International Journal of Social Sciences
Vol. 18, No 2, pp. 37 – 51, 2026
ISSN 1119 – 4898 www.ijss.com.ng/index/php/home

INTERNATIONAL
JOURNAL OF
SOCIAL SCIENCES

END-POINT SECURITY PRACTICES AND BLOCKCHAIN INTEGRATION AS PREDICTORS OF CYBERCRIME MITIGATION IN SOUTH-SOUTH NIGERIA.

Ushie Peter Ochiche, Ezikeudu, Chukwudi Charles, John T. Okpa,
Department of Criminology and Security Studies
University of Calabar

Ushie, Hannah Oizamisi
Department of Education, University of Hull

Akpan Emmanuel Mendie*
Department of Educational Foundations,
University of Calabar, Nigeria

DOI: https://doi.org/10.60787.ijss.vol118no2.274

Abstract

Recent observation has shown increased rate of cybercrime incidence in South-South geopolitical zone of Nigeria in spite of the pervasive rate of digital information technologies and services. Based on this observation, this study investigated end-point security practices and blockchain integration as the prediction of cybercrime mitigation in the South-South geopolitical zone of Nigeria. The study adopted a cross-sectional research design. The population of the study was 42,859,300. The sample size of 1,200 respondents was determined using Taro Yamane's (1967) formula. A stratified random sampling technique was adopted by dividing the population into relevant groups and randomly selecting respondents from each stratum to ensure adequate representation of the various categories within the study population. Data was collected with a structured questionnaire designed and developed for the purpose, christened, Cyber Security Technologies and Cybercrime Questionnaire (CSTCQ). Reliability of the instrument was tested with Cronbach Alpha (values between 0.77 to 0.89). Questionnaires were administered with the help of 3 research assistants who used purposive sampling technique to select respondents, who had adequate knowledge about issues pertaining to cybersecurity. Information from the questionnaires were coded and analyzed using the Statistical Package for Social sciences (SPSS) with simple linear regression analysis. The

* **Address of Corresponding Author:** Dr. Akpan Emmanuel Mendie, Department of Educational Foundations, University of Calabar. Email: emmanuelakpan9966@gmail.com, Phone: 08038828403

results of the analysis showed that end-point security practices is a statistically strong prediction of cybercrime mitigation in South-South geopolitical zone of Nigeria. Blockchain integration was also a statistically significant, but weaker prediction of cybercrime mitigation. The study recommended stronger enforceability of end-point security practices and better awareness; the incorporation of blockchain gradually into the sector with proper infrastructure and policy is emphasized.

Keywords: Blockchain integration; Cybercrime mitigation; Cybersecurity; End-point security practices; South-South Nigeria.

Résumé

Des observations récentes ont mis en évidence une augmentation de l'incidence de la cybercriminalité dans la zone géopolitique « Sud-Sud » du Nigeria, malgré la généralisation des technologies et services d'information numériques. À partir de ce constat, cette étude a examiné dans quelle mesure les pratiques de sécurité des terminaux (end-point security) et l'intégration de la blockchain permettent de prédire l'atténuation de la cybercriminalité dans cette région. L'étude a adopté un plan de recherche transversal. La population cible s'élevait à 42 859 300 personnes. Un échantillon de 1 200 répondants a été déterminé à l'aide de la formule de Taro Yamane (1967). Une technique d'échantillonnage aléatoire stratifié a été utilisée : la population a été divisée en groupes pertinents et des répondants ont été sélectionnés au hasard dans chaque strate afin d'assurer une représentation adéquate des diverses catégories de la population étudiée. Les données ont été recueillies au moyen d'un questionnaire structuré conçu spécifiquement pour cette étude, intitulé « Cyber Security Technologies and Cybercrime Questionnaire » (CSTCQ). La fiabilité de l'instrument a été vérifiée à l'aide du coefficient alpha de Cronbach (valeurs comprises entre 0,77 et 0,89). Les questionnaires ont été administrés avec l'aide de trois assistants de recherche ayant recours à un échantillonnage raisonné pour sélectionner des répondants possédant des connaissances suffisantes sur les questions de cybersécurité. Les informations recueillies ont été codées et analysées à l'aide du logiciel SPSS (Statistical Package for the Social Sciences) via une analyse de régression linéaire simple. Les résultats de l'analyse indiquent que les pratiques de sécurité des terminaux constituent un prédicteur statistiquement puissant de l'atténuation de la cybercriminalité dans la zone géopolitique Sud-Sud du Nigeria. L'intégration de la blockchain s'est également révélée être un prédicteur statistiquement significatif, bien que plus faible, de l'atténuation de la cybercriminalité. L'étude préconise une application plus rigoureuse des pratiques de sécurité des terminaux ainsi qu'une meilleure sensibilisation ; elle souligne également la nécessité d'une intégration progressive de la blockchain dans le secteur, appuyée par des infrastructures et des politiques adéquates.

