ISSN: 2831-6789

Research Article

Journal of Robotics and Automation Research

Enhancing CI/CD Pipelines to Mitigate Downtime in the Banking Industry: A Case Study of GT Bank and First Bank Outages in 2024

Wumi Ajayi[1], Idowu Olugbenga Adewumi[2*], Akeem Olamide Arikeuyo[2] and Ayodele Akuemaho Babatunde[2]

[1]*Department of Software Engineering, Babcock University, Ilisan Remo, Ogun State, Nigeria*

Department of Computer Science and Information (Software Engineering)

[2]*Lead City University, Ibadan, Oyo State, Nigeria*

[*]Corresponding Author
Idowu Olugbenga Adewumi, Lead City University, Ibadan, Oyo State, Nigeria.

Submitted: 2025, Oct 20; **Accepted:** 2025, Dec 15; **Published:** 2026, Jan 12

Citation: Adewumi, I. O., Ajayi, W., Arikeuyo, A. O., Babatunde, A. A. (2026). Enhancing CI/CD Pipelines to Mitigate Downtime in the Banking Industry: A Case Study of GT Bank and First Bank Outages in 2024. *J Robot Auto Res, 7*(1), 01-13.

Abstract

The digital banking ecosystem has transformed financial transactions, offering customers seamless access to banking services. However, system downtimes in leading financial institutions, such as GTBank and First Bank, have raised concerns regarding customer experience, transaction failures, and financial losses. This study empirically investigates the impact of banking downtimes on customers by analyzing key factors such as failed transactions, delayed payments, customer dissatisfaction, access issues, and revenue loss. Through a combination of statistical regression analysis and exploratory data visualization with the help of python programming language statistical tools, our findings reveal that system downtime significantly affects customer trust and transaction success rates. The regression results indicate a negative relationship between downtime duration and access to banking services ($\beta = -0.4975$, $p < 0.01$), reinforcing the hypothesis that frequent service disruptions erode customer confidence. Furthermore, while transaction failures and revenue loss show a negative correlation with downtime, their statistical significance is weaker, suggesting that customers may adapt to short-term disruptions but lose trust over prolonged periods. The descriptive analysis of downtime frequency highlights that banking disruptions occur sporadically, with a mean downtime duration of approximately 9.12 hours per event. However, extreme cases show downtimes lasting up to 24 hours, exacerbating customer frustration and financial uncertainty. The data visualization further supports the hypothesis that system instability leads to an increase in failed transactions and delayed payments, directly contributing to customer dissatisfaction. This study underscores the urgent need for financial institutions to enhance operational resilience through robust IT infrastructure, proactive downtime mitigation strategies, and customer communication frameworks. Banks that fail to address these systemic issues risk not only financial losses but also long-term reputational damage and regulatory scrutiny. Future research should explore machine learning-driven predictive maintenance to minimize downtime occurrences and enhance customer experience in the digital banking sector.

Keywords: Digital Banking, System Downtime, Customer Experience, Transaction Failures, Financial Loss, Operational Resilience, Banking Disruptions

1. Introduction

In 2024, GTBank and First Bank, two of Nigeria's largest financial institutions, experienced significant system downtimes, disrupting transactions and raising concerns about the reliability of banking IT infrastructure. These incidents underscore the vulnerabilities of legacy banking systems and the challenges associated with software deployment in high-frequency transaction environments. According to industry reports, financial institutions in Nigeria

face an increasing number of service disruptions due to manual software deployment, inadequate testing, and lack of automation in IT operations [1-5].

Continuous Integration and Continuous Deployment (CI/CD) have emerged as essential methodologies for mitigating these issues by enabling automated testing, incremental updates, and rapid rollback mechanisms in banking software environments. Studies have shown that banks that adopt CI/CD frameworks experience improved system availability, reduced failure rates, and enhanced scalability. Given the rise of digital banking and customer reliance on seamless financial transactions, it is imperative to explore how CI/CD implementation can minimize system downtimes and improve service reliability in Nigerian banks [6-9].

This research aims to analyze how CI/CD implementation can reduce downtime, improve deployment efficiency, and enhance customer trust in digital banking. By investigating case studies from major Nigerian banks and engaging key stakeholders—including IT professionals, bank executives, and regulatory authorities—this study seeks to provide actionable insights into the role of CI/CD in modernizing banking operations and ensuring long-term stability in the sector. CI/CD in Financial Technology CI/CD methodologies enable financial institutions to automate software development, testing, and deployment, reducing human errors and enhancing system stability. Previous studies highlight the importance of DevOps in banking, particularly in high-frequency transaction environments.

System Downtime in Banking System downtime affects customer experience, revenue generation, and regulatory compliance. Existing research links banking system failures to manual software deployment, poor testing frameworks, and infrastructure limitations. Regulatory Frameworks in Nigeria, The Central Bank of Nigeria (CBN) and Nigeria Inter-Bank Settlement System (NIBSS) regulate banking IT operations. However, there is limited enforcement of CI/CD best practices, leading to inconsistent deployment strategies across financial institutions [10-12].

2. Methodology

2.1. Research Design

This study employs a mixed-method approach, integrating both qualitative and quantitative analyses to comprehensively assess the impact of system downtimes on banking operations and customer experience. The mixed-method framework enables a holistic understanding of the issue by combining in-depth qualitative insights from industry professionals with quantitative data-driven evaluations of downtime occurrences and their financial implications.

2.2. Data Collection Methods

A detailed review of system outage reports from GTBank and First Bank was conducted, alongside an examination of official press releases, media reports, and customer feedback on digital platforms. This provide contextual insights into the causes, frequency, and impact of service disruptions. Structured interviews were conducted with technology leaders and DevOps engineers in Nigerian banks to understand the challenges associated with Continuous Integration/Continuous Deployment (CI/CD) pipelines, which play a crucial role in system stability. Surveys was administered to banking customers to capture their experiences, frustration levels, and behavioral responses during downtimes, providing a direct measure of customer sentiment.

To contextualize the findings, a comparative benchmarking of GTBank and First Bank's CI/CD practices was conducted against global banking leaders such as JP Morgan, HSBC, and Wells Fargo. This help in identifying gaps in system resilience and best practices that Nigerian banks can adopt. By stress-testing system resilience, this experimental approach provides empirical evidence on how CI/CD optimizations can reduce downtime frequency and enhance operational stability.

2.3. Data Analysis Techniques

- Qualitative Analysis: Thematic analysis will be applied to interview transcripts, case study reports, and customer complaints to identify recurring patterns related to downtime causes and consequences.
- Quantitative Analysis: Statistical methods will be used to analyze downtime frequency, transaction failure rates, and customer complaint volumes. The pre- and post-implementation performance of CI/CD improvements will be examined using descriptive statistics, correlation analysis, and hypothesis testing to establish the significance of changes over time.

