Journal of Electrical and Electronic Engineering
2025, Vol. 13, No. 3, pp. 131-142
https://doi.org/10.11648/j.jeee.20251303.12

Research Article

Evaluating the Application of Zero Trust Architecture (ZTA) Implementation in Nigeria's Banking Industry

Adewale Ashogbon[1, *], **Oscar Ukpere**[2]

[1]Department of Computer and Information Sciences, Walker School of Business and Technology, Webster University, Missouri, United States

[2]Department of Cybersecurity, School of Management Science and Information Technology, American University, of St. Vincent and the Grenadines

Abstract

The growing number and sophistication of cyberattacks against financial institutions have underscored the need for a more robust cybersecurity framework in Nigeria's banking industry. This research examines the implementation of Zero Trust Architecture (ZTA), a contemporary security model that focuses on identity authentication, the principle of least privilege, and micro-segmentation to mitigate threats. The primary objectives were to assess the level of adoption of ZTA principles in Nigerian banks, identify the challenges associated with ZTA implementation, and evaluate the impact of ZTA on cybersecurity resilience and regulatory compliance. A quantitative research approach was employed, and structured questionnaires were used to gather data from IT and security professionals, banking personnel, and regulators. The collected data were analyzed using statistical techniques, such as SPSS, to generate descriptive statistics. The findings indicate a moderate level of implementation, with high adoption of identity verification practices but low adoption of more advanced practices, such as micro-segmentation and real-time authentication. Notable barriers include high implementation costs, difficulties integrating with legacy systems, and a shortage of cybersecurity professionals. However, despite these difficulties, it was found that ZTA had a positive impact on banks' ability to detect and address cyber threats, as well as enhance compliance with regulatory standards, such as the NDPR, PCI DSS, and SWIFT CSP. The research highlights the need to adopt a phased, strategic approach to ZTA integration, bolster regulatory support, and enhance capacity building. This research contributes to the growing body of knowledge in the field of cybersecurity in emerging economies, providing practical recommendations for policymakers and financial institutions.

Keywords

Zero Trust Architecture (ZTA), Cybersecurity, Banking Industry, Regulatory Compliance

1. Introduction

The banking sector has witnessed increased digitalization, and most financial institutions depend much on technology to offer services, store sensitive customer information, and conduct transactions [32]. Digital transformation, however, has also made banks a primary target for Cyber-attacks. In the global context, the list of organizations most often under

*Corresponding author: adewaleashogbon@webster.edu (Adewale Ashogbon)

Received: 22 May 2025; **Accepted:** 5 June 2025; **Published:** 23 June 2025

attack includes financial institutions, and the Nigerian banking industry is no exception [23]. Nigerian banks have been exposed to various cybersecurity threats over the past decade, including phishing, malware attacks, insider threats, and advanced ransomware attacks [5]. These threats have not only resulted in massive financial losses but also eroded customer confidence and raised questions about the robustness of the country's financial system. The traditional security model, which operates on the premise that there are no threats within the organization's network, has failed to contain modern cybersecurity threats [37]. This old guard perimeter-based model provides tacit trust when a user or system obtains access to the network, leaving it open to intrusions from within and lateral movement by bad actors [21]. With the growing threats of cyberattacks, there is an increasing consensus on the need for a more robust and evolving security framework to secure sensitive data and maintain operational continuity [35].

Zero Trust Architecture (ZTA) is one of the most popular cybersecurity paradigms developed to address these limitations [6]. Essentially, ZTA works based on the "never trust, always verify" paradigm. It assumes threats may come from within and outside the network, so it requires consistent authentication, least privilege management, micro-segmentation, and a tightened security policy [10]. ZTA shifts the focus from network boundary protection to resource protection, which is more suitable for the current complex and distributed IT environments. Recently, regulatory bodies, cybersecurity scholars, and international financial stakeholders have been gaining interest in ZTA as a tactical defense paradigm [20]. Although the relevance of ZTA has increased, the level of its adoption and implementation in the Nigerian banking field is underexplored. The banking sector in Nigeria is a vital part of the national economy, and its cybersecurity stance is far-reaching and crucial for maintaining financial stability and public trust [14]. However, few studies have investigated the adoption of Zero Trust principles in Nigeria due to the constraints banks face in the process and the overall effectiveness of the implementations [16]. It is expected that this research will inform banks on how to enhance their cybersecurity strategies, help policymakers create enabling cybersecurity regulations, and influence the development of cybersecurity theory in developing economies.

2. Literature Review

2.1. Overview of Zero Trust Architecture (ZTA) Principles

The Zero Trust Architecture (ZTA) is a cybersecurity approach that diverges from the previously accepted mentality of trusting those within the perimeter of a network. Avoiding the veiled trust, ZTA works on the assumption of "never trust, always verify" [22]. This strategy is, however, particularly significant in critical industries, such as the banking system, where confidential data and systems must be kept safe from all intrusion, both internal and external. Identity verification, the least privileged access, and micro-segmentation are key principles of Zero Trust Architecture (ZTA), which play a significant role in enhancing an organization's security.

1. Identity Verification: In ZTA, there is rigorous and constant identity examination. ZTA differs from traditional models, which validate users only upon entry and require identity verification for every access request, regardless of the location or device used. This entails multi-factor authentication (MFA), device posture checks, and real-time behavioral analytics [10]. As daily internet-assisted remote work and digital banking services continue to rise in Nigeria's banking industry, adequate identity verification safeguards are crucial to ensure that only verified and authorized users or devices are granted access to sensitive banking systems or information. Figure 1 shows the Identity Verification in Zero Trust Architecture.

