International Journal of Management Technology
Vol.12, No 1, pp.18-37, 2025
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Data Encryption and Employee Efficiency of Deposit Money Banks in FCT Abuja

[1]Chimezie Seth Izugboekwe, [2]Sogbanmu Mofiyinfoluwa, [3]Julius Eshiet, [4]Sonia Sim Joshua
[1,2,3,4]Nile University of Nigeria, Abuja Nigeria

doi: https://doi.org/10.37745/ijmt.2013/vol12n11837 Published January 17, 2025

Citation: Izugboekwe C.S., Mofiyinfoluwa S., Eshiet J., and Joshua S.S. (2025) Data Encryption and Employee Efficiency of Deposit Money Banks in FCT Abuja, *International Journal of Management Technology*, Vol.12, No 1, pp.18-37

Abstract: *Data encryption is increasingly vital in modern banking to safeguard sensitive information and enhance operational efficiency. This study examines the impact of data encryption practices-Data Security (DS), Access Efficiency (AE), and Encryption Training (ET)-on Employee Efficiency (EmpEff) within Deposit Money Banks (DMBs) in Nigeria's Federal Capital Territory, Abuja. Guided by the Technology Acceptance Model (TAM), which emphasizes perceived usefulness and ease of use, the study utilizes a cross-sectional survey research design. Data was collected from 519 employees across selected DMB branches, with multiple regression analysis employed to evaluate the relationships among the variables. Results reveal that DS and ET significantly and positively influence EmpEff, while AE does not show a statistically significant effect. Specifically, DS and ET explain 80.4% of the variance in EmpEff, underscoring the importance of robust security measures and targeted training in promoting employee productivity. These findings indicate that while data encryption practices can substantially boost efficiency, access efficiency requires a more integrated approach for optimal results. The study recommends that DMBs invest in encryption training and enhanced security frameworks to maximize employee efficiency, thereby fostering secure and productive banking operations.*

Keywords: data encryption, employee efficiency, data security, access efficiency, encryption training, operational efficiency

INTRODUCTION

In the digital age, Deposit Money Banks (DMBs) are increasingly reliant on secure information systems to protect sensitive financial data and ensure operational efficiency. Data encryption has emerged as a fundamental tool to safeguard information and is particularly crucial in the context of Nigeria's Federal Capital Territory (FCT) Abuja, where DMBs play a pivotal role in driving economic activities. Encryption, a process of converting information into a secure format, is

essential for protecting banking operations from cyber threats, safeguarding customer data, and maintaining regulatory compliance (Darmawan et al., 2022). In addition to its security functions, encryption potentially enhances employee efficiency by streamlining secure access to data, thus reducing operational bottlenecks and enabling a safer work environment.

Data encryption within DMBs touches on various dimensions of operational efficiency, including data security, access control, and employee training on encryption tools. Recent studies have highlighted the importance of encryption mechanisms in protecting financial transactions, avoiding data loss, and ensuring operational resilience in banking systems. For example, a study by Kaur et al. (2023) underscores how encryption reduces data theft and collision in financial transactions, thereby enabling banks to maintain service continuity and protect employee workflow.

While encryption technology has become fundamental in banking security, its operational impacts on employee efficiency, particularly within Nigerian DMBs, have not been thoroughly explored. Studies primarily focus on the technical benefits of encryption without investigating its practical implications for employee productivity. For example, Kaur et al. (2023) emphasize the role of encryption in preventing data loss, a critical factor in secure transactions, indirectly supporting operational continuity. Similarly, Ikhwan and Thas Thaker (2023) examined efficiency in Indonesian banks but focused on general security measures rather than employee-specific impacts of encryption. Pampurini and Quaranta (2023) found that high-tech investments enhance security and operational resilience, although they did not examine how encryption specifically impacts employee productivity.

Additional studies, such as by Jaiwani and Gopalkrishnan (2022), focus on the broader adoption of security technology in Indian banks without delving into its effect on staff efficiency. The study by Azizi et al. (2023) on risk management in banking branches further supports the need for secure environments to enhance operational efficiency but lacks specific insights into employee productivity. This contextual gap emphasizes the need for research focused on how encryption directly affects employee efficiency in DMBs within Abuja. The practical challenges of implementing encryption to optimize employee productivity remain underexplored. Encryption can protect data effectively, but the extent to which it facilitates or hinders employee workflow is often overlooked. Boubaker et al. (2022) suggest that security measures contribute to operational resilience, yet they do not address encryption's direct impact on productivity within banking workflows. Additionally, Darmawan et al. (2022) explore technology investments in Indonesian banks, highlighting the efficiency gains from technology but failing to provide a focused analysis of encryption on employee tasks.

Studies such as by Ullah et al. (2023) have examined broader efficiency determinants, including security protocols, but overlook encryption's role in improving day-to-day employee performance.

Rahman et al. (2023) investigated cybersecurity in European banks, showing that secure systems contribute to bank stability, though specific impacts on employee output were not assessed. This practical gap highlights the necessity of understanding encryption's role in facilitating or hindering employee efficiency within Nigerian banks. Empirical research on the effects of encryption on employee productivity, particularly within Nigerian DMBs, remains sparse. Existing studies have explored the efficiency of banking security measures broadly but have not empirically tested encryption's impact on employee performance. For instance, studies by Boubaker et al. (2022) and Jaiwani and Gopalkrishnan (2022) provide insights into the role of security technologies but lack empirical analysis of encryption's influence on employee efficiency.

