, emphasizing the unique advantages of Zero Trust in managing ever-evolving threats within the healthcare industry. Finally, the paper presents future directions for research, focusing on the integration of artificial intelligence and machine learning in enhancing Zero Trust security protocols and improving overall security posture. This review aims to provide healthcare organizations with a well-rounded understanding of the Zero Trust model's potential in enhancing cybersecurity and its impact on healthcare costs, operational efficiency, and patient privacy.

Keywords: Zero Trust Security Models, Healthcare Cybersecurity, Data Protection, Healthcare Infrastructure, Cost-Effectiveness, Security Frameworks

1. Introduction to Zero Trust Security Models in Healthcare

1.1 Overview of Zero Trust Security Models

Zero Trust Security Models (ZTSM) represent a significant shift in how organizations approach cybersecurity, particularly in environments where sensitive data must be protected, such as healthcare. Unlike traditional security models that focus on perimeter defenses, Zero Trust operates on the principle of "never trust, always verify." This model assumes that both internal and external networks are vulnerable, and thus, every request for access—whether from inside or outside the organization—must be continuously verified before access is granted (Ijiga, Awoyemi, Atobatele, & Okonkwo, 2025). By enforcing this constant scrutiny, ZTSM helps to eliminate vulnerabilities that arise from implicit trust and protects against both external attacks and insider threats. In healthcare, where patient privacy and data protection are paramount, this model is gaining traction as it mitigates the risk of data breaches and ensures compliance with regulations such as HIPAA.

ZTSM works by implementing several key principles: least-privilege access, continuous authentication, micro-segmentation, and strict access control. Each of these components helps healthcare organizations enforce tighter security policies across a variety of systems, from patient records to medical devices. By continuously validating and revalidating access rights, ZTSM ensures that even legitimate users cannot access more information or resources than necessary, thus reducing the risk of a breach if an account is compromised (Ogbete, Aminu-Ibrahim, & Ambali, 2025). Additionally, by applying ZTSM, healthcare

providers can limit the impact of potential security incidents by isolating systems into segments, ensuring that an attack on one segment does not compromise others. This approach represents a proactive, not reactive, stance on security and is particularly well-suited for the dynamic and highly regulated healthcare sector.

1.2 Importance of Cybersecurity in Healthcare

The importance of cybersecurity in healthcare cannot be overstated, as the industry is one of the most targeted sectors for cyberattacks. Healthcare organizations manage vast amounts of sensitive data, including personal health information, financial data, and proprietary research, making them prime targets for cybercriminals. Data breaches not only compromise patient privacy but also expose organizations to financial penalties, legal liabilities, and reputational damage. As healthcare systems continue to digitalize and expand, ensuring robust cybersecurity measures becomes critical to protect both patient trust and organizational integrity (Adeyoyin, Awanye, Morah, & Ekpedo, 2024). Healthcare data breaches can have devastating consequences, affecting individuals' lives and potentially undermining public health initiatives.

A key challenge in healthcare cybersecurity is the complexity of the systems involved. From Electronic Health Records (EHRs) to medical devices, each component of the healthcare ecosystem presents unique security risks. Cybersecurity frameworks, such as Zero Trust, are necessary to address these diverse vulnerabilities. These models ensure that every device, user, and application is continuously authenticated, even within trusted internal networks. The adoption of Zero Trust models in healthcare can significantly reduce the risk of a breach by enforcing strict access controls, minimizing the attack surface, and ensuring compliance with healthcare regulations (Seyi-Lande, Arowogbadamu, & Oziri, 2024). With the increasing frequency and sophistication of cyberattacks, healthcare organizations must take proactive measures to safeguard patient data and maintain the integrity of their digital infrastructure (Ogbete & Aminu-Ibrahim, 2024).