Mots-clés: Atténuation de la cybercriminalité; Cybersécurité; Intégration de la blockchain; Pratiques de sécurité des terminaux; Sud-Sud du Nigeria.

Introduction

The rapid spread of digital technologies has reshaped economic and social life across Nigeria, with the South-South region experiencing steady growth in internet use, mobile connectivity, and digital financial services. Cities such as Port Harcourt, Uyo, and Warri now rely heavily on digital platforms for banking, education, governance, and commerce. This expansion has improved access to opportunities, yet it has also widened exposure to cyber threats that target individuals, institutions, and critical infrastructure.

Globally, the shift toward digital systems continues at a fast pace. Studies by Gupta and Khan, Butt, and Shamshirband (2024) showed that increased reliance on e-commerce, cloud computing, and mobile technologies has expanded the attack surface for cybercriminals. Recent estimates indicated that global retail e-commerce sales reached about 5.8 trillion US dollars in 2023 and may exceed 8 trillion dollars by 2027 (Mouna and Yassine 2024). At the same time, non-cash transactions were projected to grow at about 15 percent annually, driven by digital payment systems (Capgemini Research Institute 2023). These patterns show how deeply digital systems are shaping economic activity.

As digital adoption increases, cybercrime has grown in scale and complexity. Reports from the FBI Internet Crime Complaint Center indicate losses of over 10 billion US dollars in 2022, with more than 800,000 complaints recorded. Data breaches alone cost organizations an average of 4.45 million US dollars in 2023 (IBM). These attacks include phishing, ransomware, identity theft, and system intrusion. Scholars such as Sowmya and Anita and Raymond noted that cybercrime has become more organized and technically advanced, often targeting both financial systems and public infrastructure.

In Nigeria, the situation reflects global trends but with added structural challenges. Despite the enactment of the Cybercrime (Prohibition and Prevention) Act No.17 of 2015, cybercrime incidents remain frequent. Nigeria's ranking among countries with high cybercrime complaints and its position in global cybercrime indices suggest persistent vulnerabilities. Weak enforcement, limited technical capacity, and low public awareness contribute to this problem. In the South-South region, where oil and gas operations, maritime activities, and financial services are prominent, cyber threats can disrupt economic stability and reduce trust in digital systems.

Within the current cybersecurity landscape, scholars have begun to pay closer attention to specific technological and behavioral practices that may influence cybercrime mitigation outcomes. One such area is end-point security practices, which focus on protecting user devices that connect to networks. End-point devices, including laptops, smartphones, automated teller machines, and point-of-sale terminals, are widely recognized as common entry points for cyberattacks due to their direct interaction with users and networks. According to Stallings (2018), vulnerabilities at the device level often arise from weak authentication systems, unpatched software, and poor configuration settings, all of which can be exploited by attackers. Similarly, Behl and Behl (2017) argued that user negligence, such as weak password practices and failure to install updates, increases exposure to malware and phishing attacks.

