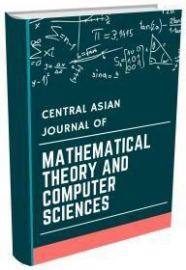

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

Article

Examining The Relationship Between IoT Device Authentication Protocols and Data Security in Nigerian Banks

Aburuotu, Emmanuel Chinwendu[1], Evaristus Chibuzor Nwoke[2], Eva Nwereka Obinna[3]

1,3 Department of Computer Science, Faculty of Natural and Applied Sciences, Ignatius Ajuru University of Education, Port Harcourt, Rivers State, Nigeria
2. Department of Computer Science, Faculty of Science and Computing, University of Agriculture and Environmental Sciences, Umuagwo, Imo State, Nigeria
* Correspondence: [1]emmanuel.aburuotu@iaue.edu.ng, [2]evaristus.nwoke@uaes.edu.ng, [3]eva.obinna@iaue.edu.ng

Citation: Chinwendunu A. E., Nwoke E. C., Obinna E. N. Examining The Relationship Between IoT Device Authentication Protocols and Data Security in Nigerian Banks. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 316-328.

Received: 16th Jan 2026
Revised: 24th Feb 2026
Accepted: 20th Mar 2026
Published: 26th Apr 2026

Abstract: This study examines the relationship between IoT device authentication protocols and data security in Nigerian banks. The increasing integration of Internet of Things (IoT) technologies in banking operations has improved service delivery but has also introduced significant cybersecurity challenges, particularly in relation to device authentication and protection of sensitive financial data. The study adopted a correlational survey research design and was conducted within the banking sector in Nigeria. The population comprised IT personnel, cybersecurity experts, and digital banking staff, from which a sample of 367 respondents was determined using the Taro Yamane formula. Data were collected using a structured questionnaire and analyzed using mean, standard deviation, and Pearson Product-Moment Correlation Coefficient. The findings revealed that IoT device authentication protocols such as multi-factor authentication, biometric systems, and cryptographic mechanisms are widely adopted in Nigerian banks. The study also found that the level of data security in IoT-enabled banking systems is relatively high, although concerns about data breaches persist. Furthermore, the results indicated a strong and statistically significant relationship between IoT authentication protocols and data security ($r = 0.642$, $p < 0.05$), suggesting that improvements in authentication mechanisms significantly enhance data protection. The study concludes that effective authentication protocols are critical to ensuring data security in IoT-driven banking environments. It recommends the strengthening of authentication systems, regular updates of security protocols, and stricter regulatory oversight by institutions such as the Central Bank of Nigeria to enhance cybersecurity resilience in Nigerian banks.

Keywords: Internet of Things, Authentication Protocols, Data Security, Banking Systems, Cybersecurity, Nigeria.

1. Introduction

The rapid evolution of digital banking systems has significantly transformed financial service delivery across the globe, with emerging economies such as Nigeria increasingly adopting advanced technologies to enhance operational efficiency, customer experience, and financial inclusion. Among these technologies, the Internet of Things (IoT) has gained prominence for enabling interconnected devices such as smart ATMs, biometric sensors, surveillance systems, and mobile banking endpoints to communicate and exchange data in real time. IoT integration in banking environments supports automation,

remote monitoring, and intelligent decision-making processes, thereby redefining traditional banking operations [1], [2].

Despite the operational advantages, the proliferation of IoT devices introduces complex security challenges, particularly in relation to device authentication and data protection. IoT ecosystems are inherently heterogeneous, consisting of devices with varying computational capabilities, communication protocols, and security standards. This diversity creates vulnerabilities that can be exploited by malicious actors if authentication mechanisms are weak or improperly implemented. Authentication protocols serve as the first line of defense by ensuring that only legitimate devices can access network resources and transmit sensitive financial data [3], [4].

In the context of banking systems, data security is of paramount importance due to the sensitive nature of financial information, including customer credentials, transaction records, and institutional data. Breaches in data security can lead to financial losses, reputational damage, regulatory sanctions, and erosion of customer trust. Nigerian banks, like many financial institutions in developing economies, are increasingly targeted by cyber threats due to the rapid expansion of digital infrastructure and the relatively uneven implementation of cybersecurity frameworks [5], [6]. As IoT devices become more embedded in banking operations, the risk surface expands, making robust authentication protocols essential for safeguarding data integrity, confidentiality, and availability.