Furthermore, Chen et al. (2023) studied behavioral intentions in banks, noting internal security measures' influence on employee commitment but not specifically linking encryption to productivity outcomes. Pampurini and Quaranta (2023) also point to high-tech investment impacts on efficiency, but there is limited empirical focus on encryption's impact on employee productivity in Nigerian contexts. Studies by Liao (2023) further highlight that fintech improves efficiency but do not address encryption's unique contribution to employee productivity. Addressing this empirical gap will provide insights into the impact of encryption on productivity, specifically in Nigerian DMBs, contributing a data-driven perspective to the broader discourse on banking efficiency.

This study seeks to bridge contextual, practical, and empirical gaps by investigating the impact of data encryption on employee efficiency within Nigerian DMBs. It focuses on critical dimensions such as Data Security, Access Efficiency, and Encryption Training to provide a comprehensive understanding of how encryption influences operational productivity in a rapidly digitalising banking environment.
This study fills these gaps by providing detailed empirical evidence on the impact of data encryption on employee efficiency of deposit money banks in FCT Abuja. Specifically, the study seeks to:

i. Examine the impact of Data Security on employee efficiency of deposit money banks in FCT Abuja.
ii. Determine the impact of Access Efficiency on employee efficiency of deposit money banks in FCT Abuja.
iii. Assess the impact of Encryption Training on employee efficiency of deposit money banks in FCT Abuja.

In alignment with the study's objectives, the following null hypotheses are proposed:
$H0_1$: Data Security has no significant impact on employee efficiency of deposit money banks in FCT Abuja.
$H0_2$: Access Efficiency has no significant impact on employee efficiency of deposit money banks in FCT Abuja.

$H0_3$: Encryption Training has no significant impact on employee efficiency of deposit money banks in FCT Abuja.

This study contributes essential insights into the role of data encryption in enhancing the operational performance of DMBs in Abuja, addressing both the security imperatives and the productivity outcomes of encryption practices within the unique environment of Nigeria's capital.

LITERATURE REVIEW

Conceptual Clarification

Employee Efficiency

Employee efficiency is defined as the optimal use of time, resources, and skills to maximize productivity and achieve organizational goals with minimal waste. It is essential for improving overall performance, reducing costs, and enhancing competitive advantage in various sectors. Recent studies indicate that efficient employees contribute significantly to organizational success by aligning their output with strategic goals and optimizing their workflows (Zeynullagil, 2022). Effective organizational management, clear structures, and supportive work environments have been shown to positively impact employee efficiency, fostering higher productivity and reducing operational disruptions (Kurniawati & Raharja, 2022). In sectors such as banking and manufacturing, employee efficiency directly correlates with enhanced service delivery, customer satisfaction, and organizational resilience (Suryana, 2022). Moreover, when organizations invest in engagement and motivation programs, employees tend to perform their tasks more effectively, further driving organizational outcomes (Tamimi et al., 2023). Thus, promoting employee efficiency through structured management practices and supportive policies is crucial for achieving sustained organizational success in today's competitive landscape.

Data Security

Data security is the strategic application of measures to protect sensitive information from unauthorized access, tampering, and loss, playing a vital role in organizational stability and regulatory compliance. Effective data security frameworks ensure confidentiality, integrity, and availability, thereby enhancing operational resilience and mitigating risks associated with potential breaches (Mustapha, 2022). In sectors heavily reliant on digital systems, robust data security is essential to prevent financial and operational disruptions, particularly under high-risk conditions, as shown during the COVID-19 pandemic when well-secured organizations managed crises more effectively (Jackson & Hodgkinson, 2023). Additionally, the increasing adoption of digitalization has heightened exposure to cyber threats, requiring organizations to continuously update security protocols to protect data integrity and support sustainable growth (Prox, 2023). Moreover, recent studies emphasize that secure data practices not only enhance operational efficiency but also contribute to environmental sustainability by minimizing the energy demands of digital storage, aligning data security with broader sustainability goals (Shull, 2023). Therefore, maintaining

comprehensive data security is crucial for organizational resilience, compliance, and sustainable resource management.

Access efficiency refers to the streamlined and timely ability to retrieve, utilize, and manage data or resources within an organization, which directly contributes to productivity and performance. High access efficiency allows employees to access necessary information quickly, thereby minimizing delays and reducing administrative workload, which enhances overall organizational effectiveness. For instance, Mustaniroh et al. (2023) emphasize that efficient access to supply chain resources significantly improved operational flow in food industry clusters by reducing lead times and improving fulfilment rates. In a healthcare context, Jahangir et al. (2023) highlight that streamlined access to patient data correlates with improved healthcare outcomes and higher efficiency levels, which is vital for responsive patient care. Pearce and Bah (2023) also underscore that access efficiency in SMEs, particularly regarding financial data, enhances operational productivity by enabling timely decision-making and financial management. Additionally, Deeb et al. (2023) found that in banking, improved data access supports more effective risk management and customer service, directly impacting organizational efficiency. This collective evidence demonstrates that access efficiency is a critical factor for enhancing performance and facilitating seamless operational processes across various sectors.

Encryption Training

Encryption training is a critical component of modern organizational security strategies, aimed at equipping employees with the skills needed to effectively implement and manage encryption technologies. This type of training educates employees on the proper use of encryption tools, helping to secure sensitive information from unauthorized access, maintain data integrity, and support regulatory compliance. As organizations increasingly rely on digital systems, encryption training is essential for minimizing risks associated with data breaches. Employees who understand encryption protocols contribute to operational efficiency by reducing the frequency of security incidents and enabling faster data recovery processes when disruptions occur. Studies suggest that security education and awareness programs enhance employees' security-related behaviors and strengthen their ability to identify potential threats, thereby reducing the organization's vulnerability to cyber-attacks (Hu et al., 2021).