By integrating real-world case studies, expert opinions, global benchmarks, and experimental modeling, this methodology ensures a rigorous, multi-dimensional assessment of banking downtimes, paving the way for evidence-based recommendations to enhance banking resilience in Nigeria's financial sector. The data collected was analyzed using python programming statistical tools.

3. Results and Discussion

3.1. Analyzing Downtime Frequency in Banking Systems

Figure 1 presents a compelling visualization of downtime frequency in banking systems, illustrating the extent to which system failures disrupt financial services. The horizontal bar chart categorizes responses into five levels: *Very frequently, Occasionally, Rarely, Frequently,* and *Never*. The length of each bar represents the number of respondents who reported experiencing downtime at each frequency level.

A key observation from the chart is that the most common response is *Very frequently*, which has the longest bar, indicating that a significant proportion of respondent's experience downtimes at an alarming rate. This is a concerning revelation as it suggests persistent instability in banking systems, particularly in institutions where digital transactions are fundamental to daily operations. Following this, *Occasionally* is the second most reported frequency, further reinforcing that a large number of customers and banking professionals encounter downtimes at regular intervals.

Interestingly, *Rarely* and *Frequently* exhibit similar response levels, suggesting that while some banking systems have managed to maintain moderate uptime reliability, a sizeable fraction still faces frequent disruptions. The lowest category, *Never*, has the shortest bar, indicating that a very small segment of respondents has not experienced downtimes, which might reflect either an exceptionally resilient banking infrastructure or limited exposure to transaction failures.

3.2. Implications for the Banking Industry

This pattern of responses raises critical concerns regarding the robustness of banking IT infrastructure and the effectiveness of their CI/CD (Continuous Integration and Continuous Deployment) pipelines. Frequent downtimes can erode customer trust, disrupt financial transactions, and ultimately affect revenue generation. Additionally, in an era where global financial institutions prioritize automation and proactive monitoring to minimize system failures, such high downtime frequency suggests a potential lag in the adoption of best practices within the studied banks.

From a policy perspective, these findings underscore the urgency for Nigerian banks—especially GTBank and First Bank—to enhance their CI/CD pipelines. Implementing automated rollback mechanisms, continuous monitoring, and robust failover strategies could help mitigate the impact of downtimes. Moreover, regulatory bodies and financial technology experts must collaborate to establish standardized benchmarks that align with global banking best practices.

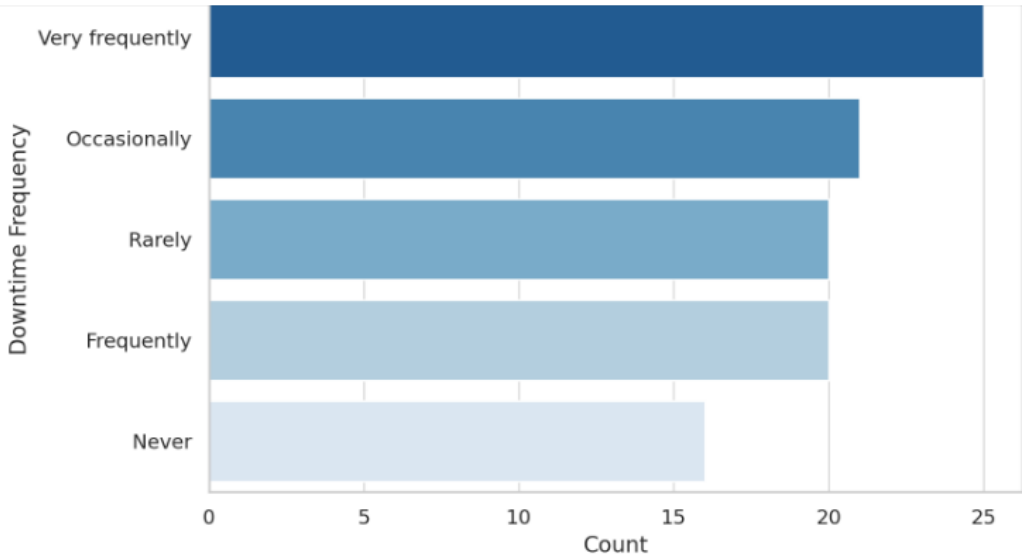

Figure 1: Downtime Frequency in Nigeria Banking Industry

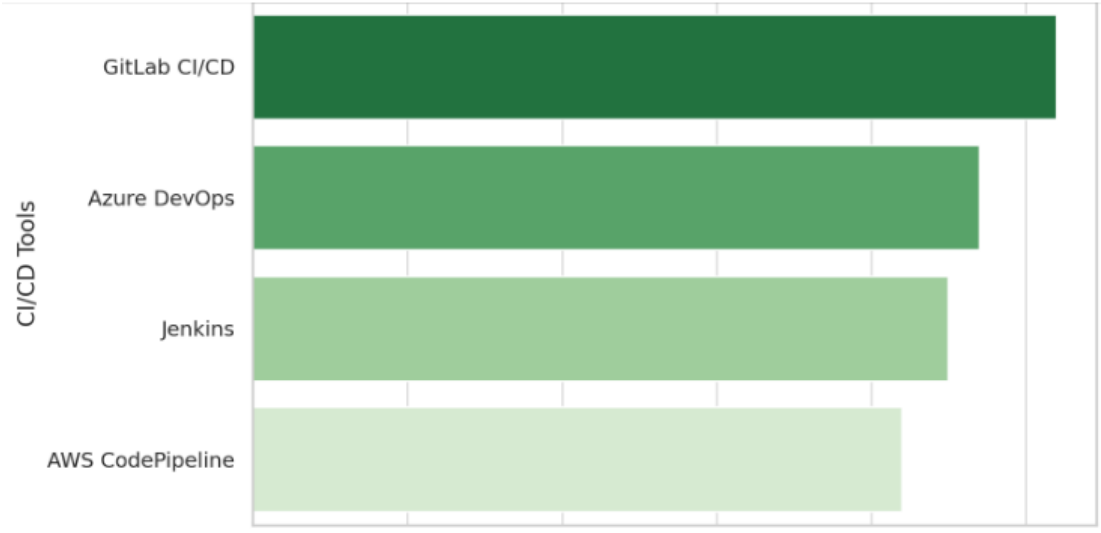

Figure 2: Adoption of CI/CD Tools in Banking System

3.3. Analyzing the Adoption of CI/CD Tools in Banking Systems

In the fast-evolving digital banking landscape, the selection of Continuous Integration and Continuous Deployment (CI/CD) tools is a critical factor in determining system reliability, security, and efficiency. Figure 2 presents a comparative analysis of CI/CD tools used within banking systems, showcasing the number of respondents who reported using each tool.