Authentication protocols in IoT environments encompass various mechanisms, including password-based systems, biometric authentication, cryptographic key exchange, and multi-factor authentication schemes. Recent advancements emphasize lightweight authentication protocols designed specifically for resource-constrained IoT devices, ensuring both security and efficiency. However, the effectiveness of these protocols depends on their ability to resist common cyber threats such as replay attacks, man-in-the-middle attacks, and device spoofing [7], [8]. Inadequate authentication mechanisms can serve as entry points for unauthorized access, thereby compromising entire banking networks.

In Nigeria, the adoption of IoT in banking is closely linked to broader digital transformation initiatives driven by regulatory bodies such as the Central Bank of Nigeria, which promotes cashless policies and electronic payment systems. While these initiatives have improved financial accessibility and transaction efficiency, they have also increased the exposure of banking systems to cybersecurity risks. The integration of IoT devices without corresponding advancements in authentication protocols may lead to systemic vulnerabilities that undermine data security frameworks within the sector [9], [10].

Furthermore, existing studies have examined IoT security and banking cybersecurity independently, but there is a limited body of research that specifically investigates the relationship between IoT device authentication protocols and data security outcomes within the Nigerian banking context. Most prior research focuses on general cybersecurity practices or isolated authentication techniques without establishing empirical links between authentication robustness and data security performance indicators. This gap highlights the need for a comprehensive investigation into how authentication protocols influence data security in IoT-enabled banking environments.

Therefore, this study is situated within the growing need to understand the intersection of IoT authentication mechanisms and data security in Nigerian banks. By examining this relationship, the study aims to provide insights that will inform the development of more secure IoT frameworks, enhance cybersecurity strategies, and support the resilience of banking systems in an increasingly digital and interconnected financial landscape.

Statement of the Problem

The integration of Internet of Things (IoT) technologies into modern banking systems has introduced new dimensions of efficiency, automation, and real-time service delivery within the Nigerian financial sector. Devices such as smart ATMs, biometric verification systems, surveillance infrastructure, and mobile banking endpoints are increasingly interconnected, forming complex digital ecosystems. However, while these advancements have enhanced banking operations, they have simultaneously expanded the attack surface for cyber threats, particularly in relation to device authentication and data security [11], [12].

A critical concern lies in the authentication of IoT devices within banking networks. Many IoT devices are resource-constrained and may not support robust, computationally intensive security protocols, leading to the adoption of lightweight authentication mechanisms that may be vulnerable to sophisticated attacks. Weak or poorly implemented authentication protocols can allow unauthorized devices to gain access to banking systems, thereby compromising sensitive financial data. This creates opportunities for cyberattacks such as device spoofing, man-in-the-middle attacks, and unauthorized data interception, all of which pose serious risks to banking operations [13], [14].

In the Nigerian context, the situation is further complicated by the rapid pace of digital transformation driven by regulatory and market pressures. Institutions operating under the framework of the Central Bank of Nigeria have adopted various digital banking solutions to support cashless policies and financial inclusion. However, the implementation of IoT technologies has not always been matched with equally robust cybersecurity infrastructure. Reports of increasing cyber fraud and data breaches in Nigerian banks suggest gaps in existing security frameworks, particularly in the authentication and authorization of connected devices [15], [16].

Furthermore, although existing studies have explored cybersecurity challenges in banking and the general security issues associated with IoT systems, there is a notable lack of empirical research that directly examines how IoT device authentication protocols influence data security outcomes within Nigerian banks. Most studies tend to address these variables in isolation, without establishing a clear relationship between the strength or type of authentication protocols and the level of data protection achieved in practice. This disconnect limits the ability of stakeholders to make informed decisions regarding the design and implementation of secure IoT frameworks.

Consequently, the core problem this study addresses is the uncertainty surrounding the effectiveness of IoT device authentication protocols in ensuring data security within Nigerian banking environments. Without a clear understanding of this relationship, banks may continue to deploy IoT systems with inadequate security measures, thereby exposing critical financial data to persistent cyber threats. This study therefore seeks to bridge this gap by empirically examining the relationship between IoT device authentication protocols and data security in Nigerian banks.

Aim and Objectives of the Study

The aim of this study is to examine the relationship between IoT device authentication protocols and data security in Nigerian banks.

The specific objectives of the study are to:

1. Examine the types of IoT device authentication protocols adopted in Nigerian banks
2. Assess the level of data security in IoT-enabled banking systems in Nigeria
3. Determine the relationship between IoT device authentication protocols and data security in Nigerian banks

Research Questions

The study will be guided by the following research questions:

1. What types of IoT device authentication protocols are adopted in Nigerian banks?

2. What is the level of data security in IoT-enabled banking systems in Nigeria?
3. What is the relationship between IoT device authentication protocols and data security in Nigerian banks?