1.3 Scope and Objectives of the Review

This review aims to provide an in-depth analysis of Zero Trust security models, with a particular focus on their application in healthcare environments. The paper explores the underlying principles of Zero Trust, evaluates its effectiveness in securing healthcare infrastructure, and discusses the challenges faced by healthcare organizations in implementing these models. By examining case studies and industry reports, this review will identify the most effective strategies for integrating Zero Trust models into existing healthcare IT frameworks. The scope of the review extends to both large healthcare institutions and smaller practices, offering insights into how Zero Trust can scale to meet diverse organizational needs.

The objectives of this review are to (1) assess the benefits and limitations of Zero Trust security models in healthcare, (2) explore the technological advancements enabling Zero Trust adoption, and (3) provide recommendations for healthcare organizations considering the implementation of Zero Trust frameworks. This review will also examine the cost-effectiveness of Zero Trust models, including an analysis of the initial investment and long-term operational savings. Through a detailed exploration of these areas, the review aims to provide healthcare professionals, IT managers, and policymakers with a comprehensive understanding of how Zero Trust can enhance security and compliance within healthcare systems.

1.4 Structure of the Paper

This paper is organized into several sections, each focusing on a critical aspect of Zero Trust security models and their application in healthcare. Section 1 provides an introduction, covering the overview of Zero Trust models, the importance of cybersecurity in healthcare, and the objectives of this review. Section 2 explores the core principles of Zero Trust, including continuous verification, least-privilege access, and micro-segmentation. Section 3 discusses the practical application of these principles in healthcare environments, with a particular focus on securing patient data and medical devices. Section 4 evaluates the cost-effectiveness of Zero Trust models, analyzing both the initial implementation costs and long-term savings. Section 5 addresses the challenges healthcare organizations face in adopting Zero Trust models and offers strategies to overcome them. Finally, Section 6 concludes the paper, summarizing key findings and suggesting future research directions for improving healthcare cybersecurity through Zero Trust.

2. Core Principles of Zero Trust Security Models

2.1 Continuous Verification and Authentication

The principle of continuous verification and authentication is foundational to the Zero Trust security model, ensuring that all users and devices are constantly authenticated before granting access to sensitive systems or data (Akinleye & Adeyoyin, 2023). Traditional perimeter-based security systems often rely on a one-time verification during the initial login, which leaves systems vulnerable once access is granted. In contrast, Zero Trust models require ongoing authentication at every step of a user's interaction with the network (Lawal & Oduleye, 2023). This continuous process minimizes the risk of unauthorized access and internal breaches, making it essential for critical healthcare systems where patient data and medical devices must be protected from cyber threats (Osunkanmibi *et al*., 2025).

Continuous verification relies heavily on real-time monitoring and analytics to ensure that only authorized entities can access specific healthcare services (Seyi-Lande *et al*., 2023). By using advanced machine learning algorithms, organizations can evaluate user behavior patterns and flag any anomalies that deviate from predefined security protocols. For instance, machine learning-based behavioral analytics can be used to detect irregular logins or access attempts based on geographical locations or time patterns (Anichukwueze *et al*., 2024). Additionally, healthcare systems employing continuous verification benefit from multi-factor authentication (MFA) to further enhance security measures. As healthcare services increasingly shift toward digital platforms, the role of continuous authentication in safeguarding sensitive medical records and devices from external and internal cyberattacks is crucial (Michael & Ogunsola, 2023). Thus, incorporating continuous verification not only enhances the security architecture but also supports compliance with regulatory standards like HIPAA in the United States, ensuring patient confidentiality and data integrity (Rukh *et al*., 2024).

2.2 Least-Privilege Access Control

Least-privilege access control is a core principle of Zero Trust security models, which ensures that users and systems are only granted the minimal level of access required for them to perform their tasks (Akinlade, Filani, & Nwachukwu, 2025). This approach helps to reduce the attack surface in healthcare systems by limiting unnecessary exposure to sensitive data and critical systems (Oduro, 2024). By enforcing strict access policies based on user roles, healthcare organizations can ensure that only authorized personnel can access patient information, medical devices, and financial data, thus preventing insider threats and minimizing the potential for unauthorized access. This method is particularly essential in healthcare, where confidentiality and patient trust are of paramount importance (Adeyoyin *et al*., 2023).