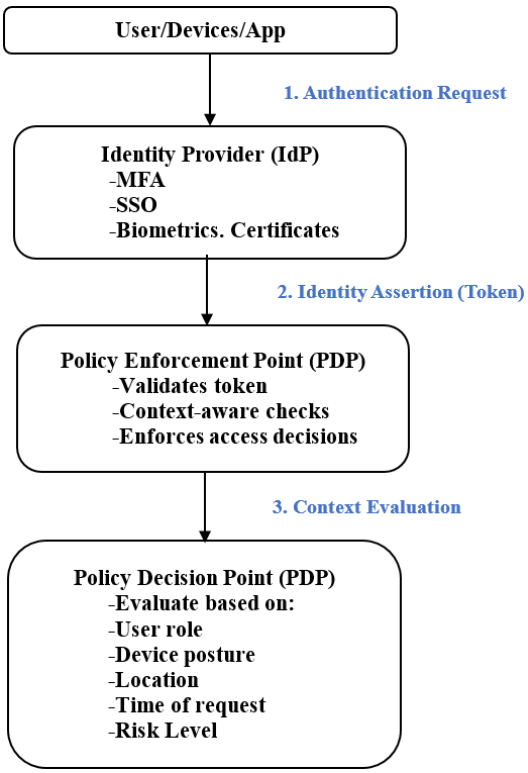

Figure 1. *Identity Verification in Zero Trust Architecture (ZTA).*

2. Least Privilege Access: The principle of least privilege imposes minimal levels of access to users and systems to perform their tasks. This curtails the attack surface and limits the potential damage in the event of a breach [13]. For banks, this may translate into segmenting employees' access to customer data, financial records, and administrative controls based on their roles and responsibilities. Integrating least privilege aids in the prevention of ex-

ternal threats, such as insider attacks and compromised credentials, and reinforces the necessity of stricter control over critical assets [1]. Figure 2 below shows the architecture of least privilege access.

Figure 2. *Least privilege access architecture [17].*

3. Micro-Segmentation: Micro-segmentation is the process of dividing a network into smaller, autonomous zones that isolate potential threats and prevent attackers' lateral movement. There are separate access policies and security controls in place for each segment. In banking settings, micro-segmentation, for instance, can isolate transactional processing systems, customer databases, and internal management systems, to the extent that if one of those were to be compromised, the rest would be safe [26] This is especially important in ensuring high value, targets like financial transaction systems and core banking infrastructure are secured. Incorporating these principles, ZTA provides a dynamic and resilient security framework that can adapt to the complex and evolving threats facing Nigeria's banking industry. Together, these principles emphasize an environment where trust is not presumed but repeatedly proven, access is highly regulated, and compromises are isolated quickly to avoid the spread [8]. Figure 3 below shows the Micro-Segmentation process for banks and financial sectors.

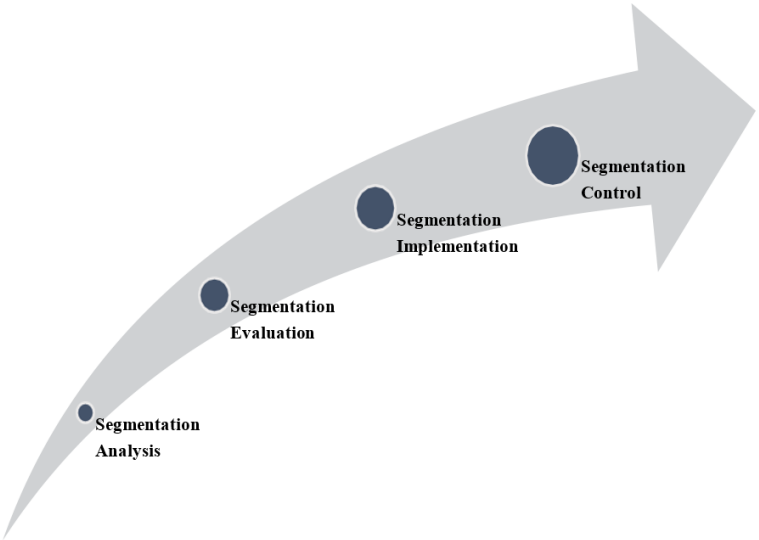

Figure 3. *Micro-Segmentation process for banks [12].*

4. Device Trust and Security Posture: In the Zero Trust model, the trustworthiness of a device is continuously measured before and during access. ZTA assesses the health of a device, compliance status, location, and security configurations to decide whether access should be granted [11]. In a country like Nigeria, where employees typically access banking systems from multiple endpoints, including corporate laptops and personal

smartphones, device compliance helps prevent intrusions through unsecured or compromised devices. Figure 4 below shows the architecture of Zero Trust Security.

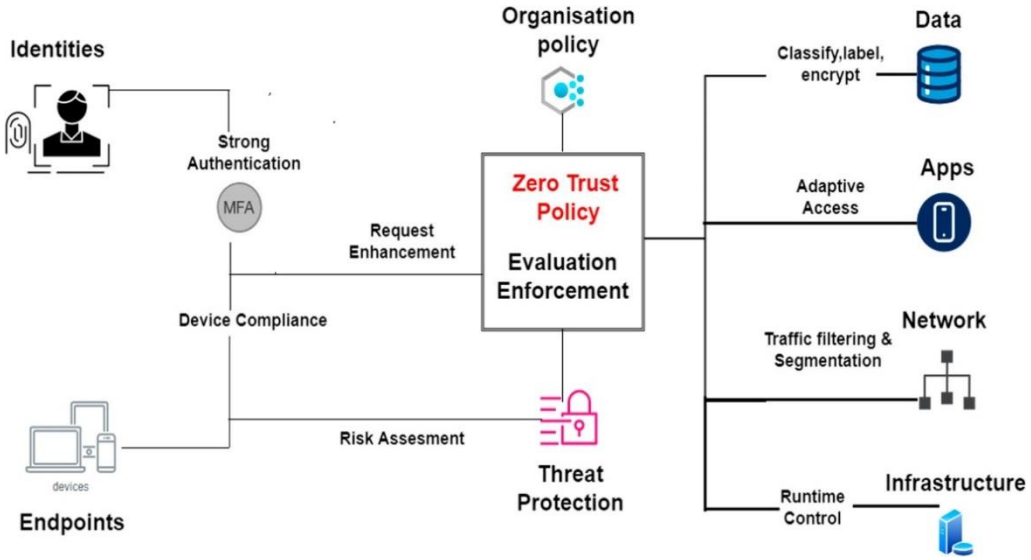

Figure 4. *Zero Trust Security Architecture [9].*

5. Continuous Monitoring and Risk Assessment: ZTA requires real-time visibility into network activity, user behavior, and system access patterns. Continuous monitoring enables the observation of anomalies, the detection of potential threats at an early stage, and the development of automated responses. This is critical in the cutthroat world of banking, where delays of even the smallest amount of time in threat detection can result in substantial financial losses [29]. Figure 5 below shows the Three-tiered banking management information of the system.