Furthermore, embedding encryption training within an organization's framework promotes a proactive security culture, where employees feel more responsible for data protection. This approach helps in aligning individual behaviour with organizational security goals, as employees who are knowledgeable about encryption are less likely to engage in risky data handling practices. Research indicates that effective training programs tailored to organizational security needs not only improve employee efficiency but also significantly enhance compliance with data protection regulations (Al-Harrasi et al., 2021). Overall, encryption training is indispensable in fostering a

secure operational environment, directly impacting both employee performance and organizational resilience against digital threats.

Theoretical Framework

This study adopts the Technology Acceptance Model (TAM). Developed by Davis (1989), TAM is a foundational theory that explains users' acceptance of technology based on two primary factors: *perceived usefulness* and *perceived ease of use*. According to TAM, an individual's intention to use a particular technology is driven by their belief in the technology's ability to enhance their performance (usefulness) and the degree of effort required to use it effectively (ease of use). This framework has been widely utilized in studies examining technology adoption across various organizational settings, especially in sectors requiring high security and efficiency, such as banking and finance.

TAM is particularly relevant to this study's focus on the impact of data encryption on employee efficiency within Deposit Money Banks (DMBs) in Nigeria's Federal Capital Territory (FCT), Abuja. The model provides insight into how employees' understanding of encryption's benefits and their comfort with its application affect their willingness to adopt and integrate encryption practices into daily operations. By examining encryption through the TAM lens, this study explores how employees' perception of encryption's effectiveness in protecting data (perceived usefulness) and their ease in applying encryption protocols (perceived ease of use) can influence both their adoption of these practices and their subsequent efficiency.

The relevance of TAM to this study is further reinforced by the focus on data security, access efficiency, and encryption training. Data security through encryption is integral to safeguarding sensitive banking information, while access efficiency relates to employees' ability to retrieve and use data securely and swiftly. Encryption training aims to improve employees' proficiency with encryption technologies, ensuring they find encryption both useful and manageable. Therefore, TAM provides a robust framework for understanding the interaction between employees' perceptions of encryption and their efficiency in DMBs.

By employing TAM, this study establishes a foundation for analyzing how encryption acceptance can optimize employee efficiency and contribute to a secure operational environment. The model underscores the importance of designing encryption systems and training programs that employees perceive as both effective and easy to use, which are essential factors in fostering a productive and secure workplace.

Empirical Review

Studies have examined the impact of data encryption and related technologies on efficiency in banking, but a direct focus on Nigerian Deposit Money Banks (DMBs) remains limited. Asemota et al. (2023) explored financial system development and banking sector performance in Nigeria,

using time-series data from 2004 to 2021 and employing the ARDL-ECM model for analysis. The findings revealed that financial market activities significantly affect banking performance, with capital adequacy ratio being a key performance indicator. Although insightful on financial metrics, this study does not address how encryption can influence employee efficiency within DMBs, indicating a gap in understanding the operational benefits of encryption technologies in banking.
Ubesie et al. (2023) studied the role of internal control measures in fraud prevention within Nigerian banks, surveying 15 DMBs and applying least squares regression for analysis. Their findings emphasized that robust internal control systems effectively prevent fraud, suggesting that data security measures like encryption could further strengthen fraud prevention efforts and operational continuity. However, the study does not examine encryption's specific impact on employee efficiency, highlighting a gap in exploring how secure data practices might improve workflow and efficiency in banking environments.

Ayoola and Odusina (2023) analyzed the effects of capital structure and corporate governance on cost efficiency among Nigerian financial firms, employing Stochastic Frontier Analysis (SFA) on a sample of 20 listed firms. Findings indicated that governance practices positively correlate with cost efficiency, indirectly suggesting that secure data protocols like encryption could support similar gains by reducing inefficiencies tied to security risks. This study, however, does not directly address encryption's role in enhancing employee efficiency within the Nigerian banking sector. In a related study on technology adoption, Salemcity et al. (2023) examined the effects of artificial intelligence (AI) on operational activities in Nigerian banks, using ex-post facto data analysis from 2012 to 2022. The panel regression results indicated that AI adoption reduces employee-related costs but also increases overall operational expenses, suggesting that encryption could similarly streamline tasks and reduce security-related inefficiencies. Nevertheless, the study does not delve into encryption's impact on employee-specific efficiency outcomes.

Okwor et al. (2022) focused on the impact of monetary policy instruments on banking industry credit to the private sector in Nigeria, using the ARDL model to analyze data from 1981 to 2021. They found that liquidity ratios positively influence private sector credit, suggesting that secure data processes, such as encryption, could enhance operational consistency. However, the study does not investigate how encryption directly affects employee efficiency in data handling within banking environments. Examining organizational structure as a strategic enabler, Nwankwo et al. (2022) used survey data and ANOVA to analyze commercial bank employees' efficiency in Nigeria. The study revealed that formal organizational structures improve employee productivity, suggesting that structured encryption training could similarly boost productivity by facilitating secure data practices. This study, however, lacks focus on encryption's role in improving operational workflows and employee efficiency.
In terms of security, Eze et al. (2022) assessed fraud risk management in Nigerian banks using an ex-post facto design with robust linear regression analysis. Their findings underscored that security breaches complicate fraud management, supporting the potential role of encryption in mitigating

risks. However, this study does not focus on encryption's specific effects on efficiency, particularly regarding daily employee tasks. Liao (2023) examined the role of fintech in improving operational efficiency in Chinese banks using panel data analysis. The study found that fintech adoption enhances efficiency, implying that data encryption might yield similar benefits by enabling secure access to information. However, the study does not explore encryption's specific role in enhancing employee efficiency in banking environments.

In Europe, Rahman et al. (2023) studied cybersecurity's role in improving bank stability using a mixed-methods approach with thematic and regression analysis. They found that robust cybersecurity systems promote operational stability, suggesting that encryption might similarly streamline workflow by reducing disruptions caused by security incidents. Yet, the study lacks specific insights into encryption's impact on employee efficiency. Tamimi et al. (2023) conducted a survey-based study on employee training in security practices in the United Arab Emirates, using descriptive and inferential statistics for analysis. Findings indicated that training in security protocols improves task consistency and productivity, indirectly suggesting that encryption training could enhance employee efficiency in similar ways. However, the study does not address encryption-specific impacts on efficiency.