Research Hypotheses

The following null hypothesis will be tested in the study:

H_{01}: There is no significant relationship between IoT device authentication protocols and data security in Nigerian banks.

Literature Review

Concept of Internet of Things (IoT) in Banking

The Internet of Things (IoT) refers to a network of interconnected physical devices embedded with sensors, software, and communication capabilities that enable them to collect, exchange, and act on data without direct human intervention. In the banking sector, IoT represents a significant shift from traditional digital banking to an ecosystem of smart, responsive, and automated financial services. These devices include smart ATMs, biometric authentication systems, wearable banking devices, surveillance systems, and mobile-enabled endpoints that collectively enhance operational efficiency and customer experience [17], [18].

In modern banking environments, IoT enables real-time monitoring of transactions, predictive maintenance of infrastructure such as ATMs, and personalized financial services based on user behavior. For instance, IoT-enabled devices can track customer interactions and provide tailored financial recommendations, thereby improving service delivery and customer engagement. This technological integration aligns with global trends in digital transformation and financial inclusion, particularly in developing economies where access to traditional banking services may be limited [19], [20].

In Nigeria, the adoption of IoT in banking is closely tied to the expansion of digital payment systems and mobile banking platforms. Banks are increasingly deploying IoT-enabled infrastructure to support cashless transactions, remote banking, and automated service delivery. However, the rapid adoption of IoT technologies has outpaced the development of comprehensive security frameworks, raising concerns about system vulnerabilities and exposure to cyber threats [21], [22].

Despite its benefits, IoT in banking introduces complexities related to device interoperability, data management, and security. The heterogeneity of devices and communication protocols creates challenges in ensuring consistent security standards across the network. As a result, while IoT enhances banking efficiency, it simultaneously increases the potential for cyberattacks if not properly secured [23], [24].

IoT Device Authentication Protocols

Authentication protocols are fundamental components of IoT security architecture, designed to verify the identity of devices before granting access to network resources. In IoT-enabled banking systems, authentication ensures that only authorized devices can initiate transactions, access sensitive data, or communicate within the network. Without robust authentication mechanisms, IoT devices become vulnerable entry points for cybercriminals [25], [26].

Traditional authentication methods, such as password-based systems, are often inadequate in IoT environments due to their susceptibility to attacks and the limited computational capabilities of many IoT devices. Consequently, modern authentication protocols have evolved to include multi-factor authentication, cryptographic key exchange mechanisms, biometric verification, and certificate-based authentication systems. These approaches aim to enhance security while maintaining efficiency in resource-constrained environments [27], [28].

Lightweight authentication protocols have gained prominence in IoT systems because they are specifically designed to minimize computational overhead while

maintaining acceptable security standards. These protocols use techniques such as hash functions, symmetric key cryptography, and challenge-response mechanisms to authenticate devices efficiently. However, the trade-off between security strength and computational efficiency remains a critical concern, as overly simplified protocols may expose systems to vulnerabilities.

In banking applications, authentication protocols must also address advanced threats such as replay attacks, impersonation, and man-in-the-middle attacks. The effectiveness of these protocols depends on their ability to provide mutual authentication, session key establishment, and forward secrecy. Therefore, the selection and implementation of appropriate authentication protocols are crucial for maintaining secure IoT-enabled banking systems.

Data Security in Banking Systems

Data security in banking systems involves the protection of financial information from unauthorized access, disclosure, alteration, or destruction. It encompasses key principles such as confidentiality, integrity, and availability, which collectively ensure that sensitive banking data is secure and reliable. Given the high value of financial data, banking institutions are prime targets for cyberattacks, making data security a critical priority.

With the integration of IoT technologies, the volume, velocity, and variety of data generated within banking systems have increased significantly. This expansion introduces new vulnerabilities, as data is transmitted across multiple devices and networks, often in real time. Ensuring data security in such environments requires the implementation of robust encryption techniques, secure communication protocols, intrusion detection systems, and access control mechanisms.

In the Nigerian banking sector, data security challenges are exacerbated by factors such as evolving cyber threats, infrastructural limitations, and inconsistent implementation of cybersecurity policies. Incidents of cyber fraud, identity theft, and unauthorized transactions have highlighted weaknesses in existing security frameworks. Regulatory efforts by bodies such as the Central Bank of Nigeria aim to strengthen cybersecurity practices, but gaps remain in enforcement and technological capacity.

Moreover, data security is not solely a technical issue but also an organizational and human factor challenge. Poor security practices, lack of employee awareness, and inadequate risk management strategies can undermine even the most advanced technological safeguards. Therefore, a holistic approach to data security is required, integrating technical, organizational, and regulatory measures.