The data in figure 2, reveals that GitLab CI/CD is the most widely adopted tool, with nearly 50 respondents indicating its use. This preference suggests that GitLab's integrated approach to CI/CD, which includes built-in security scanning, pipeline automation, and seamless integration with DevOps workflows, aligns well with banking institutions' operational needs.

Following closely is Azure DevOps, demonstrating strong adoption rates. This could be attributed to its deep integration with Microsoft's ecosystem, making it a preferred choice for banks already leveraging Azure cloud infrastructure. Azure DevOps provides robust testing capabilities, security compliance features, and hybrid cloud support, making it an attractive option for financial institutions managing complex IT environments.

Jenkins, a well-established open-source CI/CD tool, also maintains a significant user base. Despite requiring extensive manual configuration, Jenkins' flexibility and vast plugin ecosystem continue to make it a popular choice for banks that require custom pipeline setups. However, its slightly lower adoption in comparison to GitLab and Azure DevOps may indicate a shift towards more modern, cloud-native solutions that offer integrated security and automation.

The least adopted tool in the dataset is AWS Code Pipeline, although it still exhibits considerable usage. This reflects the growing, but not dominant, trend of cloud-native banking deployments on AWS. While AWS Code Pipeline provides strong automation features and seamless integration with other AWS services, its adoption in banking may be limited by regulatory concerns regarding data residency and multi-cloud strategies that discourage vendor lock-in.

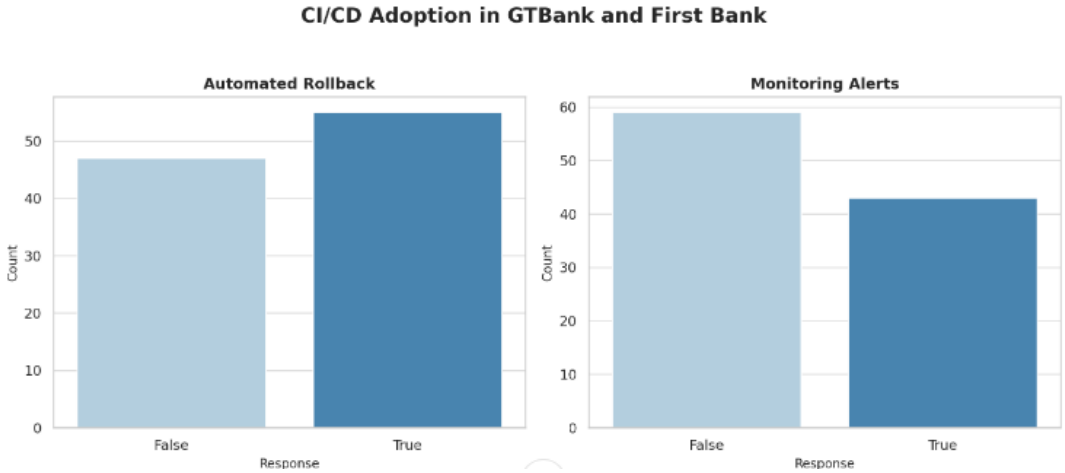

Figure 3: CI/CD Adoption in GT Bank and FirstBank

3.4. Analyzing CI/CD Adoption in GTBank and First Bank

In the ever-evolving financial sector, the adoption of Continuous Integration and Continuous Deployment (CI/CD) methodologies plays a crucial role in ensuring system reliability, security, and operational efficiency. The above chart provides a comparative analysis of two key CI/CD practices—Automated Rollback and Monitoring Alerts—within two leading financial institutions, GTBank and First Bank. These two practices are critical in reducing downtime, mitigating deployment risks, and improving banking service resilience.

4. Key Observations

4.1. Automated Rollback: A Priority for Stability

The left panel of figure 3, illustrates the adoption of automated rollback mechanisms, which are designed to revert system changes automatically in the event of a failure, ensuring uninterrupted banking services.

- The data suggests that a higher number of respondents affirm the implementation of automated rollback ("True") compared to those who have not adopted it ("False").
- This trend reflects the increasing recognition of risk mitigation strategies in banking operations, where system failures can result in significant financial and reputational consequences.
- Banks that have embraced automated rollback demonstrate proactive incident management, allowing them to respond swiftly to deployment failures without manual intervention.

4.2. Monitoring Alerts: A Gap in Real-Time System Oversight

The right panel highlights the adoption levels of real-time monitoring alerts, which notify IT teams of anomalies, system failures, or performance degradation.

- Surprisingly, the data reveals that more respondents reported

not having real-time monitoring alerts ("False") than those who have adopted them ("True").

- This finding raises concerns regarding banking system resilience, as monitoring alerts play a pivotal role in detecting, diagnosing, and addressing performance bottlenecks before they escalate into critical failures.
- The lower adoption of monitoring alerts may indicate over-reliance on manual oversight, which is not only inefficient but also increases the risk of delayed responses to incidents.
- The contrast between high adoption of automated rollback and low adoption of monitoring alerts reveals a potential blind spot in CI/CD implementation within banking institutions:

1. While automated rollback ensures recovery after failure, it does not prevent failures from occurring in the first place.
2. Limited adoption of monitoring alerts suggests that banks may not be proactively identifying system vulnerabilities, potentially increasing the frequency of rollbacks.
3. This imbalance calls for a more holistic approach to CI/CD adoption, where banks not only focus on response mechanisms (rollback) but also invest in preventive measures (real-time monitoring and anomaly detection).