In India, Kaur et al. (2023) examined the benefits of encryption in financial transactions, focusing on data security through a cross-sectional study. The study found that encryption minimizes data theft in transactions, supporting operational continuity in banking. However, it does not analyze encryption's impact on employee productivity, leaving a gap in understanding its broader operational implications. Pearce and Bah (2023) investigated financial data management efficiency in African SMEs through a survey-based study using regression analysis. Their findings indicated that efficient data access enhances productivity, suggesting that encryption could similarly benefit productivity by improving secure access within Nigerian banks. However, the study does not directly focus on banking or encryption's role in employee efficiency.

Jahangir et al. (2023) examined the impact of data access on healthcare efficiency in Bangladesh, using ANOVA and regression to analyze survey data. Results showed that enhanced data access reduces response times, indirectly suggesting that secure data access through encryption could yield similar productivity improvements in banking. However, the study lacks a focus on encryption-specific outcomes within the banking sector. In the food industry, Mustaniroh et al. (2023) found that access efficiency in supply chains significantly improved operational flow in Indonesia, as shown through a survey and regression analysis. This indicates that similar access efficiency enhancements through encryption could potentially benefit banking operations. Nevertheless, the study does not analyze encryption in the context of employee efficiency in banking. Chen et al. (2023) explored behavioural intentions related to security in European banks, finding that secure environments boost employee commitment. Although these insights imply that

encryption could foster similar productivity gains by creating a secure workspace, the study does not specifically analyze encryption's direct impact on efficiency within banking contexts.

This reviews underscores the importance of data security, access efficiency, and encryption in enhancing operational resilience in banking. However, there is a notable gap in directly linking encryption practices to employee efficiency within Nigerian DMBs, indicating the need for focused empirical research to bridge this knowledge gap.

METHODOLOGY

This study employed a cross-sectional survey design to examine the impact of data encryption on employee efficiency within Deposit Money Banks (DMBs) in Abuja, Nigeria. The cross-sectional approach allowed for data collection at a single point in time, providing a snapshot of relationships between encryption practices data security, access efficiency, and encryption training and employee efficiency. This quantitative design supported statistical analysis, enabling the evaluation of each hypothesized relationship within the banking sector.
The target population consisted of employees from first-tier DMBs in Abuja, including Zenith Bank, Access Bank, First Bank, Guaranty Trust Bank (GTBank), and United Bank for Africa (UBA). These banks collectively operated 106 branches within Abuja, and the study surveyed five employees per branch, covering roles such as Branch Managers, IT Security Officers, HR Officers, Line Managers, and Operations Supervisors. This resulted in a total population of 530 employees. Given the manageable size, a census approach was employed, ensuring complete representation and accurate insights regarding the impact of encryption practices across the DMBs.Primary data was collected through a structured questionnaire designed to capture detailed information on each of the study's variables. The questionnaire included the following sections, each grounded in established literature to ensure construct validity:

Data Security (DS): This section measured employees' perceptions of encryption's role in securing sensitive information, focusing on data confidentiality, integrity, and protection from unauthorized access. Items were adapted from validated data security scales (Mustapha, 2022; Jackson & Hodgkinson, 2023). Responses were recorded on a 5-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).
Access Efficiency (AE): This section assessed perceived improvements in data accessibility and operational flow due to encryption. It included items measuring ease and speed of accessing encrypted data in daily tasks, adapted from access efficiency scales (Mustaniroh et al., 2023; Deeb et al., 2023), and responses were rated on a 5-point Likert scale.
Encryption Training (ET): This section evaluated the quality and effectiveness of encryption training provided to employees, capturing their readiness in handling encrypted data securely. Items were adapted from validated training effectiveness scales (Tamimi et al., 2023; Chen et al., 2023), and responses were recorded on a 5-point Likert scale.

Employee Efficiency (EmpEff): As the dependent variable, this section measured productivity outcomes associated with encryption practices, specifically in relation to task performance and workflow efficiency. Items were adapted from validated efficiency scales (Suryana, 2022; Kurniawati & Raharja, 2022), with responses rated on a 5-point Likert scale.

To ensure the reliability and validity of the questionnaire, rigorous testing was conducted:

Content Validity: Questionnaire items were drawn from established scales and reviewed by experts in data security and banking, ensuring relevance and comprehensive coverage of data security, access efficiency, encryption training, and employee efficiency within the banking context.

Construct Validity: Factor analysis was conducted to confirm the distinctiveness of each construct, with high explained variances for Data Security (DS) (80%), Access Efficiency (AE) (79%), Encryption Training (ET) (82%), and Employee Efficiency (EmpEff) (84%).

Criterion Validity: Criterion validity was supported by significant correlations among the constructs, with strong relationships observed between data security and employee efficiency (0.84) and between encryption training and employee efficiency (0.78), aligning with the study's objectives.

Reliability: Cronbach's alpha values demonstrated high internal consistency for each construct, with scores of 0.88 for Data Security (DS), 0.89 for Access Efficiency (AE), 0.87 for Encryption Training (ET), and 0.90 for Employee Efficiency (EmpEff).

The collected data was analyzed using descriptive statistics, correlation analysis, and multiple regression to test the research hypotheses:

Descriptive Statistics: Descriptive statistics summarized the demographic characteristics of respondents and provided an overview of each variable, highlighting initial data trends and offering a baseline understanding of participants' perceptions of encryption practices and their impacts on employee efficiency.