Relationship between Authentication Protocols and Data Security

Authentication protocols play a central role in ensuring data security within IoT-enabled banking systems, as they regulate access to network resources and prevent unauthorized interactions. A strong authentication mechanism serves as the first line of defense against cyber threats, directly influencing the confidentiality, integrity, and availability of data. When authentication protocols are robust, the likelihood of unauthorized access and data breaches is significantly reduced.

The relationship between authentication protocols and data security is particularly critical in IoT environments, where multiple devices interact dynamically within a network. Weak authentication protocols can allow malicious devices to infiltrate the system, leading to data interception, manipulation, or disruption. Conversely, well-designed authentication mechanisms can establish trust among devices, ensuring secure communication and data exchange.

Empirical studies have shown that the implementation of multi-factor and cryptographic-based authentication protocols enhances data security by reducing vulnerabilities associated with single-point authentication failures. These protocols

provide additional layers of security, making it more difficult for attackers to compromise systems. However, the effectiveness of these protocols depends on their proper implementation and integration within the overall security architecture.

In the context of Nigerian banks, the relationship between authentication protocols and data security is influenced by factors such as technological infrastructure, regulatory compliance, and institutional capacity. While banks are increasingly adopting advanced authentication mechanisms, inconsistencies in implementation and maintenance may limit their effectiveness. This underscores the need for a systematic evaluation of how authentication protocols impact data security outcomes within the sector.

Theoretical Framework

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) was developed by Fred Davis in 1989 as an extension of the Theory of Reasoned Action to explain and predict user acceptance of information systems. The model posits that two primary factors determine the adoption and usage of a technology: perceived usefulness and perceived ease of use. Perceived usefulness refers to the degree to which an individual believes that using a particular system will enhance their job performance, while perceived ease of use relates to the degree to which the user expects the system to be free of effort.

Over time, TAM has been widely applied in various domains, including banking, cybersecurity, and digital systems adoption, due to its simplicity and strong predictive power. In the context of banking technologies, TAM explains how employees and institutions decide to adopt new systems such as IoT-enabled devices and authentication protocols. When authentication mechanisms are perceived as useful in enhancing security and easy to implement or operate, banks are more likely to adopt and consistently utilize them. Conversely, complex or resource-intensive authentication protocols may face resistance, even if they offer higher levels of security.

In IoT-enabled banking environments, the relevance of TAM becomes particularly evident when considering the adoption of authentication protocols. Advanced authentication mechanisms such as multi-factor authentication, biometric verification, and cryptographic systems may significantly improve data security, but their adoption depends on how users and system administrators perceive their usability and effectiveness. If authentication protocols are perceived as cumbersome, slow, or difficult to integrate into existing banking infrastructure, institutions may resort to weaker alternatives, thereby compromising data security. This creates a direct link between technology acceptance and the effectiveness of security systems.

Furthermore, TAM highlights the importance of balancing security and usability in system design. In the Nigerian banking sector, where rapid digital transformation is occurring under the regulatory influence of the Central Bank of Nigeria, institutions must adopt authentication protocols that not only provide strong security but are also practical and scalable. The failure to achieve this balance may lead to poor implementation, user resistance, or outright circumvention of security measures, ultimately weakening data protection frameworks.

The application of TAM to this study is therefore grounded in its ability to explain how the perceived usefulness and ease of use of IoT authentication protocols influence their adoption and implementation, which in turn affects data security outcomes. By linking user acceptance of authentication technologies with their effectiveness in protecting banking data, TAM provides a suitable theoretical lens for examining the relationship between IoT device authentication protocols and data security in Nigerian banks.

Empirical Review

Das et al. conducted a study on secure authentication protocols for IoT-enabled environments with the aim of designing an efficient and lightweight authentication scheme suitable for resource-constrained devices. The study adopted an experimental design using simulated IoT networks and evaluated performance based on security strength and computational efficiency. The population consisted of IoT devices within a controlled network environment, and the researchers implemented cryptographic techniques such as hash functions and symmetric key encryption. Reliability was ensured through repeated simulation trials, and data were analyzed using performance metrics such as latency, throughput, and resistance to attacks. The findings revealed that robust authentication protocols significantly reduced vulnerabilities to replay and impersonation attacks. The study concluded that effective authentication mechanisms are essential for securing IoT systems. This study is relevant as it establishes the importance of authentication protocols in enhancing security, which aligns with the present study's focus on banking systems.