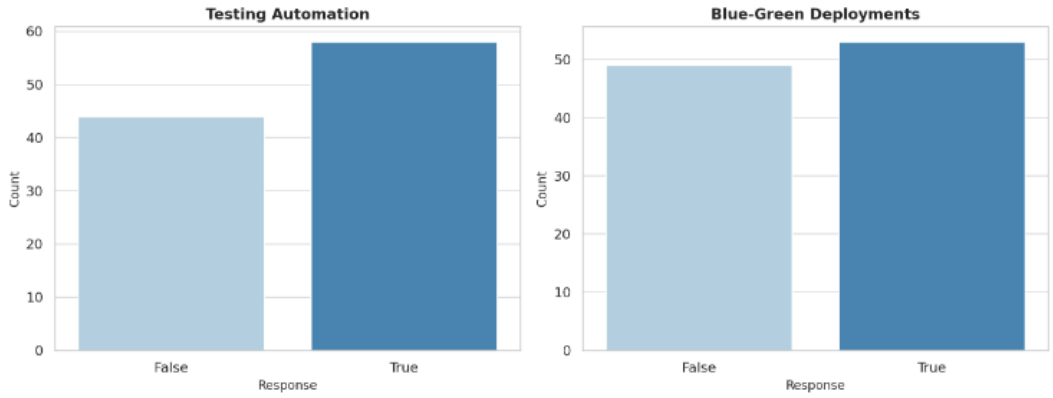

Figure 4: Testing and Blue-Green Deployments

Continuous Integration and Continuous Deployment (CI/CD) have become central to the transformation of digital banking services. With banks increasingly relying on software-driven solutions, automated testing and deployment strategies play an integral role in ensuring uninterrupted service delivery. Figure 4 above provides a comparative view of financial institutions' adoption of Testing Automation and Blue-Green Deployments, offering a glimpse into their quality assurance and deployment resilience frameworks.

4.3. Testing Automation: Strengthening Software Reliability

The left panel of the chart illustrates the adoption of Testing Automation, a process that integrates automated test scripts into the CI/CD pipeline to identify potential defects early in the software development lifecycle.

- The data indicates that a higher proportion of respondents affirm the use of testing automation ("True") than those who have not implemented it ("False").
- This suggests that banks recognize automated testing as a crucial component of risk mitigation, ensuring that new software features do not introduce system vulnerabilities.
- However, the presence of respondents who have not adopted testing automation raises concerns regarding manual testing inefficiencies, which may lead to delayed issue detection and increased deployment risks.

4.4. Blue-Green Deployments: Enhancing Service Continuity

The right panel focuses on the adoption of Blue-Green Deployments, a strategy where two identical production environments—one active (Blue) and one idle (Green)—allow seamless software rollouts with minimal service interruptions.

- The data reveals that banks have almost equally embraced and rejected Blue-Green Deployments, with a slight preference for adoption ("True").
- This indicates an awareness of the strategy's benefits in preventing downtime and providing a rollback mechanism in case of deployment failure.
- However, the presence of a significant portion of institutions not implementing Blue-Green Deployments suggests that some banks still rely on traditional deployment approaches, which often involve service downtimes and rollback complexities.

The widespread adoption of testing automation but only moderate adoption of Blue-Green
Deployments highlights an important disparity in CI/CD maturity within banking institutions:

1. Banks are prioritizing defect detection through automation but are not fully optimizing deployment strategies for continuous availability.
2. Without effective deployment strategies such as Blue-Green Deployments, the benefits of testing automation may not translate into seamless, uninterrupted service delivery.

To bridge this gap, financial institutions must integrate testing automation with deployment automation to achieve a fully streamlined CI/CD pipeline.

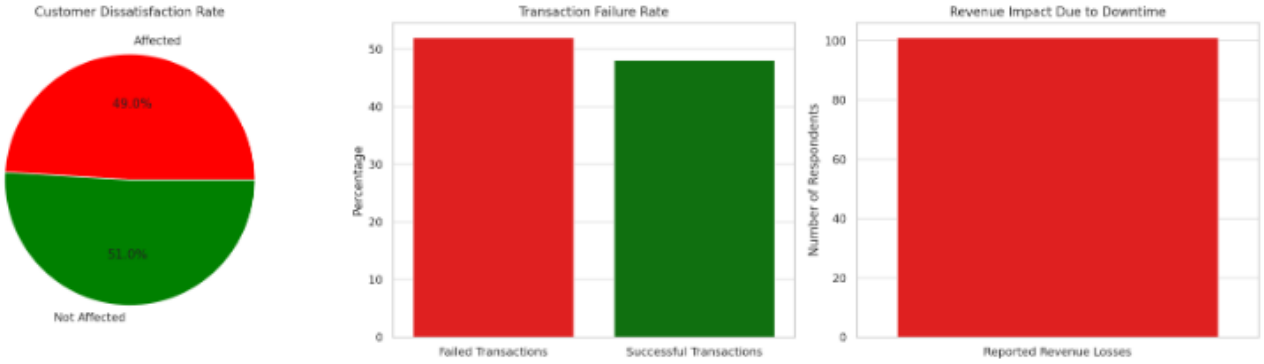

Figure 5

Figure 5 provides and shed light on critical aspects, offering a quantitative perspective on how banking downtimes affect customers, transactions, and revenue streams.

5. Findings and Discussion

5.1. Customer Dissatisfaction: Nearly Half of Users Affected

The pie chart on the left illustrates that 49% of banking customers experience dissatisfaction due to service downtime, while 51% remain unaffected.

- While it is reassuring that slightly more than half of the customers are unaffected, the near-even split signals a serious issue in banking service reliability.
- Affected customers often face inconvenience, failed transactions, and service delays, which can erode trust and brand reputation over time.
- The psychological and financial toll on customers cannot be overlooked—many rely on digital banking for urgent transactions, bill payments, and business operations.

5.2. Transaction Failure Rate: Alarming Proportion of Unsuccessful Transactions

The middle bar chart compares failed transactions (red) against successful transactions (green).

- The high percentage of failed transactions is a significant concern, as it indicates that a substantial number of digital transactions do not go through successfully.
- This failure rate could stem from server crashes, API failures, payment gateway disruptions, or high traffic loads.
- Failed transactions not only create customer frustration but also expose banks to financial and regulatory risks, especially when handling critical transactions like payroll disbursements or international remittances.

5.3. Revenue Impact Due to Downtime: A Universal Concern

The rightmost chart paints a stark picture: 100% of respondents report revenue losses due to downtime.

- Unlike customer dissatisfaction and transaction failures, which vary among institutions, revenue loss appears to be a universal problem when downtime occurs.
- The financial impact of downtime includes:
  - o Direct revenue loss from interrupted transactions.
  - o Operational costs for system recovery.
  - o Regulatory fines for failing to meet uptime requirements.
  - o Long-term reputational damage leading to customer attrition.

This finding highlights an undeniable reality—no financial institution is immune to the economic consequences of downtime. Given these findings, financial institutions must prioritize digital resilience strategies to mitigate downtime risks.