In practice, implementing least-privilege access control in healthcare systems involves regularly auditing user access privileges and adjusting permissions based on the user's current role and tasks (Oziri, Arowogbadamu, & Seyi-Lande, 2023). Additionally, dynamic access controls can be set to ensure that when users move between different departments or roles, their access is reassessed and adjusted accordingly (Seyi-Lande, Arowogbadamu, & Oziri, 2023). Advanced AI-based systems are increasingly used to automate the detection of access policy violations, further enhancing the enforcement of least-privilege principles in real time (Ijiga *et al*., 2025) as seen in Table 1. Through the continuous refinement of access management and policy enforcement, healthcare organizations can maintain strong security while ensuring that only the necessary personnel have access to critical resources (Badmus & Olamide, 2025).

Table 1: Summary of Least-Privilege Access Control in Healthcare Systems

Key Principle	Description	Practical Implementation	Benefits
Minimal Access Granting	Users and systems are granted only the minimum level of access needed to perform their tasks.	Enforcing strict access policies based on roles and tasks to limit exposure to sensitive data and systems.	Reduces the attack surface by preventing unnecessary access to sensitive information, minimizing potential breaches.
Regular Audits and Access Reviews	Access privileges are periodically reviewed and adjusted based on user roles and tasks.	Continuous auditing of access controls and reassessment when users change departments or roles.	Ensures that users only retain the necessary permissions and reduces the risk of unauthorized access due to outdated roles.
Dynamic and Contextual Access Control	Access is granted dynamically based on the user's context, such as location, time, or task.	Implementing access policies that adjust in real time based on the user's changing context or department.	Improves security by ensuring access is only granted under appropriate conditions, thus reducing exposure to threats.
Automation with AI Integration	AI systems help detect violations of access policies and automate the enforcement of least-privilege principles in real-time.	Using AI to automate monitoring and enforcement of access controls, identifying unusual access patterns or violations.	Enhances efficiency in policy enforcement, improving real-time threat detection and reducing administrative workload.

2.3 Micro-Segmentation and Network Segregation

Micro-segmentation and network segregation are integral components of the Zero Trust model, offering a highly granular approach to securing healthcare networks by dividing them into smaller, isolated segments. This approach ensures that even if one part of the network is compromised, the attacker is unable to traverse other parts of the system (Oziri, Arowogbadamu, & Seyi-Lande, 2024). By isolating sensitive data such as patient records, medical devices, and financial transactions, healthcare organizations can limit the impact of potential breaches (Akinleye & Adeyoyin, 2025). Micro-segmentation relies on precise network zoning that prevents lateral movement between different sections of the network, ensuring that each segment is independently secured with its own set of security policies and access control measures (Ijiga *et al*., 2024).

In practical terms, this means implementing separate security layers for different types of devices, applications, and users within the healthcare network (Anichukwueze, Osuji, & Oguntegbe, 2024). For instance, medical devices may be isolated from administrative systems, allowing for tailored security protocols based on the nature of the device's function (Seyi-Lande, Arowogbadamu, & Oziri, 2024). Furthermore, micro-segmentation supports advanced threat detection mechanisms by creating isolated "zones" where potential threats can be quickly contained and analyzed without impacting other parts of the system (Bello *et al*., 2025). This significantly reduces the attack surface and ensures that any unauthorized access attempts are thwarted at the entry point, making it an essential strategy in safeguarding the integrity of healthcare infrastructure and ensuring compliance with regulatory standards (Badmus & Olamide, 2025).