Zhang et al. examined various authentication protocols for IoT systems through a comprehensive survey-based empirical analysis. The study aimed to evaluate the strengths and weaknesses of existing authentication mechanisms in IoT environments. Using a comparative research design, the authors analyzed multiple authentication frameworks across different IoT architectures. The study population included previously published authentication models, and data were extracted from peer-reviewed sources. Analytical methods involved classification and performance benchmarking of protocols. The findings indicated that multi-factor and cryptographic-based authentication protocols offer higher security resilience compared to traditional methods. The study concluded that the selection of appropriate authentication protocols is critical for ensuring data security. This study relates to the present research by highlighting the direct link between authentication strength and system security.

Amin et al. conducted an empirical study on authentication mechanisms in wireless sensor networks, which are closely related to IoT systems. The aim was to develop a secure authentication scheme capable of preventing unauthorized access in networked environments. The study employed a simulation-based design, with a population consisting of sensor nodes in a network environment. Sampling involved selecting representative communication scenarios, while instrumentation included cryptographic algorithms and authentication models. Reliability was established through validation testing, and data were analyzed using computational cost and security performance indicators. The results showed that enhanced authentication protocols significantly improved data confidentiality and system integrity. The study concluded that authentication mechanisms are vital for maintaining secure communication in IoT-based systems. This supports the present study by reinforcing the role of authentication in safeguarding data security.

Wazid et al. investigated lightweight authentication protocols for IoT applications with the aim of balancing security and efficiency. The study adopted an experimental design using simulated IoT frameworks and evaluated protocols based on computational overhead and resistance to cyber threats. The population consisted of IoT devices with limited processing capabilities, and sampling focused on various authentication scenarios. The instrumentation included hash-based and key agreement protocols, while reliability was ensured through repeated testing. Data analysis involved measuring execution time, memory usage, and attack resistance. The findings revealed that lightweight authentication protocols can provide adequate security without significantly affecting system performance. The study concluded that efficient authentication mechanisms are essential for IoT environments. This is relevant to the present study as it addresses the practicality of implementing authentication protocols in banking systems.

Oladimeji et al. examined cybersecurity threats and data protection practices in Nigerian banks. The study aimed to assess the effectiveness of existing security frameworks in preventing cyber fraud and data breaches. A survey research design was adopted, with a population comprising banking staff and IT professionals in Nigeria. A sample was selected using purposive sampling, and data were collected using structured questionnaires. The instrument's reliability was confirmed using Cronbach's alpha, while data were analyzed using descriptive statistics and regression analysis. The findings indicated that inadequate authentication mechanisms and weak security controls contribute significantly to data breaches in Nigerian banks. The study concluded that strengthening authentication protocols is critical for improving data security. This study directly relates to the present research by providing empirical evidence within the Nigerian banking context.

Nwachukwu and Okeke conducted a study on digital transformation and cybersecurity resilience in Nigerian financial institutions. The aim was to evaluate how technological adoption influences cybersecurity performance. The study employed a correlational research design, with a population consisting of financial institutions in Nigeria. The sample included selected banks and fintech organizations, and data were collected using questionnaires and system audit reports. Reliability was established through internal consistency testing, and data were analyzed using Pearson correlation and regression techniques. The findings showed a significant relationship between the adoption of advanced security technologies, including authentication systems, and improved data security outcomes. The study concluded that effective implementation of authentication protocols enhances cybersecurity resilience. This study is relevant as it empirically supports the relationship between authentication mechanisms and data security, which is the core focus of the present study.

2. Materials and Methods

This study will adopt a correlational survey research design. The design is considered appropriate because it enables the researcher to examine the relationship between IoT device authentication protocols and data security in Nigerian banks without manipulating any variables. The correlational approach allows for the measurement of the degree and direction of association between the independent variable (IoT device authentication protocols) and the dependent variable (data security), making it suitable for achieving the objectives of the study.

The study will be conducted within the banking sector in Nigeria. The Nigerian banking sector comprises commercial banks, microfinance banks, and other financial institutions regulated by the Central Bank of Nigeria. The sector has experienced rapid digital transformation driven by the adoption of electronic banking, mobile platforms, and IoT-enabled systems. Major banking operations are concentrated in urban centers such as Lagos, Abuja, and Port Harcourt, where technological infrastructure and digital banking penetration are highest. The increasing deployment of IoT devices in these banks makes the sector suitable for investigating issues related to authentication protocols and data security.

The population of the study will comprise IT personnel, cybersecurity officers, and digital banking staff working in selected commercial banks in Nigeria. These categories of staff are directly involved in the implementation, management, and monitoring of IoT systems and data security frameworks within banking institutions. The estimated population is 8,000 staff drawn from major commercial banks operating across Nigeria.