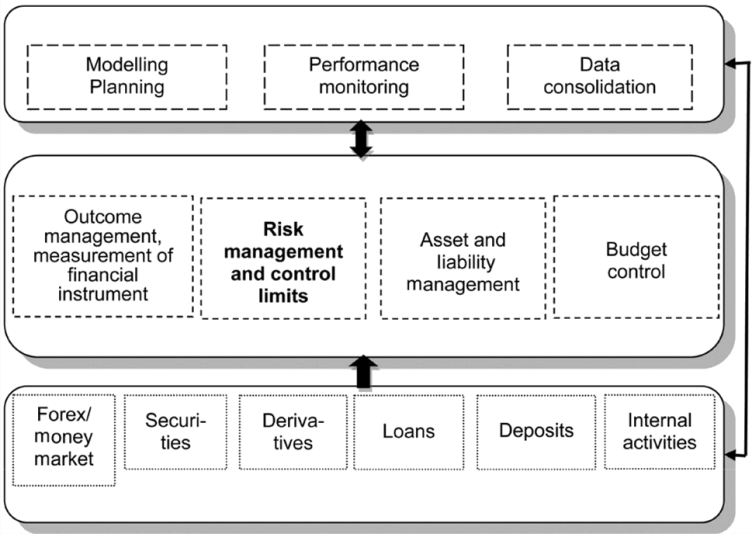

Figure 5. *Three-tiered banking management information [31].*

6. Policy-Based Access Control: In ZTA, access is controlled by dynamic policies that take into account multiple contextual aspects such as user role, time of access, device status, location, and behavior. These adaptive policies make access decisions dynamic rather than static, responding to dynamic risk conditions. This adaptability is critical in controlling access along the vast pool of banking workforce and clientele that Nigeria possesses [28]. The inclusion of these principles allows for a stronger and safer banking infrastructure. For Ni-

gerian banks operating in an environment characterized by digital transformation, regulatory oversight, and cyber threats, Zero Trust is a proactive, layered protection strategy [25]. Understanding and applying these principles effectively is crucial for mitigating risks, protecting customer assets, and maintaining public confidence in the financial system on a continuous basis. Figure 6 shows the Workflow of Policy-Based Access Control.

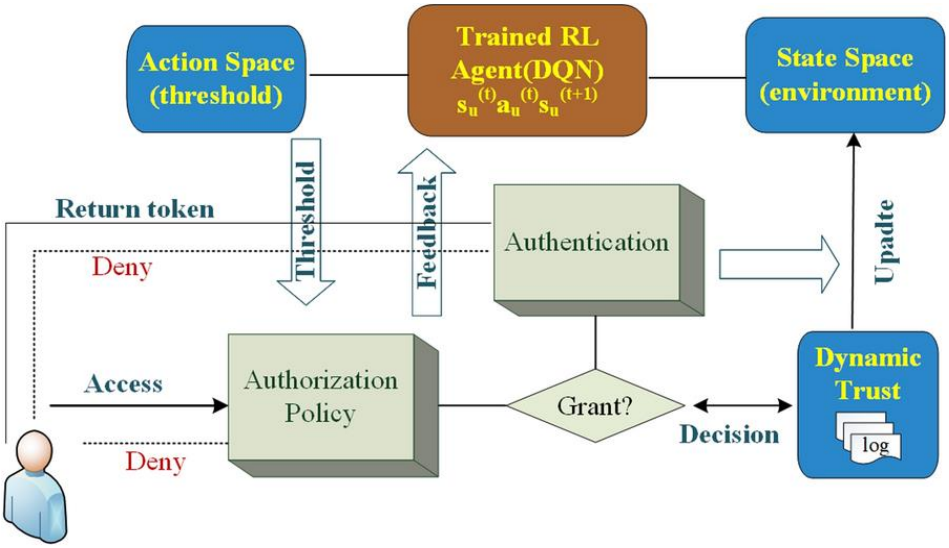

Figure 6. *Workflow of Policy-Based Access Control [36].*

2.2. Zero Trust Architecture (ZTA) in Global Banking

Zero Trust Architecture (ZTA) has gained significant popularity in the global banking industry, as financial institutions seek to enhance their cybersecurity against disruptive and persistent threats [38]. The implementation of ZTA principles, which include continuous verification, least privilege access, micro-segmentation, and policy-based controls, has been instrumental in transforming various banking scenarios into a secure environment [4]. In North America, the United States has been at the forefront of adopting ZTA frameworks in the financial sector. Well-known institutions, such as JPMorgan Chase and Goldman Sachs, have incorporated the two most important ZTA components: multi-factor authentication (MFA), network micro-segmentation, and continuous threat monitoring, to protect sensitive data and critical infrastructure [7]. These efforts are based on standards developed by the National Institute of Standards and Technology (NIST), where identity-centric security and robust access controls serve as the foundation of a Zero Trust model.

Canada has also made tremendous improvements. One of the Canadian banks, which focuses on commercial and residential loans, is considered successful in implementing the Zero Trust concept with the help of Privileged Access Management (PAM) tools, such as HashiCorp Vault and Boundary. Such implementation was effective in enhancing secret management, creating an environment of "trust nothing and authenticate everything," which significantly strengthened the institution's overall cybersecurity stance [24]. Turmoil in European financial markets has prompted financial institutions to turn to ZTA to comply with stringent data protection regulations and protect against the growing threat of cyberattacks. GDPR and other regional systems have spurred the adoption of identity-focused security systems, network segmentation, and risk-based authentication processes [18]. European banks have focused on safeguarding customers' data and ensuring their operations comply with privacy and compliance standards; the Zero Trust principles are a natural choice for their regulatory environment.