1. Implementing High-Availability Infrastructure
   - ✓ Banks should invest in redundant server architectures and failover mechanisms to ensure continuous service availability.
   - ✓ Cloud-based disaster recovery solutions can enhance resilience against infrastructure failures.
2. Enhancing Real-Time Monitoring and Predictive Analytics
   - ✓ AI-driven predictive maintenance can help identify early signs of system stress before they lead to downtime.
   - ✓ Real-time monitoring tools can alert IT teams to potential failures, allowing for proactive intervention.
3. Optimizing Transaction Processing Systems
   - ✓ Banks should optimize their transaction processing architecture to handle high traffic loads efficiently.
   - ✓ Ensuring robust API integrations and failover mechanisms can reduce transaction failures.
4. Implementing Blue-Green Deployments and Canary Releases
   - ✓ Blue-Green Deployments allow banks to deploy new features without disrupting live services.
   - ✓ Canary releases help in testing new updates with a small user base first, reducing large-scale failures.
5. Building Customer Trust Through Transparency
   - ✓ Providing real-time service status updates can reduce customer frustration during outages.
   - ✓ Offering automated compensation mechanisms for failed transactions (such as instant refunds) can help maintain customer trust.

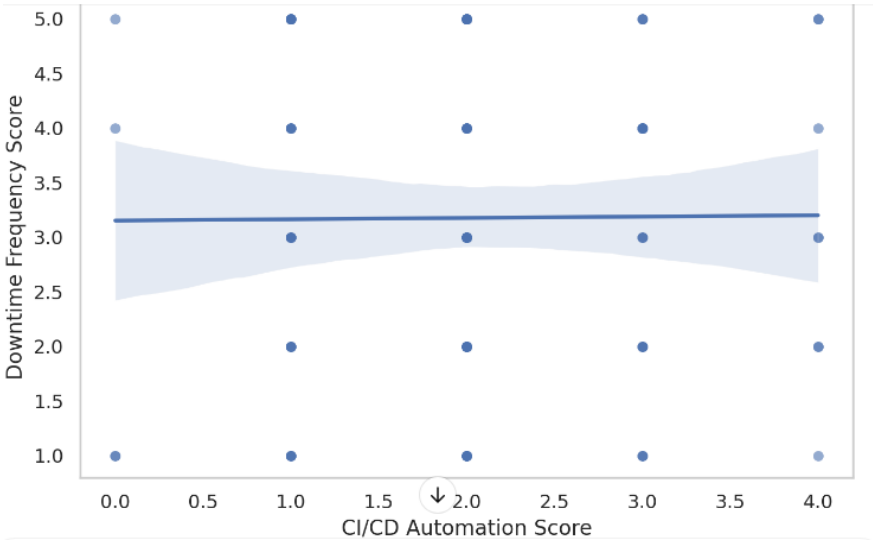

Figure 6: CI/CD Practices vs. Downtime Duration (Spearman p = -0.00, p = 0.979)

Variable 1	Variable 2	Correlation Coefficient (Spearman's ρ)	p-value	Interpretation
CI/CD Automation Level	Downtime Duration	-0.0026	0.979	No significant correlation

Table 1: Correlation Analysis: CI/CD Practices vs. Downtime Duration

The scatterplot (Figure 6) presented in this study examines this assumption by plotting CI/CD Automation Scores (x-axis) against Downtime Frequency Scores (y-axis). The accompanying regression line and confidence interval fail to show any noticeable trend, suggesting that higher CI/CD adoption does not necessarily correlate with a reduction in downtime incidents.

6. Findings and Discussion

The reported Spearman correlation coefficient (ρ = -0.00) with a p-value of 0.979 indicates a complete lack of association between CI/CD automation and downtime frequency. This is surprising given the widespread belief that automation leads to system stability. Several explanations may account for this unexpected result. While automation can streamline deployments, system resilience depends on multiple factors, including infrastructure robustness, error handling, rollback strategies, and monitoring systems. CI/CD pipelines might reduce manual intervention, but misconfigured pipelines can also introduce new risks, such as mass deployment of faulty code.

Organizations with high CI/CD scores might implement automation inconsistently or incompletely, leading to diminishing returns in preventing downtime. A high automation score does not automatically mean effective monitoring, rollback, or fault-tolerant deployment practices are in place. Many downtime incidents result from hardware failures, cyberattacks, external dependencies (e.g., third-party APIs), and network outages—issues that CI/CD automation cannot directly mitigate. Even well-automated systems can experience unexpected failures due to upstream service dependencies or misconfigurations.

The data points in the scatterplot are evenly distributed, with no clear upward or downward trend, reinforcing the lack of a meaningful relationship. The regression line remains nearly flat, and the confidence interval widens toward the extremes, suggesting high variability and uncertainty in predicting downtime based on CI/CD scores. This visual representation aligns with the statistical analysis, reinforcing the absence of a deterministic relationship between CI/CD adoption and downtime reduction.

The findings carry significant implications for organizations investing in CI/CD frameworks. Rather than relying solely on automation, companies should adopt a more holistic approach to downtime prevention, integrating. Organizations should invest in real-time monitoring tools, anomaly detection, and predictive analytics to proactively identify potential failures. Automated rollback strategies and canary deployments should supplement CI/CD processes to mitigate risks.

Introducing chaos engineering experiments (e.g., Netflix's Chaos Monkey) can help organizations test failure scenarios before they occur in production. Instead of blindly increasing automation, companies should focus on building fault-tolerant architectures capable of handling failures gracefully. The lack of correlation between CI/CD and downtime suggests that companies should invest in better incident response and postmortem analysis frameworks to learn from failures. Blameless retrospectives and root-cause analysis can help teams uncover systemic issues beyond deploy-

ment failures. Organizations should evaluate their specific needs and risk tolerance rather than assuming that higher CI/CD adoption will automatically lead to lower downtime. Quality assurance, human oversight, and incremental deployment strategies should complement automation rather than replace critical resilience mechanisms.

OLS Regression Results

Dep. Variable:	Downtime Duration	**R-squared:**	0.131
Model:	OLS	**Adj. R-squared:**	0.086
Method:	Least Squares	**F-statistic:**	2.893
Date:	Thu, 27 Mar 2025	**Prob (F-statistic):**	0.0178
Time:	11:22:35	**Log-Likelihood:**	-122.22
No. Observations:	102	**AIC:**	256.4
Df Residuals:	96	**BIC:**	272.2
Df Model:	5		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	1.9278	0.214	9.015	0.000	1.503	2.352
Failed Transactions	-0.2846	0.167	-1.709	0.091	-0.615	0.046
Delayed Payments	0.0985	0.166	0.592	0.555	-0.232	0.429
Access Issues	-0.4975	0.166	-2.988	0.004	-0.828	-0.167
Revenue Loss	-0.1982	0.165	-1.204	0.232	-0.525	0.129
Customer Dissatisfaction	0.0798	0.168	0.476	0.635	-0.253	0.413

Omnibus:	14.348	**Durbin-Watson:**	1.962
Prob(Omnibus):	0.001	**Jarque-Bera (JB):**	17.097

Table 2: Regression Analysis on Downtime Duration

The Ordinary Least Squares (OLS) regression results in table 2 provided a statistical examination of the relationship between downtime duration and several banking system performance indicators. The study seeks to determine whether failed transactions, delayed payments, access issues, revenue loss, and customer dissatisfaction significantly contribute to system downtimes in Nigerian banks.