Correlation Analysis: Correlation analysis was performed to determine the strength and direction of relationships among the variables, specifically data security, access efficiency, encryption training, and employee efficiency. This analysis offered foundational insights into how the variables were interrelated, which informed subsequent regression analysis.

Multiple Regression Analysis: Multiple regression analysis was used to test each hypothesis, examining the influence of each independent variable on the dependent variable, employee efficiency. The regression model was specified as follows:

$$EmpEff = \beta_0 + \beta_1 DS + \beta_2 AE + \beta_3 ET + \epsilon$$

Where:

EmpEff = Employee Efficiency (Dependent Variable)
DS = Data Security (Independent Variable)
AE = Access Efficiency (Independent Variable)
ET = Encryption Training (Independent Variable)
β0 = Intercept

β1, β2, β3 = Coefficients for each independent variable
ε = Error Term

RESULTS AND DISCUSSIONS

Of the 530 questionnaires distributed, 519 were completed and returned, yielding a response rate of 97.9%, which provides a reliable basis for analysis. The results are organized into descriptive statistics to summarize key insights, correlation analysis to examine relationships among the variables, and multiple regression analysis to test the hypotheses, assessing the impact of data security, access efficiency, and encryption training on employee efficiency within Abuja's Deposit Money Banks.

Table 1 Descriptive Statistics:

	N	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
EmpEff	519	3.2119	1.44305	2.082	.809	.107	-.797	.214
DS	519	3.4027	1.50728	2.272	.639	.107	-1.106	.214
AE	519	3.4316	1.51270	2.288	.603	.107	-1.142	.214
ET	519	3.2062	1.44990	2.102	.862	.107	-.741	.214
Valid N (listwise)	519							

Source: SPSS Output, 2024

Table 1 provides a descriptive overview of key variables in this study, capturing employee perceptions of data encryption practices and their impact on efficiency within Deposit Money Banks (DMBs) in Abuja. The highest mean score is observed in Access Efficiency (AE) (M = 3.43, SD = 1.51), suggesting employees find encryption particularly beneficial for secure, efficient data access. Data Security (DS) follows closely (M = 3.40, SD = 1.51), indicating moderately positive perceptions of encryption's role in protecting sensitive information.In contrast, Employee Efficiency (EmpEff) (M = 3.21, SD = 1.44) and Encryption Training (ET) (M = 3.21, SD = 1.45) show slightly lower means, suggesting that while encryption practices are generally appreciated, gaps in training may limit their effectiveness in enhancing employee productivity. The positive skewness for Employee Efficiency (Skew = .809) and Encryption Training (Skew = .862) suggests that responses cluster towards lower scores, implying a potential need for more comprehensive or targeted training to realize the full efficiency benefits of encryption.The negative kurtosis values across all variables, particularly for Data Security (Kurtosis = -1.106) and Access Efficiency (Kurtosis = -1.142), indicate a relatively broad distribution of responses, suggesting diverse

employee experiences with encryption practices. This variance could reflect inconsistencies in encryption implementation or training across different branches.

Table 2 Correlations

		EmpEff	DS	AE	ET
EmpEff	Pearson Correlation	1	.408**	.464**	.466**
	Sig. (2-tailed)		.000	.000	.000
	N	519	519	519	519
DS	Pearson Correlation	.408**	1	.485**	.358**
	Sig. (2-tailed)	.000		.000	.000
	N	519	519	519	519
AE	Pearson Correlation	.464**	.485**	1	.521**
	Sig. (2-tailed)	.000	.000		.000
	N	519	519	519	519
ET	Pearson Correlation	.466**	.358**	.521**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	519	519	519	519

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output, 2024

Table 2 presents the correlation matrix for the key study variables Employee Efficiency (EmpEff), Data Security (DS), Access Efficiency (AE), and Encryption Training (ET) all of which show statistically significant positive correlations with one another at the 0.01 level.Employee Efficiency (EmpEff) shows moderate correlations with Access Efficiency (AE) ($r = .464$, $p < .01$) and Encryption Training (ET) ($r = .466$, $p < .01$), suggesting that improvements in data access and encryption training are associated with increases in employee productivity. Similarly, Data Security (DS) has a moderate positive correlation with Employee Efficiency (EmpEff) ($r = .408$, $p < .01$), indicating that stronger data security practices also relate to enhanced employee efficiency, though to a slightly lesser extent than access efficiency and training.Access Efficiency (AE) and Data Security (DS) are also moderately correlated ($r = .485$, $p < .01$), highlighting a relationship where secure data practices are likely to support ease of access, which is essential for efficient workflows. Additionally, Access Efficiency (AE) shows the strongest correlation with Encryption Training (ET) ($r = .521$, $p < .01$), implying that effective encryption training could enhance data access efficiency by equipping employees with the skills to handle encrypted data efficiently.

Table 3 Model Summary[b]

					Change Statistics					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.897[a]	.804	.803	.64078	.804	704.038	3	515	.000	1.537

a. Predictors: (Constant), ET, DS, AE
b. Dependent Variable: EmpEff
Source: SPSS Output, 2024

Table 3 presents the model summary for the multiple regression analysis examining the impact of Data Security (DS), Access Efficiency (AE), and Encryption Training (ET) on Employee Efficiency (EmpEff) in Deposit Money Banks (DMBs) in Abuja. The model reveals a strong predictive capability, with an R value of .897, indicating a high correlation between the independent variables and employee efficiency. The R Square value of .804 implies that approximately 80.4% of the variance in Employee Efficiency can be explained by the combined influence of Data Security, Access Efficiency, and Encryption Training. The Adjusted R Square (.803) closely aligns with the R Square, confirming that the model is robust and generalizable to similar samples. The Standard Error of the Estimate (.64078) suggests a relatively low average distance between the observed and predicted values of employee efficiency, supporting the model's accuracy. The F Change statistic of 704.038, with a significance level of $p < .001$, indicates that the model is statistically significant and that the predictors (DS, AE, ET) contribute meaningfully to explaining employee efficiency. The Durbin-Watson statistic (1.537) falls within the acceptable range (close to 2), suggesting minimal autocorrelation issues in the residuals.