A sample size of 367 respondents will be determined using the Taro Yamane formula for sample size determination at a 5% level of significance. A stratified random sampling technique will be employed to ensure adequate representation of different categories of

banking staff, including IT personnel, cybersecurity experts, and digital operations staff. Within each stratum, simple random sampling will be used to select respondents. This approach ensures that the sample reflects the diversity of roles involved in IoT implementation and data security management in Nigerian banks.

Data for the study will be collected using a structured questionnaire titled *IoT Authentication and Data Security Questionnaire (IADSQ)*. The instrument will be divided into sections:

Section A will capture demographic information of respondents, while Section B will assess IoT device authentication protocols, and Section C will measure data security indicators. The questionnaire will be structured on a four-point Likert scale of Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD). Items will be designed to capture respondents' perceptions of authentication protocol types, effectiveness, and their impact on data security components such as confidentiality, integrity, and availability.

The instrument will be subjected to face and content validity by the researcher's supervisor and two experts in cybersecurity and information systems. Their input will ensure that the items adequately measure the constructs of IoT authentication protocols and data security. To establish reliability, a pilot study will be conducted using 30 respondents from a bank outside the study sample. The data obtained will be analyzed using Cronbach's alpha coefficient to determine internal consistency. A reliability coefficient of 0.70 and above will be considered acceptable for the study.

Data will be collected through the administration of the questionnaire to selected respondents in the sampled banks. The researcher will employ both physical distribution and electronic means (such as email and online forms) to ensure a high response rate. Respondents will be given adequate time to complete the questionnaire, and follow-up measures will be taken to retrieve completed copies.

Data collected will be analyzed using both descriptive and inferential statistics. Descriptive statistics such as mean and standard deviation will be used to answer the research questions. For hypothesis testing, the Pearson Product-Moment Correlation Coefficient (PPMC) will be used to determine the relationship between IoT device authentication protocols and data security in Nigerian banks. All analyses will be conducted using the Statistical Package for the Social Sciences (SPSS), and hypotheses will be tested at a 0.05 level of significance.

3. Results

Analysis of IoT Authentication Protocols

Table 1. Analysis of IoT Device Authentication Protocols.

S/N	Item Description	SA	A	D	SD	Mean	SD
1	Multi-factor authentication is widely used in banking systems	180	110	40	20	3.29	0.88
2	Biometric authentication improves device security	190	100	35	25	3.30	0.91
3	Cryptographic protocols are implemented in IoT devices	170	120	40	20	3.26	0.89
4	Authentication protocols prevent unauthorized device access	200	90	40	20	3.34	0.92
5	IoT authentication systems are regularly updated	150	110	60	30	3.03	0.97

Grand Mean = 3.24 | Grand SD = 0.91

The results indicate a high level of adoption of IoT authentication protocols in Nigerian banks, with a grand mean of 3.24 above the criterion mean of 2.50. The highest-rated item was the ability of authentication protocols to prevent unauthorized access (Mean = 3.34), while the least-rated item related to regular system updates (Mean = 3.03). The relatively low standard deviations suggest consistency in responses, indicating general agreement among respondents regarding the presence and effectiveness of authentication protocols.

Analysis of Data Security Indicators

Table 2. Analysis of Data Security in Banking Systems.

S/N	Item Description	SA	A	D	SD	Mean	SD
1	Banking data is protected against unauthorized access	185	105	40	20	3.30	0.89
2	Encryption techniques are effectively implemented	175	115	40	20	3.28	0.90
3	Data integrity is maintained across IoT systems	165	120	45	20	3.23	0.92
4	Systems are available and resilient to cyber threats	160	125	45	20	3.21	0.93
5	Data breaches are minimal due to strong security measures	150	120	55	25	3.06	0.96

Grand Mean = 3.22 | Grand SD = 0.92

The findings reveal that data security in Nigerian banks is relatively high, with a grand mean of 3.22. Respondents strongly agreed that data is protected against unauthorized access (Mean = 3.30), while the perception of minimal data breaches recorded the lowest mean (3.06). This suggests that although security measures are in place, concerns about breaches still exist. The closeness of the standard deviation values indicates a stable pattern of responses.

Test of Hypotheses

H_{01}: There is no significant relationship between IoT device authentication protocols and data security in Nigerian banks.

Table 3. Pearson Correlation Analysis on IoT Device Authentication Protocols and Data Security.