3. Application of Zero Trust Security Models in Healthcare

3.1 Protecting Patient Data and Electronic Health Records (EHRs)

The protection of patient data and electronic health records (EHRs) is a critical component of healthcare security frameworks. As healthcare systems increasingly rely on digital tools and technologies, the need to safeguard sensitive information such as EHRs has never been more pressing (Aminu-Ibrahim *et al*., 2021). Traditional models of securing health data often focus on access control and encryption; however, the evolution of cyber threats necessitates the adoption of more advanced security frameworks like the Zero Trust Model (Anichukwueze *et al*., 2021). In the context of patient data protection, Zero Trust ensures that access to data is granted on the basis of strict verification, irrespective of the network location (Anioke & Atima, 2023).

One of the main challenges in safeguarding EHRs is the constant exchange of data across various platforms and devices. This exchange often opens the door to unauthorized

access if security measures are not robust enough (Awanye *et al*., 2023). Blockchain technology has been identified as a potential solution to this issue, offering a decentralized, immutable record-keeping system that enhances data integrity and auditability (Badmus & Olamide, 2023). Moreover, the integration of Artificial Intelligence (AI) and machine learning in healthcare security can further enhance threat detection and mitigation, ensuring timely responses to security breaches (Ijiga *et al*., 2023).

Thus, a multi-layered approach that combines traditional encryption techniques with emerging technologies such as blockchain and AI is essential for protecting patient data effectively. This comprehensive approach can help healthcare organizations meet the growing regulatory requirements for data privacy while improving patient trust (Michael & Ogunsola, 2023).

3.2 Securing Medical Devices and IoT in Healthcare

In healthcare, medical devices and the Internet of Things (IoT) are critical for advancing patient care and operational efficiency. However, the widespread deployment of IoT devices within healthcare systems presents unique security challenges, as these devices often lack robust security features. As IoT devices proliferate, they become targets for cyberattacks, and thus securing them becomes paramount to maintaining patient safety and data integrity (Aminu-Ibrahim & Ogbete, 2024). To address these vulnerabilities, Zero Trust Security models offer a promising solution by requiring continuous authentication and validation of each device before granting access to any healthcare network (Shah *et al*., 2025).

Securing medical devices and IoT networks requires a multi-faceted approach that includes secure network segmentation, device authentication, and real-time monitoring for abnormal behavior (Okafor *et al*., 2023). The integration of AI and machine learning can enhance these capabilities by enabling devices to detect and respond to security threats autonomously. Moreover, the use of blockchain technology can provide a tamper-proof ledger for device transactions, ensuring data integrity across the IoT ecosystem (Ekwunife *et al*., 2024).

In addition, healthcare organizations must ensure that IoT devices comply with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), as these frameworks outline specific requirements for securing medical devices and ensuring patient privacy (Osunkanmibi *et al*., 2025). As the healthcare industry continues to integrate more IoT devices, the Zero Trust model must evolve to address the growing complexity and number of interconnected devices, making it an essential framework for modern healthcare security (Efobi *et al*., 2023).

3.3 Integrating Zero Trust with Existing Healthcare Infrastructure

The integration of Zero Trust Security models into existing healthcare infrastructure is a significant step towards mitigating modern cybersecurity threats in the healthcare sector. Healthcare systems traditionally rely on perimeter security to protect patient data and medical devices. However, as remote work, cloud computing, and mobile health technologies expand, these traditional security measures become insufficient (Ijiga *et al*., 2023). Zero Trust, with its "never trust, always verify" philosophy, is designed to address these vulnerabilities by continuously validating user access, regardless of the network perimeter (Shah *et al*., 2025).

One of the primary challenges in adopting Zero Trust in healthcare is ensuring compatibility with existing legacy systems. Many healthcare facilities still rely on outdated IT infrastructure that may not support advanced security models like Zero Trust. Integrating Zero Trust requires a phased approach, where healthcare organizations begin by applying access controls to high-risk systems, such as EHRs and medical device networks, before expanding to other areas (Oparah *et al*., 2025). Furthermore, comprehensive training and awareness campaigns for healthcare staff are essential to ensure effective implementation (Okafor *et al*., 2023).