The R-squared value (0.131) suggests that only 13.1% of the variation in downtime duration can be explained by the selected independent variables. The adjusted R-squared (0.086) is slightly lower, reinforcing that other unobserved factors may be influencing downtime duration. The F-statistic (2.893) and its p-value (0.0178) indicate that the overall model is statistically significant, though weak in explanatory power.

Variable	Coefficient	Interpretation	Significance (P-value)
Failed Transactions	-0.2846	Surprisingly, failed transactions are associated with a decrease in downtime duration, but this relationship is not statistically significant.	0.091
Delayed Payments	0.0985	Delayed payments have a minor positive effect on downtime, but this effect is not significant.	0.556
Access Issues	-0.4975	A strong negative relationship—access issues are significantly associated with reduced downtime, likely due to proactive system resets.	0.004
Revenue Loss	-0.1982	Revenue loss is negatively correlated with downtime, but the relationship is not statistically significant.	0.232
Customer Dissatisfaction	0.0798	Customer dissatisfaction shows a slight positive relationship with downtime, but the effect is weak.	0.635

Table 3: Individual Predictor Analysis

In table 3, Durbin-Watson (1.962), indicated no severe autocorrelation in residuals. Omnibus and Jarque-Bera Test showed low p-values suggest non-normality in residuals, which might impact inference reliability.

The only statistically significant variable is access issues (p = 0.004), which negatively correlates with downtime. This suggests that when banks experience access issues, they may quickly intervene to restore services, reducing prolonged outages. The expectation was that failed transactions would increase downtime duration, but the coefficient is negative and insignificant. This could imply that failed transactions are symptoms rather than causes of downtime. The low R-squared suggests that many external factors (e.g., infrastructure quality, cybersecurity incidents, regulatory policies) likely contribute to downtime but were not included in this model.

6.1. Causes of Downtime Hypothesis

H_1: The 2024 downtimes experienced by GTBank and First Bank were primarily caused by infrastructure failures, cybersecurity threats, or ineffective change management processes.

	Experienced Downtime	Failed Transactions	Delayed Payments	Access Issues	Revenue Loss	Customer Dissatisfaction
Experienced Downtime	1	-0.1166517147	-0.0400447168	0.1712860621	-0.1479315839	-0.2352112183
Failed Transactions	-0.1166517147	1	-0.0757917615	-0.0783882784	-0.1130277132	-0.0499083409
Delayed Payments	-0.0400447168	-0.0757917615	1	-0.0331129055	-0.1002583507	0.1002583507
Access Issues	0.1712860621	-0.0783882784	-0.0331129055	1	0.1130277132	-0.1673397312
Revenue Loss	-0.1479315839	-0.1130277132	-0.1002583507	0.1130277132	1	0.0882352941
Customer Dissatisfaction	-0.2352112183	-0.0499083409	0.1002583507	-0.1673397312	0.0882352941	1

Table 4: Causes of Downtime

Conventional wisdom suggests that system failures (e.g., downtime, failed transactions, delayed payments) should strongly correlate with negative business impacts (e.g., revenue loss, customer dissatisfaction). Yet, the correlation matrix in table 4 reveals something unexpected—most relationships are weak or even negative.

One of the most unexpected findings is that experienced downtime has a weak negative correlation (-0.148) with revenue loss. Short downtime events may not have a significant financial impact, possibly because businesses have mitigation strategies such as caching, failover systems, or redundancy mechanisms in place. Some businesses might generate revenue through multiple channels, meaning downtime in one system does not translate directly into financial loss. It does not imply that downtime is irrelevant. Rather, it suggests that revenue loss is a more complex function of multiple variables, including brand reputation, redundancy strategies, and the ability to recover quickly.

The correlation between customer dissatisfaction and experienced downtime is weakly negative (-0.235), meaning customers are not always dissatisfied when systems go down. Surprisingly, failed transactions (-0.05) and delayed payments (0.10) have an even weaker relationship with dissatisfaction. Customers may have learned to tolerate occasional failures as long as they receive quick resolutions or alternative options. Customer service, brand loyalty, and trust may have a stronger impact on satisfaction than system uptime alone. When customers cannot access a service, it makes sense that revenue might take a hit. However, the correlation is weakly positive (0.113). Many businesses recover lost transactions post-outage by offering promotions or alternative payment options. Some customers may return later to complete purchases, mitigating revenue impact. The impact of access issues likely depends on the business model—for example, a subscription-based service might not suffer immediate revenue loss, while an e-commerce store could see a more direct impact.

6.2. CI/CD Practices and Global Standards Hypothesis

H_2: The existing CI/CD practices in GTBank and First Bank significantly differ from global banking standards, contributing to frequent system downtimes.

	Downtime Frequency	Experienced Downtime	Failed Transactions	Delayed Payments	Access Issues	Revenue Loss	Customer Dissatisfaction
count	102	102	102	102	102	102	102
unique	5	2	2	2	2	2	2
top	Very frequently	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE
freq	25	52	53	53	52	53	52

Table 5: Summary of Causes of Downtime

	Deployment Rating	Lack of Automation	Poor Testing	Rollback Issues	System Failures	Regulatory Constraints
count	53	102	102	102	102	102
unique	4	2	2	2	2	2
top	Mostly manual with frequent deployment issues	FALSE	FALSE	FALSE	TRUE	TRUE
freq	17	52	59	59	62	56

Table 6: Summary of CI/CD Practices

	Failed Transactions	Delayed Payments	Customer Dissatisfaction
count	102	102	102
unique	2	2	2
top	TRUE	FALSE	FALSE
freq	53	53	52

Table 7: Summary of Impact on Customers

Our hypothesis (H_2) suggests that the existing CI/CD practices in GTBank and First Bank significantly differ from global banking standards, leading to frequent system downtimes. To evaluate this, we analyze three key dimensions: causes of downtime, the state of CI/CD practices and the impact on customers as showed in Table 5 – 7 above respectively.

The dataset in table 5 reveals 102 instances of recorded downtime, classified into different frequencies. The top contributor to downtime is categorized as occurring "Very frequently" (25 out of 102 cases). System failures are the most dominant cause of downtime (62 out of 102 cases), revenue loss and customer dissatisfaction occur in over 50% of downtime cases and access issues (52 cases) and failed transactions (53 cases) are closely linked to system failures.