		IoT Authentication Protocols	Data Security
IoT Authentication Protocols	Pearson correlation	1.000	0.642
	Sig. (2-tailed)	.	.000
	N	367	367
Data Security	Pearson correlation	0.642	1.000
	Sig. (2-tailed)	.000	.
	N	367	367

The result shows a strong positive correlation (r = 0.642) between IoT authentication protocols and data security. The p-value (0.000) is less than 0.05, indicating statistical significance. Therefore, the null hypothesis is rejected. This implies that improved authentication protocols are associated with higher levels of data security in Nigerian banks.

4. Discussion

The findings revealed that IoT device authentication protocols are widely adopted in Nigerian banks, with a high grand mean indicating strong agreement among respondents. Specifically, multi-factor authentication, biometric systems, and cryptographic mechanisms were identified as commonly implemented strategies for securing IoT-enabled banking systems. This suggests that Nigerian banks are not entirely asleep when it comes to security, at least at the level of adopting authentication mechanisms. The prominence of authentication protocols in preventing unauthorized access further reinforces their perceived importance within banking environments.

This finding aligns with the work of Das et al., who reported that robust authentication protocols significantly enhance system security by preventing unauthorized access and reducing vulnerabilities in IoT environments. Similarly, Wazid et al. emphasized that the adoption of lightweight yet effective authentication protocols is critical in resource-constrained IoT systems, ensuring both efficiency and protection. The current result also supports the position of Zhang et al., who found that advanced authentication mechanisms, particularly those involving cryptographic techniques, are essential for securing IoT infrastructures. However, the relatively lower mean score for regular system updates suggests that while authentication protocols are present, their continuous maintenance and upgrading may not be consistently prioritized. This gap could undermine the overall effectiveness of security systems, as noted by Kumari et al., who argued that outdated authentication schemes are highly susceptible to evolving cyber threats.

The findings showed that data security in Nigerian banks is relatively high, with respondents indicating that banking data is largely protected against unauthorized access and supported by encryption mechanisms. This suggests that banks have implemented foundational security measures to safeguard sensitive financial information. However, the lower rating for minimal data breaches indicates that despite these measures, security challenges persist, and breaches are not entirely eliminated. In other words, the locks are there, but someone somewhere still has a way in.

This observation is consistent with Akinwale and Kyari, who reported that although Nigerian banks have adopted various cybersecurity measures, incidents of cyber fraud and data breaches remain prevalent due to gaps in implementation and enforcement. Similarly, Oladimeji et al. found that weaknesses in authentication and access control systems contribute significantly to data security breaches in Nigerian financial institutions. The findings also support the broader argument by Conti et al. that the increasing complexity of IoT systems expands the attack surface, making it more difficult to achieve complete data security. Thus, while the overall level of data security appears satisfactory, it is not immune to vulnerabilities.

The test of Hypothesis One revealed a strong and statistically significant positive relationship between IoT device authentication protocols and data security in Nigerian banks ($r = 0.642$, $p < 0.05$). This indicates that improvements in authentication protocols are associated with corresponding increases in data security. In practical terms, better authentication means fewer opportunities for unauthorized access, which is exactly what one would hope in a banking system handling sensitive financial data.

This finding is in agreement with Amin et al. (2018), who demonstrated that enhanced authentication mechanisms significantly improve data confidentiality and integrity in networked systems. It also supports the findings of Nwachukwu and Okeke (2023), who reported a significant relationship between advanced security technologies and improved cybersecurity outcomes in Nigerian financial institutions. Furthermore, the result corroborates the conclusions of Sicari et al. (2018), who emphasized that authentication is a critical component of IoT security architecture and directly influences data protection. The strong correlation observed in this study reinforces the argument that

authentication protocols are not just technical add-ons but central determinants of data security performance.

Overall, the findings suggest that while Nigerian banks have made commendable progress in adopting IoT authentication protocols and implementing data security measures, the effectiveness of these systems is closely tied to the strength, consistency, and continuous improvement of authentication mechanisms. The relationship established in this study underscores the need for banks to prioritize robust and regularly updated authentication protocols as a core strategy for enhancing data security.

5. Conclusion

This study examined the relationship between IoT device authentication protocols and data security in Nigerian banks, with a focus on the adoption of authentication mechanisms, the level of data security, and the relationship between both variables. The findings revealed that Nigerian banks have largely adopted various IoT authentication protocols, including multi-factor, biometric, and cryptographic-based systems, indicating a growing awareness of the need for secure digital infrastructure.

The study further established that data security within IoT-enabled banking systems is relatively high, with strong measures in place to protect sensitive financial information. However, the persistence of data breaches and security concerns suggests that existing measures are not entirely sufficient, particularly in the area of continuous system updates and protocol maintenance.