In the Asia-Pacific region, a significant difference exists in the adoption of ZTA. Advanced economies, such as Singapore, Japan, and Australia, are leading the ZTA integration with progressive cybersecurity policies and high digital maturity. Singapore's monetary authority (MAS) has provided extensive recommendations in favor of the use of zero-trust approaches, including the enforcement of the strictest identity verification and the establishment of the least privilege principle [27]. Australian banks have a robust system of endpoint protection, supplemented by local and national security structures, such as the Essential Eight and network segmentation. However, in various developing Southeast Asian countries, the pace of ZTA implementation remains slow due to limited resources, infrastructure issues, and a lesser concern about cybersecurity.

Awareness of ZTA is emerging in Africa. South African institutions and pan-African banks are beginning to imple-

ment Zero Trust models, often complementing them with Software-Defined Wide Area Networking (SD-WAN) technologies to enhance both connectivity and security. For example, the African Bank adopted the Zero Trust Access strategy, which combines SD-WAN technology with advanced security options, thereby increasing protection from threats and compliance with global standards, such as the Payment Card Industry Data Security Standard (PCI DSS) and the SWIFT Customer Security Program [15]. In Nigeria, which has one of the most dynamic financial sectors in Africa and is rapidly digitizing, the demand for sophisticated cybersecurity strategies has never been greater. The increased digitalization of platforms and online services by banks brings along escalating threats, including phishing, ransomware, data breaches, and insider attacks. The Central Bank of Nigeria (CBN) has responded to the increased cybersecurity guidelines and requirements, as well as the need to comply with standards such as the National Data Protection Regulation (NDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the SWIFT Customer Security Program (CSP) [19].

However, regulatory compliance is not enough to counter the changing threats and has led top Nigerian banks to seek ZTA as a more comprehensive and proactive security model. Despite a limited full-scale adoption of the ZTA in Nigeria, a few premier banks in the country have started adopting its main components. Companies such as Access Bank, GTBank, Zenith Bank, and UBA are implementing ZTA-supporting technologies like multi-factor authentication, role-based access control, endpoint detection and response systems, and cloud-native data encryption technologies. It is a process of gradually building up towards Zero Trust maturity, as evidenced by such developments. However, significant challenges remain. In Nigeria, most banks operate on legacy infrastructures that are not flexible enough to integrate zero-trust frameworks. High implementation costs, lack of ZTA-trained cybersecurity specialists, and the reluctance to organizational change still slow down the process [23, 33].

2.3. Cybersecurity Landscape in Nigeria

The cybersecurity landscape in Nigeria is continually evolving due to the ongoing digitization, the growth of the fintech sector, and a rising threat environment [12]. Since Nigeria is one of Africa's largest and most vibrant financial hubs, the banking sector in the country is strategically significant for the country's economy and, therefore, is an attractive target for cybercrime. The constant increase in the adoption of digital banking, mobile transactions, and cloud services has opened financial institutions to more diverse forms of cyber threats, requiring a rethink of traditional security practices [23]. The regulatory environment has embraced some level of development in recent years. The Central Bank of Nigeria (CBN) issues several guidelines on cybersecurity such as the Risk-Based Cybersecurity Framework and the Guidelines for Deposit Money Banks and Payment Service Providers (2021). This document requires financial institutions to ensure and reinforce appropriate cybersecurity governance, monitoring, and incident response plans [2]. Nigeria Data Protection Regulation (NDPR), a guideline regulated by the Nigeria Data Protection Bureau (NDPB), provides guidelines on customer data privacy. Regulators are also increasing pressure on compliance with global standards, such as the Payment Card Industry Data Security Standard (PCI DSS) and the SWIFT Customer Security Program (CSP).

Despite all these efforts, cyber-attacks remain an intractable and threatening problem. The banks in Nigeria have experienced numerous high-profile breaches, including phishing, ATM fraud, ransomware, and insider threats [30]. Nigerian financial institutions logged more than seventy thousand attempted fraud cases in 2023, and losses ran into 5B, according to a report by the Nigeria Inter-Bank Settlement System (NIBSS). A number of these attacks were successful because of a lack of internal controls. Nigerian banks are among the most technologically advanced in sub-Saharan Africa, offering numerous propositions that include robust mobile and internet banking services, API-driven services, and cloud integrations [25]. These developments, however, have occurred more rapidly than the corresponding development of cybersecurity capabilities. Many institutions continue to rely on perimeter-based defenses that are not well-equipped to handle the advanced tactics of modern threat actors, especially those targeting internal systems or leveraging compromised user credentials [34].

3. Methodology

This study employs a quantitative research approach to assess the utilization and effectiveness of Zero Trust Architecture (ZTA) in the Nigerian banking industry. The aim is to produce empirical data that reveals the level of ZTA awareness, adoption, and attendant challenges amongst key stakeholders in the financial sector. Quantitative methods are preferred because they can deliver measurable insights and objective facts that can be statistically analyzed to identify trends and correlations [3]. The data collection process was conducted using structured surveys designed to gather information on current cybersecurity practices, understanding, and the level of implementation of ZTA principles, as well as perceived benefits and barriers to adoption. The survey was structured using closed-ended responses with Likert scales, multiple-choice questions, and ranking options to provide consistency and comparability of responses. The survey was sent electronically to improve accessibility and coverage. The target population for sampling includes cybersecurity and IT experts in Nigerian commercial banks, as well as representatives from regulatory organizations such as the Central Bank of Nigeria (CBN) and the Nigeria Data Protection Bureau (NDPB). A purposive sampling approach was utilized to

recruit individuals with knowledge and experience in cybersecurity only. For data analysis, SPSS (Statistical Package for the Social Sciences) was used. Descriptive statistics like means, standard deviation, and percentages were used to summarize the data, and inferential statistical techniques such as analogous correlations and cross-tabulations were used to establish relationships among variables and make meaningful conclusions from the research.