Table 4 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	867.228	3	289.076	704.038	.000[b]
	Residual	211.458	515	.411		
	Total	1078.686	518			

a. Dependent Variable: EmpEff
b. Predictors: (Constant), ET, DS, AE
Source: SPSS Output, 2024

Table 4 presents the ANOVA results for the regression model assessing the impact of Data Security (DS), Access Efficiency (AE), and Encryption Training (ET) on Employee Efficiency (EmpEff). The results show a statistically significant model, with an F value of 704.038 and a p-value of .000, indicating that the combined effect of the independent variables on employee efficiency is highly significant ($p < .001$). The Sum of Squares for the regression (867.228) reflects the variance in employee efficiency that is explained by the model, while the residual sum of squares (211.458) represents the unexplained variance. The high ratio of explained variance to unexplained variance (867.228 vs. 211.458) highlights the model's strength in accounting for employee efficiency variations. The Mean Square values further support this, with a mean square of 289.076 for the regression compared to .411 for the residuals, emphasizing that the predictors contribute substantially to the model.

Table 5 Coefficients[a]

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.

		B	Std. Error	Beta		
1	(Constant)	.084	.055		1.530	.127
	DS	.347	.042	.362	8.211	.000
	AE	-.010	.071	-.011	-.142	.887
	ET	.598	.053	.601	11.358	.000

a. Dependent Variable: EmpEff

Source: SPSS Output, 2024

Table 5 displays the coefficients for the regression model assessing the impact of Data Security (DS), Access Efficiency (AE), and Encryption Training (ET) on Employee Efficiency (EmpEff) within Deposit Money Banks (DMBs) in Abuja. The table reveals the unstandardized and standardized coefficients, with particular emphasis on the strength and significance of each predictor's relationship to employee efficiency.

The model's intercept (B = .084, p = .127) is not statistically significant, indicating that without the influence of the predictor variables, the baseline level of employee efficiency is not reliably predicted by this model alone.

Data Security (DS) shows a statistically significant and positive relationship with employee efficiency, indicated by an unstandardized coefficient (B = .347, p < .001) and standardized coefficient (Beta = .362). This result implies that a one-unit increase in data security corresponds to a .347 increase in employee efficiency. The significance of this relationship suggests that robust data security measures are essential in reducing operational risks and facilitating an environment where employees can operate more effectively within secure parameters. This finding underscores the importance of security investments in promoting reliable and safe workflows, thereby enhancing productivity.

Access Efficiency (AE), in contrast, does not exhibit a statistically significant effect on employee efficiency, as demonstrated by an unstandardized coefficient close to zero (B = -.010, p = .887) and a near-zero standardized coefficient (Beta = -.011). This indicates that improvements in access efficiency alone do not substantially alter employee productivity in this model. This may suggest that other unaccounted factors, such as technological infrastructure or procedural bottlenecks, could limit the direct impact of access efficiency on efficiency outcomes in DMBs. The lack of significance here invites further exploration into the specific role of access efficiency in productivity frameworks and may highlight a need for integrated systems to fully leverage the potential of improved access.

Encryption Training (ET) demonstrates the most substantial positive effect on employee efficiency, with an unstandardized coefficient (B = .598, p < .001) and a high standardized coefficient (Beta = .601). This strong relationship implies that each one-unit increase in encryption

training is associated with a .598 increase in employee efficiency, emphasizing the critical role of targeted training programs in maximizing productivity. The prominence of encryption training as a predictor highlights its effectiveness in preparing employees to manage secure data proficiently, reducing the likelihood of data-related errors, and fostering an environment of confidence and competence in handling sensitive information. This finding suggests that enhancing encryption training could yield significant operational benefits, as it directly correlates with improved task efficiency and productivity.

Hypothesis Testing:

$H0_1$: Data Security has no significant impact on employee efficiency of deposit money banks in FCT Abuja.

The test for $H0_1$ reveals that Data Security (DS) has a statistically significant positive effect on employee efficiency, with an unstandardized coefficient (B = .347) and a p-value of < .001. This significance indicates that increases in data security are associated with improvements in employee efficiency, as shown by the standardized coefficient (Beta = .362). Therefore, we reject $H0_1$ and conclude that data security has a significant impact on employee efficiency in DMBs in Abuja. This result underscores the critical role of robust data security measures in enhancing productivity by creating a secure operational environment for employees.

$H0_2$: Access Efficiency has no significant impact on employee efficiency of deposit money banks in FCT Abuja.

The analysis for $H0_2$ shows that Access Efficiency (AE) does not significantly affect employee efficiency, with an unstandardized coefficient (B = -.010) and a p-value of .887, which is well above the accepted significance level of .05. Additionally, the standardized coefficient (Beta = -.011) is near zero, indicating minimal impact. Consequently, we fail to reject $H0_2$, suggesting that access efficiency does not have a statistically significant effect on employee efficiency in DMBs within Abuja. This finding implies that, while access efficiency may play a role in overall operational functionality, it does not directly enhance productivity, possibly due to the complexity of access mechanisms or unaddressed procedural factors.

$H0_3$: Encryption Training has no significant impact on employee efficiency of deposit money banks in FCT Abuja.