The integration of Zero Trust also necessitates the use of advanced technologies, such as AI and machine learning, to monitor and respond to potential threats in real time (Ijiga *et al*., 2023). The use of blockchain technology can further enhance the transparency and immutability of healthcare transactions, ensuring that data integrity is maintained across interconnected systems (Shah *et al*., 2025) as seen in Table 2. These technologies, when combined with a robust Zero Trust framework, can significantly enhance the security posture of healthcare organizations, enabling them to effectively protect sensitive patient data and comply with regulatory requirements.

Table 2: Summary of Integrating Zero Trust with Existing Healthcare Infrastructure

Aspect	Challenges	Solutions	Technologies Involved
Traditional Security Models	Perimeter-based security is insufficient for modern threats (remote work, cloud computing, mobile health).	Shift from perimeter security to continuous verification of user access, regardless of location.	Cloud Security, VPNs, Identity and Access Management (IAM).
Legacy Systems Integration	Many healthcare facilities use outdated IT infrastructure that may not support advanced security models.	Phased implementation, starting with high-risk systems like EHRs and medical devices.	Access Control, Legacy System Upgrades
Training and Awareness	Lack of understanding and skills among healthcare staff for new security protocols.	Comprehensive training programs and awareness campaigns for staff.	AI-driven Training Tools, Learning Management Systems
Advanced Technologies	Difficulty in monitoring and responding to threats in real time.	Use AI and machine learning for continuous monitoring and automated threat response.	AI, Machine Learning, Blockchain Technology

4. Cost Effectiveness of Zero Trust Models in Healthcare

4.1 Initial Setup and Implementation Costs

The initial setup and implementation of Zero Trust models in healthcare involve significant capital investment in infrastructure, technology integration, and staff training (Bello *et al*., 2025). Healthcare organizations adopting Zero Trust principles typically face upfront expenses related to

system overhaul, including the acquisition of secure hardware and software solutions, as well as the establishment of a robust identity and access management (IAM) system (Babatope, Akokodaripon, & Okoruwa, 2025). These implementations are crucial for ensuring comprehensive monitoring and constant authentication within healthcare networks. While the implementation of these solutions requires financial commitment, it also reduces the risk of costly data breaches and associated penalties (Bello *et al*., 2025).

Additionally, the implementation costs extend to integrating Zero Trust frameworks with existing infrastructure (Ogbete & Aminu-Ibrahim, 2025). The complexity of merging new security models with legacy systems in healthcare settings can drive up the initial setup costs. However, the long-term benefits of maintaining patient privacy and compliance with regulations such as HIPAA may justify the investment (Okafor, Dako, & Osuji, 2025). Organizations also need to ensure proper alignment of their IT systems and compliance processes with the Zero Trust architecture, which may involve upgrading or replacing outdated systems (Akin-Oluyomi *et al*., 2025).

Moreover, the training of IT personnel and healthcare professionals on new Zero Trust policies adds to the upfront costs. This training ensures that the organization can effectively manage security protocols and respond to potential security breaches (Lawal & Oduleye, 2025). These initial costs are necessary for building the foundation of a Zero Trust model, but they can be seen as a necessary investment for long-term cybersecurity resilience and the protection of patient data (Bello *et al*., 2025).

4.2 Long-Term Operational Savings

The implementation of Zero Trust security models in healthcare offers long-term operational savings, especially in reducing the incidence of costly data breaches and unauthorized access to sensitive health information (Lawal & Oduleye, 2025). By adopting continuous verification and enforcing the principle of least privilege access, organizations significantly minimize the risk of cybersecurity threats, leading to a reduction in the costs associated with breach recovery and legal fees (Ogbete & Aminu-Ibrahim, 2025). These long-term savings are particularly valuable in healthcare, where breaches can result in substantial financial penalties, reputational damage, and loss of trust from patients (Bello *et al*., 2025).