4. Results

(1) Research Question 1

To what extent have Nigerian banks implemented the core principles of Zero Trust Architecture (ZTA), such as identity verification, least privilege access, and micro-segmentation?

Table 1. *Implementation of Core ZTA Principles in Nigerian Banks.*

S/N	Statement	Mean (x)	Standard Deviation (S. D)	Percentage (%)	Remark
1.	Identity verification mechanisms like MFA are actively used.	4.20	0.80	84%	High Implementation
2.	Least privilege access controls are enforced bank wide.	3.70	1.00	74%	Moderate Implementation
3.	Micro-segmentation is applied in network security architecture.	3.30	1.20	66%	Fair Implementation
4.	Real-time authentication and session validation are in use.	3.10	1.10	62%	Fair Implementation
5.	Policy-based access is regularly reviewed and updated.	3.50	0.95	70%	Moderate Implementation

Table 1 provides empirical values that assess the degree of adoption of core Zero Trust Architecture (ZTA) principles in Nigerian banks. The analysis has deployed five essential elements of ZTA identity verification: least privilege access, micro-segmentation, real-time authentication, and policy-based access reviews. These elements are analyzed using mean scores, standard deviation values, and percentages derived from survey responses. The most highly rated statement, "Identity verification mechanisms like MFA are actively used," has a mean score of 4.20 and a standard deviation of 0.8, indicating strong agreement among the respondents and a relatively consistent implementation among banks. That is, with an 84% implementation rate, this shows the maturity and priority accorded to identity-centric security within the Nigerian banking sector. This high score is likely due to pressure from regulations, increased phishing attacks, and the convenience of MFA deployment.

Unlike "Least privilege access controls are enforced bank-wide," which demonstrates an average implementation level of 3.70 and 74% compliance. Although this principle is the foundation of ZTA, its implementation is hindered by operational complexity and the need for highly detailed, role-based authorization policies that may not be consistently implemented across all banking units. Some more technical components, such as "Micro-segmentation is applied in network security architecture" and "Real-time authentication and session validation are in use," demonstrate a moderate approach to their inclusion, with scores of 3.30 and 3.10, respectively. The larger standard deviations (1.20 and 1.10) imply inconsistent application at the institutions, which may be because of technical complexities, the cost of deployment, and limitations of legacy infrastructure. The last indicator, "Policy-based access is regularly reviewed and updated," had a mean of 3.50 and an implementation rate of 70%, indicating moderate implementation. This implies that although many banks have established access policies, the rate of updates and their comprehensiveness may differ, which could detract from the continuity-verification ethos of ZTA. According to the overall result, the table indicates that Nigerian banks are in the early to intermediate stages of ZTA implementation, with identity verification being the most mature domain. However, moderate to fair scores for other principles reveal systemic issues — specifically in employing dynamic and granular controls, such as micro-segmentation and continuous authentication. As such, these findings highlight the need to invest more in cybersecurity infrastructures, personnel training, and policy enforcement to realize the full potential benefits of Zero Trust in protecting Nigeria's rapidly digitizing banking sector.

(2) Research Question 2

What are the key challenges and barriers affecting the adoption of ZTA in Nigeria's banking industry?

Table 2. Challenges and Barriers to ZTA Adoption in Nigerian Banks.

S/N	Statement	Mean (x)	Standard Deviation (S. D)	Percentage (%)	Remark
1.	Integration of ZTA with legacy systems is difficult.	4.30	0.75	86%	High Challenge
2.	High cost of implementation limits adoption.	4.10	0.90	82%	High Challenge
3.	Lack of skilled cybersecurity professionals hinders progress.	4.00	1.00	80%	High Challenge
4.	Organizational resistance to new security frameworks exists.	3.60	1.05	72%	Moderate Challenge
5.	Limited awareness of ZTA among decision-makers affects implementation.	3.40	1.15	68%	Moderate Challenge

Table 2 offers critical insights into the challenges faced by Nigerian banks in adopting Zero Trust Architecture (ZTA). The five statements represent significant technical, financial, human, and organizational barriers and were measured using respondents' perceptions through mean scores, standard deviations, and percentage ratings. These results reveal the systemic and strategic obstacles that hinder the large-scale implementation of ZTA in the Nigerian banking sector. The integration of ZTA with legacy systems is the most challenging identified aspect, with a mean of 4.30, a standard deviation of 0.75, and an implementation difficulty of 86%. This indicates a pervasive sentiment among respondents that aging IT infrastructures are incompatible with the granular control and visibility required by ZTA frameworks. The small standard deviation also shows a similar experience with this challenge across institutions. Right next to it is the high cost of implementation, with a mean score of 4.10 and 82%, which is another significant challenge. Advanced technologies, such as identity governance, network segmentation, and continuous monitoring, are essential for ZTA, all of which require substantial capital investment and ongoing operational costs.

This is a significant hurdle to medium-sized or resource-limited banks. Skilled cybersecurity professionals' shortage also became an important barrier (4.00) with a relatively higher standard deviation of (1.00), implying that despite the agreement on the severity of the skill gap across respondents, the gap may not be the same among institutions. It highlights Nigeria's overall lack of a ZTA-clued cybersecurity workforce, which affects implementation design, enforcement, and system maintenance. Organizational resistance and low awareness among decision-makers were both average challenges, with means of 3.60 and 3.40, respectively. Such issues indicate cultural and managerial inertia. A lack of understanding concerning the advantages and mechanics of ZTA can impede adoption or reduce implementation if security is not considered a strategic priority at the executive level. As revealed by the data, Nigerian banks have technical and organizational barriers on their path to adopting Zero Trust. Legacy infrastructure cost burdens and skills shortages are high-priority, national, and institutional-level challenges. At the same time, cultural and awareness gaps highlight the need for enhanced executive education, stakeholder engagement, and policy advocacy. To advance the phased implementation strategy, which will begin with awareness, pilot projects, and targeted investments, may aid in overcoming these barriers and boosting the maturity of ZTA in the sector.

(3) Research Question 3

How does the application of ZTA influence cybersecurity resilience and compliance with regulatory standards in Nigerian banks?