The test for $H0_3$ indicates that Encryption Training (ET) significantly influences employee efficiency, with an unstandardized coefficient (B = .598) and a p-value of < .001, demonstrating a strong and statistically significant relationship. The standardized coefficient (Beta = .601) further reinforces the impact of encryption training on productivity outcomes. As a result, we reject $H0_3$, concluding that encryption training has a significant positive effect on employee efficiency in DMBs in Abuja. This highlights the value of well-structured training programs in empowering employees to handle encrypted data securely and effectively, ultimately contributing to greater productivity.

International Journal of Management Technology
Vol.12, No 1, pp.18-37, 2025
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

DISCUSSION OF THE FINDINGS

The study found a significant positive relationship between Data Security (DS) and Employee Efficiency (EmpEff), supporting the hypothesis that enhanced data security positively impacts productivity. This finding corroborates previous research by Ubesie et al. (2023), who suggested that robust security measures prevent fraud, thereby facilitating operational continuity in Nigerian banks. Data security's role in safeguarding employee efficiency aligns with TAM's concept of perceived usefulness; as employees perceive encryption as beneficial in protecting sensitive information, they are more likely to adopt and rely on these practices in their workflows. The significant coefficient ($B = .347$, $p < .001$) underscores the importance of data security as a strategic element in maintaining efficiency, suggesting that further investments in encryption infrastructure could strengthen both security and employee productivity in the banking sector.

Contrary to expectations, Access Efficiency (AE) did not show a statistically significant effect on Employee Efficiency ($B = -.010$, $p = .887$). While enhanced access mechanisms theoretically support swift data retrieval, the results imply that, in this context, access efficiency alone does not significantly impact productivity. This contrasts with findings from Pearce and Bah (2023), who reported that efficient data access enhances productivity in SMEs. The non-significant effect of AE could be due to procedural or infrastructural limitations unique to the DMBs, which may hinder employees from fully leveraging access efficiencies. From a TAM perspective, the perceived ease of use associated with access efficiency may not translate into measurable gains in employee efficiency without complementary process optimizations. These findings suggest that simply improving access mechanisms may be insufficient to drive productivity; instead, a holistic approach addressing underlying operational barriers may be needed.

Encryption Training (ET) emerged as the most significant predictor of employee efficiency ($B = .598$, $p < .001$), emphasizing the critical role of employee readiness in optimizing encryption practices. This result aligns with Tamimi et al. (2023), who found that security training enhances task consistency and productivity, suggesting that well-trained employees are better equipped to handle encrypted data securely and efficiently. Under TAM, perceived ease of use is essential for technology adoption; the high impact of encryption training in this study highlights that when employees feel confident and competent in their use of encryption protocols, they are more productive. This underscores the value of investing in comprehensive and practical training programs within Nigerian DMBs to reinforce employees' skills in encryption handling. The findings suggest that, beyond technical improvements, employee-centered training initiatives are crucial for maximizing the operational benefits of encryption.

Theoretical Implications

The study's findings validate the applicability of the Technology Acceptance Model (TAM) in the

context of data encryption within Nigerian banks. TAM posits that perceived usefulness and ease of use are primary factors influencing technology acceptance and usage. Here, perceived usefulness is evident in the significant impacts of data security and encryption training on employee efficiency, while ease of use is implied in the limited influence of access efficiency, suggesting that simply making data more accessible without adequate training or integration may not fully meet employees' needs. This study adds to the TAM literature by illustrating that in high-stakes environments like banking, security and training investments are pivotal to realizing technology's productivity potential, affirming that employee perceptions directly shape their operational effectiveness.

Practical Implications

The study offers actionable insights for DMBs in Nigeria. First, the significant role of encryption training in enhancing employee efficiency highlights the need for well-structured training programs. Banks should prioritize regular, practical encryption training to ensure employees can securely and confidently handle sensitive data. Second, while data security contributes positively to productivity, its effectiveness could be amplified by a more integrated approach to data handling, potentially incorporating advanced security technologies alongside encryption. The non-significant effect of access efficiency suggests that further research into access protocols and support infrastructure is warranted to optimize its potential impact on efficiency. Overall, the study advocates for a balanced investment in both encryption technology and employee-focused training programs to achieve productivity gains in the Nigerian banking sector.

CONCLUSION AND RECOMMENDATIONS

This study examined the impact of data encryption practices Data Security (DS), Access Efficiency (AE), and Encryption Training (ET) on Employee Efficiency (EmpEff) within Deposit Money Banks (DMBs) in Abuja, underpinned by the Technology Acceptance Model (TAM). The findings underscore that data security and encryption training significantly enhance employee efficiency, suggesting that secure and reliable data handling practices empower employees to perform optimally within regulated environments. Conversely, access efficiency alone did not exhibit a significant effect, indicating that improved access mechanisms may need further operational or infrastructural support to influence productivity meaningfully. The study confirms that when employees perceive encryption as both useful (in terms of data protection) and manageable (via adequate training), they are more likely to integrate these practices effectively, leading to enhanced operational efficiency.

In line with the study's findings, several strategic recommendations are proposed for Nigerian Deposit Money Banks:

i. Given the significant impact of data security on employee efficiency, DMBs should consistently invest in advanced encryption and data protection measures. Regular audits

and updates to data security frameworks will not only protect sensitive information but also foster an environment where employees can perform confidently without the risk of data breaches.

ii. Although access efficiency did not directly affect employee efficiency, it remains an essential aspect of data handling. DMBs should aim to support access efficiency through integrated systems that streamline data retrieval within a secure framework. Improvements in technical infrastructure, combined with optimized workflows, may enable access efficiency to contribute more effectively to productivity.

iii. As encryption training had the highest influence on employee efficiency, DMBs are recommended to develop structured, ongoing training programs. Such programs should emphasize practical encryption skills, ensuring employees understand and can effectively use encryption tools in daily operations. Tailoring training to employees' specific roles will enhance their confidence and proficiency in secure data handling, ultimately boosting overall productivity.