Most importantly, the study found a strong and statistically significant relationship between IoT device authentication protocols and data security in Nigerian banks. This implies that the effectiveness of data security frameworks is heavily dependent on the strength, reliability, and proper implementation of authentication mechanisms. In essence, authentication protocols are not just supportive components but central pillars of data security in IoT-driven banking environments.

Recommendations

1. Nigerian banks should strengthen the implementation of advanced authentication protocols, particularly multi-factor and cryptographic-based systems, to enhance protection against unauthorized access and emerging cyber threats.
2. Banks should establish regular update and maintenance frameworks for IoT authentication systems to ensure that security protocols remain resilient against evolving vulnerabilities and attack techniques.

Regulatory bodies such as the Central Bank of Nigeria should enforce stricter cybersecurity compliance standards and provide continuous monitoring to ensure consistent and effective implementation of authentication protocols across the banking sector.

REFERENCES

[1] Y. O. Akinwale and A. K. Kyari, "Cybersecurity challenges in the Nigerian banking sector," *Journal of Financial Crime*, vol. 27, no. 3, pp. 835–850, 2020.

[2] I. Alhassan, D. Sammon, and M. Daly, "Data governance activities: An analysis of the literature," *Journal of Decision Systems*, vol. 29, no. 1, pp. 23–45, 2020.

[3] R. Amin *et al.*, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2017.

[5] R. Böhme and T. Moore, "The economics of cybersecurity," *Science*, vol. 338, no. 6108, pp. 646–651, 2012.

[6] M. Conti *et al.*, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.
[7] A. K. Das *et al.*, "Designing secure and efficient authentication protocol for IoT-enabled smart environments," *Future Generation Computer Systems*, vol. 92, pp. 565–580, 2019.
[8] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989.
[9] S. C. Eze, V. C. Chinedu-Eze, and A. O. Bello, "The adoption of digital banking in Nigeria: Issues and challenges," *Journal of African Business*, vol. 22, no. 4, pp. 560–577, 2021.
[10] M. S. Farash *et al.*, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor networks," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.
[11] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID systems," *Computers & Security*, vol. 55, pp. 271–280, 2016.
[12] J. Gubbi *et al.*, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
[13] W. H. Hassan, M. A. Habib, and S. Islam, "IoT applications in banking and financial services," *IEEE Access*, vol. 9, pp. 123456–123470, 2021.
[14] W. R. King and J. He, "A meta-analysis of the Technology Acceptance Model," *Information & Management*, vol. 43, no. 6, pp. 740–755, 2006.
[15] N. M. Kumar, P. K. Mallick, and S. Mishra, "The Internet of Things: Insights into applications and challenges," *Procedia Computer Science*, vol. 132, pp. 109–115, 2019.
[16] S. Kumari, M. K. Khan, and X. Li, "An improved authentication scheme for IoT environments," *Journal of Network and Computer Applications*, vol. 150, p. 102472, 2020.
[17] C. F. Lai, M. Chen, and K. Hwang, "Secure mobile cloud computing with authentication and data protection," *IEEE Systems Journal*, vol. 10, no. 1, pp. 1–10, 2016.
[18] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015.
[19] N. Marangunić and A. Granić, "Technology Acceptance Model: A literature review from 1986 to 2013," *Universal Access in the Information Society*, vol. 14, no. 1, pp. 81–95, 2015.
[20] C. C. Nwachukwu and T. C. Okeke, "Digital transformation and cybersecurity resilience in Nigerian financial institutions," *African Journal of Information Systems*, vol. 15, no. 2, pp. 45–63, 2023.
[21] T. T. Oladimeji, A. A. Adeyemi, and O. S. Ogunleye, "Cyber threats and financial fraud in Nigerian banks," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 1, pp. 23–41, 2022.
[22] S. Sicari *et al.*, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2018.
[23] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Harlow, U.K.: Pearson, 2018.
[24] V. Venkatesh and F. D. Davis, "A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies," *Management Science*, vol. 46, no. 2, pp. 186–204, 2000.
[25] R. Von Solms and J. Van Niekerk, "From information security to cybersecurity," *Computers & Security*, vol. 38, pp. 97–102, 2013.
[26] M. Wazid *et al.*, "Lightweight authentication protocols for IoT," *IEEE Access*, vol. 7, pp. 141–221, 2019.
[27] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 7th ed. Boston, MA, USA: Cengage Learning, 2021.
[28] Y. Zhang, R. H. Deng, and E. Bertino, "Secure authentication protocols for IoT: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1891–1920, 2020.