Table 3. Influence of ZTA on Cybersecurity Resilience and Regulatory Compliance.

S/N	Statement	Mean (x)	Standard Deviation (S. D)	Percentage (%)	Remark
1.	ZTA has improved our bank's ability to detect and respond to threats in real-time.	4.10	0.85	82%	High Impact
2.	Applying ZTA has strengthened compliance with standards like NDPR, PCI DSS, and SWIFT CSP.	3.90	0.90	78%	High Impact
3.	Adoption of ZTA has reduced incidents of unauthorized access or data breaches.	3.70	1.05	74%	Moderate Impact
4.	Zero Trust principles have enhanced internal audit and risk	3.50	1.10	70%	Moderate Impact

S/N	Statement	Mean (x)	Standard Deviation (S. D)	Percentage (%)	Remark
	management processes.				
5.	ZTA adoption has increased customer trust and confidence in digital banking platforms.	3.30	1.15	66%	Fair Impact

Table 3 presents the evaluation of the impact of Zero Trust Architecture (ZTA) on cybersecurity resilience and regulatory compliance in Nigerian banks. The responses from five central statements represent an overall optimistic viewpoint of ZTA's efficacy, the extent of influence being heavily dependent on the field. The conclusions are made on mean scores, standard deviations, percentage rates, and qualitative remarks. The best-rated statement is "ZTA has improved our bank's ability to detect and respond to threats in real-time" which has a mean of 4.10, a standard deviation of 0.85, and an 82% rating which means a high impact. This implies that ZTA's prolonged verification and monitoring processes increase threat detection capability greatly. The low standard deviation further explains a pattern of uniform experiences of the respondents suggesting the reliability of ZTA in managing real-time threats. Applying ZTA has made compliance with standards such as NDPR, PCI DSS and SWIFT CSP stronger scoring a mean of 3.90 and 78% as high impact. This represents the alignment between the principles of ZTA, for instance, access control, data protection, and activity monitoring, and compliance needs of national, as well as global regulatory platforms. ZTA clearly supplies an effective method of readiness for audits and risk mitigation.

The next two statements indicate moderate impact: "As a result of adoption of ZTA, there has been a decrease in cases of unauthorized access or data breach" (mean 3.70, 74%). "The adoption of ZTA has led to an enhanced internal audit and risk management process based on zero-trust principles" (mean 3.50, 70%). These scores indicate positive, yet not ideal impact, which is likely caused by partial implementation of ZTA, either due to different degrees of ZTA implementation or differentiated enforcement of policy within banking units. Variations in responses signaled by standard deviation greater than one indicates that, though some institutions are gaining a lot, others are yet to enjoy the maximum benefits. Finally, "ZTA adoption has increased customer trust and confidence in digital banking platforms" scored the least with a mean of 3.30, the standard deviation of 1.15, and 66% indicating average influence. This means that though ZTA can improve the back-end security its results are not sometimes observable or communicated well to final users. Customer trust in the security of the system can be affected more by public awareness and incident transparency rather than by the architecture. Overall, the results support the claim, which states that the impacts of ZTA on Nigerian banks are positive towards both cybersecurity resilience and compliance, especially on threat response and regulatory alignment. However, its overall organizational impact, particularly on such aspects as customer trust and audit procedures, is moderate to fair still, possibly because of a non-uniform implementation or lack of observability of effects originating from ZTA. Banks therefore need to concentrate on increasing the penetration level of ZTA, increasing stakeholder involvement and infusing user education to maximize the advantages of this architecture along both the technical as well as perceptual dimensions.

5. Discussion

The findings of this study give tangible insights into the level of challenges and implications of the implementation of Zero Trust Architecture (ZTA) in Nigeria's banking industry. The results indicate that levels of implementation of ZTA principles in banks are mixed, with relatively higher adoption of identity verification mechanisms like multi-factor authentication (MFA), moderate use of least privilege access, and policy-based access. However, state-of-the-art features such as micro-segmentation and real-time session validation show only a fair level of implementation. These findings are consistent with previous studies that were done in more digitally advanced banking systems around the world, where initial ZTA implementation also started with identity and access management, which then developed into more sophisticated architectures such as segmentation and continuous validation. For instance, the literature review indicates that full-fledged adoption of ZTA was phased up and gradual in North America and parts of Europe, where legacy infrastructure and cost limitations had initially slowed it—issues also reflected by Nigerian banks in this study. In the case of the barriers, the study confirms the central role of systemic and institutional constraints in entities' ZTA adoption. The most significant challenges, namely, challenges related to integrating with legacy systems, high costs of implementation and shortage of skilled cybersecurity professionals are in line with worldwide findings, including developing countries in Africa and in Southeast Asia. These barriers imply deficiencies in structure and strategy in the industry that inhibits practical application of ZTA in anything beyond surface-level practices.

The recorded resistance from the organization and low level of awareness of top-level makers enforce the need for cultural change and participation of the executives in cyber strategy. The perceived advantages of ZTA by respondents include increased threat detection, increased regulatory compliance, and decreased data breaches, which indicates the potential

benefits of the framework if duly adopted. While the impact on customer trust and confidence in digital banking was scored low, this may speak more to an absence of observable communication about ZTA measures than to the ineffectiveness of the framework. Literature favors this interpretation by pointing out that public awareness and user engagement are essential for the back-end security investment to convert into front-end consumer confidence. The policy and practice implications are crucial. For the banking institutions, the findings are a call to a definitive move towards proactive cyber security planning that gives preference to the long-term strategy of zero trust over short-term fix of patchwork. This involves investment in training, updating technologies, and cross-functional synergy among IT, compliance, and risk management groups. For regulators including the Central Bank of Nigeria (CBN), further targeted recommendations and incentives for ZTA adoption should be issued while depending on the existing standards, such as the Nigerian Data Protection Regulation (NDPR) and following international practices such as PCI DSS and SWIFT CSP. Nigerian banks have made notable efforts in embracing some of the ZTA principles, thus a coordinated effort with adequate resources is necessary to address constant barriers and realize the cybersecurity and compliance advantages of Zero Trust Architecture.