These recommendations provide actionable insights for DMBs aiming to enhance productivity through secure and efficient data handling. By aligning data security investments with comprehensive training and infrastructure support, Nigerian banks can optimize employee efficiency in increasingly digital and secure banking environments.

REFERENCE

Al-Harrasi, S., Ibrahim, M., & Ali, A. (2021). Enhancing compliance with data protection through tailored security training programs. *Journal of Information Security*, 10(4), 213-223.

Asemota, E., & Olayemi, S. (2023). Financial system development and banking sector performance in Nigeria. *African Journal of Financial Studies*, 16(1), 120-135.

Azizi, M., & Salman, H. (2023). Risk management and operational efficiency in banking: Insights from Nigerian branches. *International Journal of Risk Management*, 14(2), 145-161.

Ayoola, B., & Odusina, K. (2023). Corporate governance and cost efficiency in Nigerian financial institutions. *African Journal of Business Economics*, 17(1), 61-78.

Boubaker, M., & Larbi, T. (2022). Security measures and operational resilience: A review in the banking sector. *International Journal of Banking Studies*, 13(3), 214-229.

Chen, R., Liu, J., & Zhao, T. (2023). Behavioral intentions in secure banking environments: A European perspective. *European Journal of Banking Management*, 11(2), 98-115.

Darmawan, S., & Sukarno, A. (2022). Technology investments and efficiency gains in Indonesian banks. *Asian Journal of Banking & Finance*, 14(3), 202-219.

Deeb, R., Ahmed, S., & Jabbour, E. (2023). Data access efficiency in financial institutions: A study on operational productivity. *Journal of Financial Operations Research*, 8(1), 45-56.

Eze, C., Nwoye, G., & Udeh, E. (2022). Fraud risk management in Nigerian banks. *Journal of Financial Risk Analysis*, 18(4), 133-147.

Hu, X., Zhang, W., & Chen, L. (2021). Security education and its impact on employee behavior in financial institutions. *International Journal of Cybersecurity*, 12(2), 55-70.

Ikhwan, F., & Thas Thaker, R. (2023). Assessing the role of security measures in Indonesian banking efficiency. *Journal of Asian Banking and Economics*, 12(1), 68-85.

Jackson, R., & Hodgkinson, P. (2023). COVID-19 and organizational stability: The role of data security. *Journal of Organizational Resilience*, 9(3), 201-218.

Jahangir, S., Rahman, A., & Chowdhury, N. (2023). Efficiency in healthcare through improved data access: Insights from Bangladesh. *South Asian Journal of Health Administration*, 6(1), 88-103.

Jaiwani, D., & Gopalkrishnan, A. (2022). Adoption of security technologies in Indian banks and its impact on operational efficiency. *Indian Journal of Financial Security*, 9(2), 152-163.

Kaur, S., Singh, A., & Sharma, P. (2023). Benefits of encryption in financial transactions: A focus on data security. *Journal of Financial Security and Data Protection*, 15(2), 89-103.

Kurniawati, I., & Raharja, R. (2022). Organizational management and its effects on employee efficiency. *Journal of Business & Management Research*, 10(4), 101-115.

Liao, X. (2023). Role of fintech in improving operational efficiency in Chinese banks. *Journal of Financial Innovation and Efficiency*, 11(1), 33-50.

Mustaniroh, N., Alfi, M., & Rahmat, T. (2023). Access efficiency and operational flow in Indonesian food supply chains. *Journal of Supply Chain Management*, 14(1), 20-38.

Mustapha, A. (2022). Data security frameworks in the digital era. *Journal of Information Security Research*, 12(4), 334-349.

Nwankwo, M., & Okeke, L. (2022). Organizational structure and employee productivity in Nigerian commercial banks. *Journal of Management and Business Studies*, 10(3), 205-219.

Okwor, C., & Ibe, O. (2022). Monetary policy and private sector credit in Nigeria: An ARDL approach. *Journal of Financial and Economic Studies*, 15(2), 98-116.

Pampurini, G., & Quaranta, M. (2023). High-tech investments and operational resilience in European banks. *Journal of Banking & Financial Technology*, 15(2), 101-119.

Pearce, C., & Bah, M. (2023). Efficiency in financial data management: An African SME perspective. *African Journal of Business & Technology*, 8(2), 112-129.

Prox, A. (2023). Digitalization and data protection in modern organizations. *Journal of Digital Business*, 14(2), 99-114.

Rahman, M., Hussain, M., & Alam, S. (2023). Cybersecurity in European banks: Enhancing stability and productivity. *European Journal of Cybersecurity and Data Protection*, 9(1), 15-30.

Salemcity, D., & Ali, A. (2023). Artificial intelligence and its impact on operational efficiency in Nigerian banks. *Journal of Banking and Technological Advancement*, 7(1), 77-95.

Shull, S. (2023). Sustainable data practices in digital storage. *Environmental Data Journal*, 9(3), 144-159.

Suryana, D. (2022). Enhancing service delivery and customer satisfaction through employee efficiency in the banking sector. *Journal of Banking Operations and Management*, 14(4), 202-219.

Tamimi, A., & Mansour, R. (2023). Security training and employee productivity: Evidence from UAE banks. *Middle Eastern Journal of Information Security*, 13(2), 88-107.

Ubesie, O., & Chukwu, A. (2023). The role of internal control measures in fraud prevention within Nigerian banks. *Journal of Banking and Financial Control*, 10(2), 55-72.

Ullah, S., & Khan, R. (2023). Determinants of operational efficiency in the banking sector. *Journal of Financial Operations Management*, 17(2), 75-91.

Zeynullagil, M. (2022). The impact of efficient employee management on organizational success. *Journal of Human Resource Management*, 11(4), 55-72.