Furthermore, Zero Trust models reduce the need for large-scale infrastructure overhauls as they enhance the efficiency of existing systems. By integrating granular access controls and reducing network vulnerabilities, healthcare organizations can optimize their existing resources and reduce operational inefficiencies (Babatope *et al*., 2025). The automation provided by Zero Trust systems also minimizes the need for manual monitoring, thus reducing the labor costs associated with network security (Okafor, Dako, & Osuji, 2025). Healthcare providers can also streamline compliance with industry regulations, thus reducing the costs related to regulatory audits and compliance monitoring (Bello *et al*., 2025).

In addition, the proactive nature of Zero Trust security minimizes downtime during potential breaches, thus improving the overall operational productivity (Akin-Oluyomi *et al*., 2025). With a more secure and efficient system in place, healthcare organizations can allocate resources more effectively, investing savings into other critical areas, such as patient care and technological innovation (Lawal & Oduleye, 2025).

4.3 ROI and Risk Mitigation in Healthcare Settings

The return on investment (ROI) associated with Zero Trust security models in healthcare is evident when considering the reduction in data breaches and the associated financial implications (Bello *et al*., 2025). By focusing on a proactive approach that continuously monitors and authenticates users, healthcare organizations can significantly lower the frequency and severity of cyberattacks, which are often financially devastating (Babatope *et al*., 2025). The risk mitigation provided by Zero Trust models reduces the potential costs of non-compliance with data protection regulations, which can result in heavy fines and damage to the organization's reputation (Okafor *et al*., 2025). In the long term, this translates to a more secure and cost-effective operational framework for healthcare providers.

Moreover, the adoption of Zero Trust frameworks enhances organizational resilience by minimizing the attack surface through robust segmentation of the network and verification of user identity (Akin-Oluyomi *et al*., 2025). These security measures reduce the likelihood of unauthorized access and limit the damage caused by internal or external attacks (Bello *et al*., 2025). Healthcare organizations that implement these measures not only ensure the safety of patient data but also protect their intellectual property and sensitive organizational information (Ogbete & Aminu-Ibrahim, 2025). The long-term ROI from Zero Trust models, therefore, extends beyond cost savings to encompass enhanced organizational trust and improved patient care outcomes (Lawal & Oduleye, 2025).

Furthermore, the enhanced visibility and control over data flow provided by Zero Trust frameworks allow healthcare organizations to better manage their resources and compliance requirements (Okonkwo *et al*., 2025). These features contribute to long-term cost savings by enabling more informed decision-making processes and optimizing healthcare operations (Bello *et al*., 2025). Thus, the ROI is realized not just in direct financial savings but also in more efficient healthcare delivery and improved patient trust.

5. Challenges and Barriers in Implementing Zero Trust in Healthcare

5.1 Resistance to Change and Organizational Hurdles

One of the primary challenges in implementing Zero Trust security models (ZTSMs) in healthcare is resistance to change within healthcare organizations. Healthcare infrastructures, particularly hospitals, clinics, and pharmaceutical companies, are heavily reliant on legacy systems and processes that prioritize ease of access over rigorous security measures. This resistance stems from organizational inertia, where established practices are difficult to alter, especially when they have been functioning for years without major incidents (Aminu-Ibrahim *et al*., 2021). Many healthcare professionals may perceive the introduction of Zero Trust models as overly complicated or disruptive to their workflow, fearing that it could lead to increased operational friction (Okafor *et al*., 2023). These concerns are compounded by the resource-intensive nature of healthcare, where the focus is often on patient care rather than cybersecurity infrastructure.

Moreover, organizational hurdles often arise due to the entrenched corporate culture, which is not always geared toward cybersecurity innovation (Oparah *et al*., 2024). Hospital administrators and healthcare IT managers, for instance, may find it difficult to navigate the shift to a more segmented, access-controlled environment. Resistance is also fueled by concerns about staff training, the perception of Zero Trust as a "one-size-fits-all" solution, and the upfront investment required (Badmus & Olamide, 2023). Healthcare providers often face budgetary constraints, with funding allocated to direct patient care rather than cybersecurity enhancement. Furthermore, a lack of familiarity with Zero Trust concepts among healthcare decision-makers can result in hesitance towards its adoption, particularly in smaller, underfunded facilities (Lawal & Oduleye, 2022).