6. Conclusion

This study aimed to evaluate the use of Zero Trust Architecture (ZTA) in the Nigerian banking sector with particular emphasis laid on the degree to which the concept has been implemented, difficulties encountered, and the impact of ZTA on the resilience of cybersecurity, and regulatory compliance. Using quantitative research of IT/security professionals, staff members in the banking sector, and regulators, the study was able to reflect upon these objectives. The findings show that although Nigerian banks are embracing some of their core ZTA principles, including multi-factor authentication and least privilege access that involves identity verification, the adoption is partial with the more advanced components such as micro-segmentation and continuous authentication not well adopted. These revelations point to increasing and uneven maturity in the deployment of the Zero Trust within the industry. The study also established crucial barriers to complete ZTA adoption, which included difficulties in integrating legacy systems, high costs, lack of sufficient cybersecurity skills, as well as limitations in organizational structure to accommodate ZTA. Such challenges are in line with the global trends, especially in the developing economies, and provide the systemic and institutional barriers to overcome. The research revealed that implementation of ZTA positively influences banks' ability to discover threats, to comply with the requirements, and address the risks within the organization, but its contribution to customer trust is less significant probably because customers cannot see the improvements that happen in the background. This study highlights the significance of a strategy-based and staged approach to ZTA adoption in the banking industry of Nigeria. For the banks and regulators, these findings are a guide to formulate policy, promote capacity building and invest in the relevant infrastructure to strengthen the level of cybersecurity resilience in a digitizing financial ecosystem.

7. Recommendation

Based on the findings of this study, the following recommendations are proposed:

1) For Banks:

Banks should use a more rigid and gradual approach to ZTA implementation. This involves enhancing identity and access management with the help of multi-factor authentication and least privilege policies, as well as the gradual implementation of advanced controls such as micro-segmentation and real-time monitoring. Banks need to invest in modernizing their IT systems to support ZTA frameworks and disengage from obsolete legacy systems. Additionally, banks should prioritize staff training and upskilling to address the cybersecurity talent shortage while also fostering internal understanding and securing C-suite-level backing for the Zero Trust security model.

2) For Policymakers and Regulators:

Regulatory bodies, such as the Central Bank of Nigeria (CBN), should release specific guidelines recommending ZTA as part of the compulsory cybersecurity packages. They should also offer supportive mechanisms, such as financial incentives, technology grants, and policy frameworks, through which banks can facilitate a smooth transition to implementing Zero Trust Strategies. Additionally, the establishment of stakeholder engagement, as well as public-private partnership platforms and national-level cybersecurity awareness campaigns, can be easily deployed.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Abbas, A. (2024). Maximizing Security with the Policy of Least Privilege and Segregation of Duties in Organizations. Preprint. Retrieved from https://www.researchgate.net/publication/373834027_Maximizing_Security_with_the_Policy_of_Least_Privilege_and_Segregation_of_Duties_in_Organizations

[2] Abikoye, B. (2021). Cybersecurity in Digital Banking: Strategies for Risk Mitigation in Nigeria and Emerging Markets. Unpublished Manuscript. Retrieved from https://www.researchgate.net/publication/352880849_Cybersecurity_in_Digital_Banking_Strategies_for_Risk_Mitigation_in_Nigeria_and_Emerging_Markets

[3] Abuhamda, E., Ismail, I., & Bsharat, T. (2021). Understanding Quantitative and Qualitative Research Methods: A Theoretical Perspective for Young Researchers. International Journal of Research, 8(5), 71-87. Retrieved from https://doi.org/10.2501/ijmr-201-5-070

[4] Adamson, K., & Qureshi, A. (2025). Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA. Preprint. Retrieved from https://www.researchsquare.com/article/rs-6602547/v1

[5] Ama, G., Onwubiko, C., & Nwankwo, A. (2024). Cybersecurity Challenge in Nigeria Deposit Money Banks. Journal of Information Security, 15(4), 494-523. Retrieved from https://doi.org/10.4236/jis.2024.154028

[6] Atetedaye, J. (2024). Zero Trust Architecture in Enterprise Networks: Evaluating the Implementation and Effectiveness of Zero Trust Security Models in Corporate Environments. Dissertation. Retrieved from https://www.proquest.com/dissertations/zero-trust-architecture-in-enterprise-networks/docview/2622267924/se-2?accountid=13362

[7] Bhaskaran, D. (2025). Zero Trust Architecture: Securing America's Critical Infrastructure. International Journal of Advances in Engineering and Management, 7, 157-164. Retrieved from https://doi.org/10.35629/5252-0702157164

[8] Cadet, E., Osundare, O., Ekpobimi, H., Samira, Z., & Weldegeorgise, Y. (2024). Comprehensive Framework for Securing Financial Transactions through API Integration in Banking Systems. The International Journal of Computing and Cyber Security, 20(2), 662-672. Retrieved from https://doi.org/10.4018/IJCCS.202402.07

[9] Daah, C., Qureshi, A., Awan, I., Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. Electronics, 13, 865. Retrieved from https://doi.org/10.3390/electronics13050865

[10] Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. Journal of Cybersecurity and Privacy, 5(1), 2. Retrieved from https://doi.org/10.3390/jcp5010002

[11] Ejiofor, O., Olusoga, O., & Akinsola, A. (2025). Zero Trust Architecture: A Paradigm Shift in Network Security. Computer Science & IT Research Journal, 6(3), 104-124. Retrieved from https://doi.org/10.51594/csitrj.v6i3.1871

[12] Erkki, E., & Song, M. (2023). The Role of Cybersecurity in Nigeria's Digital Transformation Agenda. Working Paper. Retrieved from https://www.researchgate.net/publication/370852660_The_Role_of_Cybersecurity_in_Nigerias_Digital_Transformation_Agenda

[13] Farman, M. (2024). Implementing the Policy of Least Privilege: Enhancing Security through Segregation of Duties. Preprint. Retrieved from https://www.researchgate.net/publication/363582365_Implementing_the_Policy_of_Least_Privilege_Enhancing_Security_through_Segregation_of_Duties