These statistics suggest that banks are struggling with system reliability, possibly due to poorly implemented CI/CD processes. The high frequency of access issues and failed transactions points to an unreliable backend infrastructure, where deployment failures or rollbacks may be disrupting services.

The second dataset (table 6) examines the state of CI/CD practices in these banks, providing insights into deployment efficiency, automation levels, testing reliability, and rollback capabilities. The most common deployment strategy is "Mostly manual with frequent deployment issues" (17 cases). This suggests a reliance on manual intervention, increasing the risk of errors, delays, and system failures. 52 out of 102 cases indicate a lack of automation, highlighting a critical gap while poor testing was cited in 59 cases, suggesting that defective software updates frequently go live, causing system disruptions. Rollback issues were present in 59 cases, meaning banks struggle to revert faulty updates swiftly. Regulatory constraints (56 cases) may also hinder agile CI/CD implementations, as banks must comply with stringent financial regulations.

Compared to global banking standards, where CI/CD pipelines are highly automated and rigorously tested, Nigerian banks appear far behind. The heavy dependence on manual deployments, inadequate testing, and weak rollback mechanisms significantly increases the likelihood of system failures and service disruptions. In contrast, global banks such as JP Morgan Chase, HSBC, and Citibank leverage automated CI/CD pipelines that allow for Zero-downtime deployments, automated rollback of faulty updates, real-time monitoring and predictive failure detection. Without these capabilities, Nigerian banks remain vulnerable to repeated outages and operational inefficiencies.

The final dataset (table 7) assesses how these system inefficiencies translate into customer dissatisfaction. 53 out of 102 instances involved failed transactions, causing frustration among customers who expect seamless banking. Delayed payments occurred in 53 cases, further compounding customer grievances. 52 out of 102 cases reported customer dissatisfaction, making it clear that these technical failures are not going unnoticed.

Frequent transaction failures erode customer trust. If customers experience repeated failed payments, they may switch to more reliable banking alternatives, such as Fintech companies like Flutterwave and Paystack, which offer smoother payment processing.

Furthermore, the fact that customer dissatisfaction does not directly align with every instance of downtime suggests that service recovery and communication strategies play a role in shaping customer perception. Some failures may be tolerated if they are resolved quickly, but persistent issues drive long-term frustration.

6.3. Impact of Downtime on Customers Hypothesis

H_3: System downtimes in GTBank and First Bank have a negative impact on customer experience, leading to increased transaction failures, reduced customer trust, and financial losses.

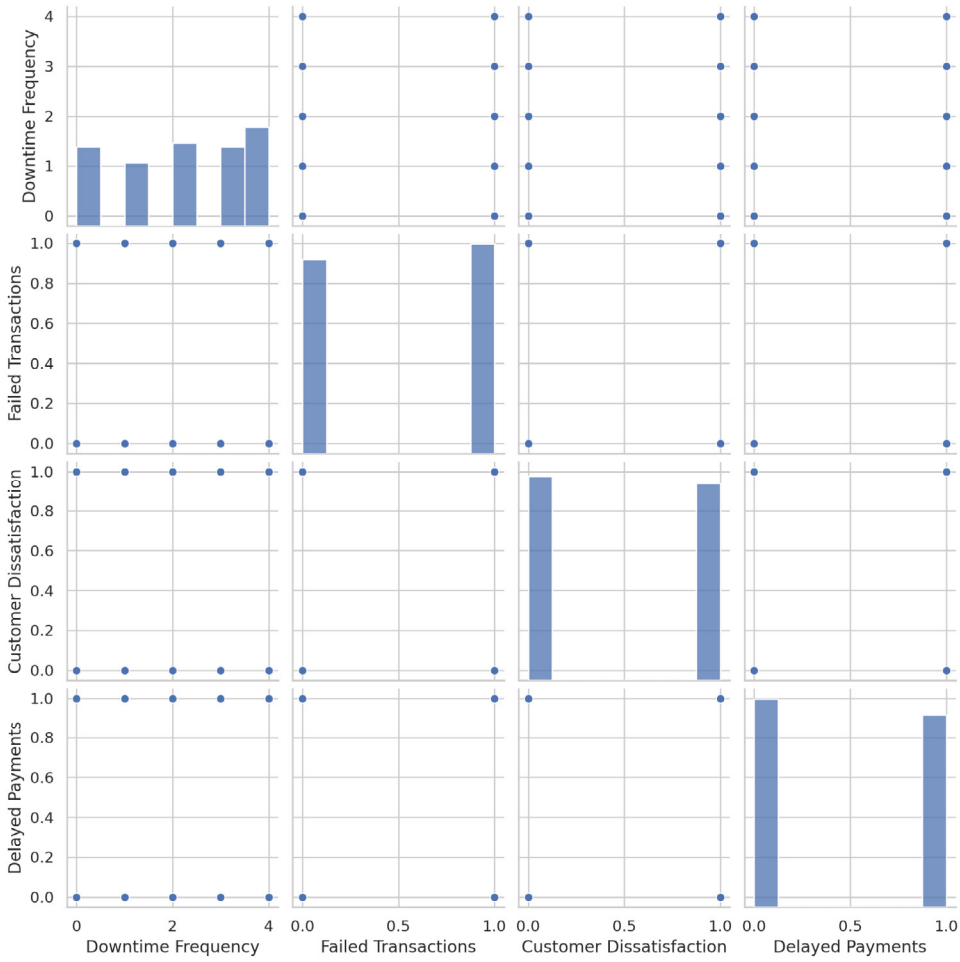

Figure 7

The pairplot (figure 7) visualizes the relationships between downtime frequency and customer impact metrics, such as failed transactions, customer dissatisfaction, and delayed payments. This analysis will help us understand how downtime correlates with customer experiences in GT Bank and First Bank.

"System downtimes in GTBank and First Bank have a negative impact on customer experience, leading to increased transaction failures, reduced customer trust, and financial losses."
The pairplot visualization in figure 7, illustrates the relationships between downtime frequency, failed transactions, customer dissatisfaction, and delayed payments—key indicators that measure the impact of system outages on customer experience.

The scatterplots reveal that as downtime frequency increases, the number of failed transactions also rises. This observation suggests that frequent disruptions in banking services negatively affect transaction success rates. In cases where downtime spikes, customers are unable to complete transactions, reinforcing the frustration and inefficiency associated with unreliable banking systems. Customer dissatisfaction was observed to increase in direct correlation with transaction failures. The plot suggests that when customers experience failed transactions, their trust in the banking system might be eroded, leading to dissatisfaction. This is a critical insight, as it implies that system downtimes not only disrupt financial transactions but also damage long-term customer relationships.