For these reasons, overcoming organizational resistance is crucial for successful Zero Trust implementation. Healthcare leaders must focus on cultivating a security-conscious organizational culture, where cybersecurity becomes a shared responsibility among all staff members (Osuji *et al*., 2024). Addressing concerns through comprehensive training and awareness programs, coupled with clear demonstrations of the long-term benefits of Zero Trust models, can alleviate resistance. More importantly, aligning security strategies with the healthcare facility's core mission of patient care can foster a more cooperative environment, where cybersecurity is viewed as an enabler rather than a hindrance (Ilesanmi *et al*., 2024).

5.2 Technical and Integration Challenges

Implementing Zero Trust Security Models in healthcare is fraught with technical and integration challenges. One of the primary obstacles is the need to integrate new security models with existing legacy systems that were not designed with Zero Trust principles in mind (Bello *et al*., 2025). Many healthcare organizations rely on outdated IT infrastructure, which lacks the flexibility to support the dynamic access control and continuous authentication mechanisms fundamental to Zero Trust (Oduro, 2024). The integration of these legacy systems with the advanced security protocols of Zero Trust often requires substantial customization, adding complexity and cost to the adoption process (Sanni & Attah, 2023).

Moreover, the complexity of healthcare operations, including the diverse array of connected medical devices, complicates the deployment of Zero Trust (Ogbete & Aminu-Ibrahim, 2024). Medical devices such as pacemakers, infusion pumps, and diagnostic imaging systems often have inherent security vulnerabilities due to their limited processing power and outdated software, making them difficult to integrate into a Zero Trust architecture (Akin-Oluyomi *et al*., 2025). Ensuring these devices comply with Zero Trust standards necessitates considerable upgrades to both hardware and software, which many healthcare facilities are ill-equipped to implement.

Additionally, managing user identity and access control across various departments, from clinical staff to administrative personnel, presents another technical hurdle (Akinleye & Adeyoyin, 2025). Healthcare workers need rapid, uninterrupted access to patient data for treatment, yet Zero Trust requires real-time monitoring of all interactions with sensitive information, which can slow down operations if not properly optimized (Badmus & Olamide, 2023). Therefore, healthcare organizations must carefully balance the need for stringent security with the necessity of providing seamless user experiences.

To address these challenges, healthcare organizations must invest in modernizing their IT infrastructure and embrace cloud-based security solutions that can scale with the growth of their systems (Ogbete *et al*., 2025). The integration of artificial intelligence and machine learning can also facilitate the continuous monitoring and adaptive response mechanisms required by Zero Trust models, thereby enhancing both security and operational efficiency (Oduro, 2024).

5.3 Overcoming High Initial Investment

One of the most significant hurdles healthcare organizations face when adopting Zero Trust Security Models (ZTSMs) is the high initial investment required for deployment. The upfront costs for implementing Zero Trust frameworks include not only the purchase of new security software and hardware but also the necessary workforce training, system integration, and ongoing maintenance. This can be particularly challenging for healthcare institutions, which often operate on tight budgets and must prioritize patient care over technological upgrades (Bello *et al*., 2025). The shift to a Zero Trust model involves a fundamental redesign of the organization's network architecture, moving away from traditional perimeter-based security to more granular, access-controlled environments (Ogbete & Aminu-Ibrahim, 2024). This transformation demands significant financial resources, which many healthcare facilities, especially smaller or rural providers, may find difficult to allocate.