[14] FATOKI, J. (2023). The Influence of Cyber Security on Financial Fraud in the Nigerian Banking Industry. International Journal of Science and Research Archive, 9(2), 503-515. Retrieved from https://doi.org/10.30574/ijsra.2023.9.2.0609

[15] Ghasemshirazi, S., Shirvani, G., & Alipour, M. (2023). Zero Trust: Applications, Challenges, and Opportunities. Preprint. Retrieved from https://arxiv.org/abs/2309.03582

[16] Gololo, I. (2018). Challenges of the Nigerian Banking Sector and the Way Forward. American Finance & Banking Review, 3(1), 26-34. Retrieved from https://doi.org/10.46281/amfbr.v3i1.216

[17] Ivan Lee (2025). Principle of Least Privilege (PoLP). Wallarm. Retrieved from https://www.wallarm.com/what/principle-of-least-privilege-polp

[18] Hassan, A., Ewuga, S., Abdul, A., Abrahams, T., Oladeinde, M., & Dawodu, S. (2024). Cybersecurity in Banking: A Global Perspective with a Focus on Nigerian Practices. Computer Science & IT Research Journal, 5(1), 41-59. Retrieved from https://doi.org/10.51594/csitrj.v5i1.701

[19] Hassan, E., Abdul, A., Abrahams, T., Oladeinde, M., & Dawodu, P. (2024). Cybersecurity in Banking: A Global Perspective with a Focus on Nigerian Practices. Computer Science & IT Research Journal, 5(1), 41-59. Retrieved from https://doi.org/10.51594/csitrj.v5i1.701

[20] Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. Preprint. Retrieved from https://arxiv.org/abs/2410.18291

[21] Jimmy, F. N. U. (2024). Zero Trust Security: Reimagining Cyber Defense for Modern Organizations. International Journal of Scientific Research and Management, 10(4), 887-905. Retrieved from https://doi.org/10.18535/ijsrm/v10i4.ec11

[22] Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. Entropy (Basel), 25(12), 1595. Retrieved from https://doi.org/10.3390/e25121595

[23] Kevin, C. (2025). Evaluating Cybersecurity Risks in Nigeria's Commercial Banking Sector: An Empirical Analysis. Research Gate. Retrieved from https://www.researchgate.net/publication/389217141_Evaluating_Cybersecurity_Risks_in_Nigeria's_Commercial_Banking_Sector_An_Empirical_Analysis/citation/download

[24] Koot, A. (2024). Introduction to Privileged Access Management. IDPro Body of Knowledge, 1, 1. Retrieved from https://doi.org/10.55621/idpro.101

[25] Lottu, O., Abdul, A., Daraojimba, D., Alabi, A., John-Ladega, A., & Daraojimba, C. (2023). Digital Transformation in Banking: A Review of Nigeria's Journey to Economic Prosperity. International Journal of Advanced Economics, 5(8), 215-238. Retrieved from https://doi.org/10.51594/ijae.v5i8.572

[26] Luz, A., John, O., & Akinyele, D. (2021). Network Segmentation and Micro-Segmentation within Virtual Device Contexts. Unpublished Manuscript. Retrieved from https://www.researchgate.net/publication/351493579_Network_Segmentation_and_Micro-Segmentation_within_Virtual_Device_Contexts

[27] Nasiruzzaman, M., Ali, M., Salam, I., & Miraz, D. (2025). The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation. IEEE Transactions on Dependable and Secure Computing, 12(2), 1-8. Retrieved from https://doi.org/10.1109/IT64745.2025.10930254

[28] Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment. Sensors, 25(2), 550. Retrieved from https://doi.org/10.3390/s25020550

[29] Ok, E., Williams, J., & Nicee, J. (2025). Understanding Zero Trust Architecture.. Retrieved from https://www.researchgate.net/publication/379446092_Understanding_Zero_Trust_Architecture

[30] Okafor, C., Onunka, O., Alabi, A., Obiki-Osafiele, A., Onunka, T., Daraojimba, C. (2023). Cybersecurity in U.S. and Nigeria Banking and Financial Institutions: Review and Assessing Risks and Economic Impacts. American International Journal of Management, 7(1), 54-62. Retrieved from https://doi.org/10.26480/aim.01.2023.54.62

[31] Okeke, I., Agu, E., Ejike, O., Ewim, C., & Komolafe, M. (2023). A Technological Model for Standardizing Digital Financial Services in Nigeria. International Journal of Frontline Research and Reviews, 1(4), 057-073. Retrieved from https://doi.org/10.56355/ijfrr.2023.1.4.0038

[32] Ranjan, R. (2024). The Evolution of Digital Banking: Impacts on Traditional Financial Institutions. International Journal of Progressive Research in Engineering Management and Science, 4(4), 753-763. Retrieved from https://doi.org/10.30499/IJPRES.2024.740455

[33] Raiter, O. (2021). Segmentation of Bank Consumers for Artificial Intelligence Marketing. International Journal of Contemporary Financial Issues, 1(1), 39–54.

[34] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), 13369. Retrieved from https://doi.org/10.3390/su151813369

[35] Salman, H., & Alsajri, A. (2023). The Evolution of Cybersecurity Threats and Strategies for Effective Protection: A Review. Shifra Journal, 9, 1-13. Retrieved from https://doi.org/10.70470/SHIFRA/2023/009

[36] Wang, R., Li, C., Zhang, K. et al. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity, 8, 12. Retrieved from https://doi.org/10.1186/s42400-024-00320-x

[37] Wells, A., Ajeigbe, K., & Stern, M. (2020). Security Trends in Networking: From Traditional Approaches to Zero Trust Architectures. Whitepaper. Retrieved from https://assets.equinix.com/content/PDF/marketing-collateral/Security-Trends-in-Networking-White-Paper.pdf

[38] Zareinia, K. (2022). Zero Trust Architecture: The Future of Secure Network Access. White Paper. Retrieved from https://info.nuage.com/rs/161-FHI-522/images/Zero_Trust_Architecture.pdf