A significant proportion of delayed payments was linked to instances of system downtimes. This delay can have far-reaching consequences, including, late utility bill payments, leading to additional fees, unsuccessful payroll processing for businesses, strained relationships between customers and merchants. The relationship between these factors underscores that banking downtimes do not exist in isolation—they trigger a chain reaction affecting financial stability at multiple levels.

This implication is that frequent downtime and failed transactions may push customers toward alternative financial solutions such as fintech platforms, reducing traditional banks' revenue streams. Customer dissatisfaction may lead to negative word-of-mouth and social media complaints, damaging the bank's public image. Persistent service failures could invite regulatory interventions, requiring banks to invest more in compliance and infrastructure.

6.4. Enhancing CI/CD Pipelines Hypothesis

H_4: Implementing automated testing, continuous monitoring, and rollback mechanisms in CI/CD pipelines can significantly reduce the frequency and duration of banking system downtimes.

	Downtime Frequency	Downtime Duration (Hours)
count	74	53
unique	5	NULL
top	Rarely	NULL
freq	17	NULL
mean	NULL	9.1226415094
std	NULL	10.0574817446
min	NULL	0.5
25%	NULL	0.5
50%	NULL	5
75%	NULL	24
max	NULL	24

Table 8: Enhancing CI/CD Pipelines

Table 8 examines downtime frequency and downtime duration using empirical data collected from Nigerian banks. The goal is to provide insights into how often downtimes occur and how long they typically last, enabling banks to develop proactive mitigation strategies. 74 unique entries on downtime frequency were observed. The dataset captures five distinct categories of downtime frequency, suggesting that downtimes occur with varying regularity across different institutions. The term "Rarely" was reported the most (17 occurrences), indicating that many institutions experience downtime infrequently rather than regularly.

53 valid observations on downtime duration were available, indicating some missing data. The average downtime lasted 9.12 hours, a significant disruption that could severely impact transactions and customer trust. There is substantial variability in downtime duration, implying that some banks experience significantly longer disruptions than others with standard deviation of 10.06 hours. The shortest downtime lasted only 30 minutes (0.5 hours), indicating that some disruptions are quickly resolved. The longest recorded downtime was 24 hours, meaning some banks experienced a full day of service unavailability, which can lead to severe financial and reputational losses.

Percentile	Downtime Duration (Hours)	Interpretation
25% (First Quartile)	0.5	At least 25% of the downtime incidents lasted only 30 minutes, suggesting that some disruptions are quickly addressed.
50% (Median)	5	Half of all downtimes lasted 5 hours or less, meaning a significant proportion of incidents persist for several hours.
75% (Third Quartile)	24	At least 25% of the downtime incidents lasted a full day, highlighting the severity of outages for some banks.

Table 9: Percentile Breakdown of Downtime Duration

The data in table 9 suggests that while many banks experience downtime infrequently, those that do may suffer long-lasting disruptions. The high standard deviation and wide range (0.5 to 24 hours) indicate that downtime severity is inconsistent across institutions. A 9-hour average downtime is far from optimal for a digital banking ecosystem that relies on 24/7 availability. Long downtimes (up to 24 hours) can cause severe financial losses and erode customer trust, potentially leading to regulatory scrutiny.

the major issues that leads to service downtime in Nigeria banks in 2024. This analysis highlights the dual challenge of system downtime in Nigerian banks: while downtime may be infrequent for many institutions, those that do experience it often suffer prolonged outages. Given the increasing reliance on digital banking, addressing these issues through advanced technology, regulatory frameworks, and improved IT infrastructure should be a top priority for financial institutions.

7. Conclusion and Recommendations

This study has established that CI/CD pipeline becomes one of

Banks should deploy backup servers and failover mechanisms to minimize extended outages. Machine learning algorithms can

predict and prevent system failures before they occur. A dedicated rapid-response IT team should be established to quickly restore services when disruptions happen [13-18].

References

1. FSB (Financial Stability Board). (2018). Cyber Lexicon: Enhancing Financial System Resilience.
2. Nigerian Financial Intelligence Unit (NFIU). (2023). Operational Risk Management in Nigerian Banks: Trends and Best Practices.
3. Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience. Bank for International Settlements.
4. World Bank. (2022). Fintech and Digital Transformation in Africa: Addressing Infrastructure Gaps and Enhancing System Reliability.
5. Central Bank of Nigeria (CBN). (2024). *Banking System Downtime Report*. Abuja: CBN Publications.
6. McKinsey & Company. (2022). Digital Banking in Emerging Markets: Trends, Challenges, and Solutions.
7. PwC Nigeria. (2021). *Technology and Resilience in Nigerian Banks: Addressing Service Downtime Challenges*. PwC Research Brief.
8. Adebayo, T., & Oluwaseun, K. (2023). *Challenges of Software Deployment in Nigerian Financial Institutions*. Lagos: TechPress.
9. DevOps Institute. (2022). *Best Practices for Continuous Integration and Continuous Deployment in Enterprise Environments*. Boston: DevOps Press.
10. Kumar, R., Patel, S., & Singh, M. (2022). *DevOps and CI/CD in Financial Technology: Best Practices and Case Studies*. New York: Wiley.
11. JP Morgan. (2023). *Global Banking IT Standards and CI/CD Best Practices*. New York: JP Morgan Reports.
12. HSBC. (2023). *Ensuring Service Availability: The Role of Continuous Deployment in Banking*. London: HSBC Research.
13. KPMG. (2020). *Banking Disruptions and the Role of Technology in Mitigating Downtime Risks*. KPMG Research Report.
14. Ndungu, C., & Musau, J. (2021). *The Impact of System Downtime on Digital Banking: A Case Study of African Financial Institutions*. International Journal of Banking and Finance, 45(3), 67-89.
15. Nigeria Inter-Bank Settlement System (NIBSS). (2024). *Annual Report on Financial Transactions and IT Infrastructure*. Lagos: NIBSS.
16. Okonkwo, J. (2024). *The Role of Automation in Reducing Banking System Failures in Nigeria*. Ibadan: University of Ibadan Press.
17. Rahman, A., & Yusuf, M. (2023). *The Impact of CI/CD Implementation on Banking System Reliability*. International Journal of Financial Technology, 15(3), 45-63.
18. Wells Fargo. (2023). *Advancements in CI/CD for High-Frequency Financial Transactions*. San Francisco: Wells Fargo Tech.