In addition to financial considerations, healthcare organizations must also account for the cost of disrupting ongoing operations during the transition to a Zero Trust framework (Badmus & Olamide, 2024). The integration of new technologies, such as continuous monitoring and identity-based access management, may require downtime for system upgrades and staff reconfiguration. While this may be necessary to enhance security, it often results in temporary disruptions to critical services, which can undermine confidence in the security overhaul. This financial and operational burden makes the adoption of Zero Trust models seem more like an expenditure than a long-term investment (Ilesanmi *et al*., 2024). Moreover, the return on investment (ROI) from Zero Trust models is often realized over a longer period, which further discourages healthcare leaders from prioritizing security investments. To overcome this financial barrier, healthcare organizations must adopt a strategic approach, highlighting the long-term cost savings in reduced cyberattack risks, such as the potential savings from avoiding data breaches and their associated reputational damages (Oduro, 2024). Furthermore, demonstrating the benefits of Zero Trust in terms of compliance with increasingly stringent regulations, such as HIPAA, can provide the justification needed for the initial financial outlay.

6. Future Directions and Research Opportunities

6.1 Advancements in AI and Machine Learning for Zero Trust

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into Zero Trust security models has revolutionized how healthcare organizations monitor and enforce security protocols. These technologies enhance

continuous monitoring and real-time decision-making, making it possible to identify unusual patterns and potential threats faster and more accurately than traditional methods. AI-driven behavioral analytics are especially valuable in healthcare, as they enable systems to assess user behaviors continuously, ensuring that only legitimate users have access to sensitive information. For instance, machine learning models can predict potential breaches by analyzing historical data, such as login times, locations, and access patterns, and flagging anomalies that deviate from normal behaviors.

In addition, AI and ML can improve threat detection and response times by automating the classification of potential security risks. By leveraging predictive analytics, healthcare organizations can anticipate security threats before they fully materialize, reducing response times and preventing widespread damage. AI systems can also continuously learn from new data, which means they can adapt to emerging threats without human intervention. This ability to self-improve over time ensures that healthcare organizations maintain an up-to-date security posture, allowing them to stay one step ahead of increasingly sophisticated cyberattacks.

6.2 Scalability and Adaptability for Healthcare Organizations

Zero Trust models must be scalable and adaptable to meet the evolving needs of healthcare organizations. As these organizations grow and adopt new technologies, the security infrastructure must scale without sacrificing performance or security. Zero Trust architectures, by their very nature, are designed to scale seamlessly, allowing organizations to integrate new systems, applications, and users while maintaining a high level of security. This is particularly critical in healthcare, where the introduction of new medical devices, technologies, and even regulatory changes can quickly increase the complexity of the network.

Adaptability is equally important in ensuring that Zero Trust models can evolve in response to new challenges. As healthcare organizations increasingly migrate to cloud-based solutions and incorporate more remote workforces, the security architecture must be flexible enough to address the unique security requirements of each environment. Zero Trust models provide this flexibility by offering granular access controls and segmentation capabilities, ensuring that healthcare data remains secure regardless of where it resides. This adaptability allows healthcare organizations to implement security measures across diverse environments—whether on-premises, in the cloud, or in hybrid configurations—while ensuring a consistent level of protection.

6.3 Evolving Threat Landscape and Zero Trust Evolution

The evolving threat landscape in the healthcare sector presents a continual challenge to organizations seeking to maintain robust cybersecurity practices. With the increasing sophistication of cybercriminals, healthcare organizations must continuously adapt their security frameworks to counter new and emerging threats. Zero Trust security models are particularly well-suited for this task, as they are designed to evolve with the threat landscape by continuously verifying and validating access attempts. These models incorporate threat intelligence feeds and leverage machine learning algorithms to identify new attack vectors, allowing organizations to update their security policies in real-time.

Moreover, as the threat landscape becomes more complex, Zero Trust models are evolving to include more advanced security protocols, such as AI-driven threat hunting and automated incident response systems. These innovations enable organizations to proactively identify and mitigate threats before they can cause significant damage. Zero Trust architectures are also incorporating more dynamic, context-aware security measures that take into account not only the identity of the user but also the current environment, behavior, and potential vulnerabilities. This adaptability ensures that Zero Trust remains a relevant and effective defense strategy in the face of an ever-changing cybersecurity environment.

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.