Empirical studies have linked improved end-point protection measures to reduced cyber risk. For instance, Kumar and Somani (2018) found that implementing strong access control mechanisms, device encryption, and regular software patching significantly reduces the likelihood of unauthorized access and data breaches. In the same vein, Von Solms and Van Niekerk (2013) emphasized that cybersecurity is not only a technical issue but also a human-centered one, where user awareness and behaviour play a critical role in securing end-point devices. In the South-South region of Nigeria, where mobile banking and digital payment platforms are widely used, reliance on personal devices for financial transactions may increase exposure to cyber threats if adequate end-point security practices are not maintained. This raises concern that gaps in user practices and device protection could contribute to persistent cybercrime incidents in the region.

Another variable gaining attention is blockchain integration. Blockchain technology has been widely discussed in the literature as a system that can enhance data security through its decentralized and immutable structure. Nakamoto (2008) introduced blockchain as a distributed ledger system where transactions are recorded in a way that resists modification. Building on this, Casino, Dasaklis and Patsakis observed-that blockchain ensures transparency

and integrity of records, making it difficult for unauthorized actors to alter stored data without detection. These properties have led to its adoption in financial systems, supply chain management, and identity verification processes.

Further studies suggested that blockchain may help reduce certain forms of cybercrime, particularly those involving data manipulation and transaction fraud. Zheng *et al* (2018) noted that the cryptographic structure of blockchain enhances trust in digital transactions by eliminating single points of failure. Likewise, Kshetri (2017) argued that blockchain can improve cybersecurity by providing secure transaction records and reducing reliance on centralized systems that are often targeted by attackers. In Nigeria, emerging applications of blockchain in financial technology and digital identity management indicate its growing relevance. However, adoption remains limited, and its practical impact on cybercrime mitigation within specific regions such as the South-South has not been sufficiently examined.

Despite these theoretical and empirical contributions, the combined influence of end-point security practices and blockchain integration on cybercrime mitigation remains unclear, particularly within the South-South geopolitical zone of Nigeria. Existing studies tend to address cybersecurity from a general or global perspective, with limited focus on how these specific variables interact within localized contexts. This creates a gap in understanding how device-level security behaviours and advanced technologies may jointly shape cybercrime outcomes.

Cybercrime in South-South Nigeria carries broader implications beyond financial loss. Disruptions to digital systems can affect critical sectors such as energy, oil and gas operations, and environmental monitoring systems. Scholars such as Kshetri (2017) have shown that cyber threats can undermine economic activities and weaken institutional systems, while Lewis (2014) noted that attacks on critical infrastructure can disrupt essential services and create environmental risks. In a region like South-South Nigeria, where economic activities are closely tied to natural resource management, cyber disruptions may indirectly affect environmental sustainability through operational failures and poor data integrity.

Given these concerns, there is need to examine how end-point security practices and blockchain integration relate to cybercrime mitigation within this specific context. The researcher considers that while both variables show potential in existing literature, their actual influence in the South-South region remains uncertain and requires empirical investigation.

Statement of the Problem

Cybercrime in Nigeria, particularly in the South-South geopolitical zone, has reached a troubling level where digital advancement now coexists with persistent security threats. Individuals, businesses, financial institutions, and government agencies continue to experience frequent cyber-attacks despite increased awareness and expanding technological infrastructure. The situation is marked by rising cases of phishing, identity theft, ransomware attacks, and unauthorized access to sensitive data. These incidents are not isolated; they affect everyday users who depend on mobile banking, online transactions, and digital communication, as well as organizations whose operations rely on secure information systems. The growing dependence on digital platforms has therefore exposed a wide segment of the population to cyber risks that are both recurrent and increasingly sophisticated.

The problem appears deeply rooted in both technological and human factors. Many users in the South-South region rely heavily on personal devices such as smartphones and laptops for financial and commercial activities, yet these devices often lack basic security measures. Weak passwords, poor update culture, and limited cybersecurity awareness create vulnerabilities that attackers exploit. At the institutional level, gaps in infrastructure, limited technical capacity, and weak enforcement of cybersecurity policies further worsen the

situation. As a result, cybercrime continues to thrive across sectors, affecting economic activities, reducing trust in digital systems, and exposing critical infrastructure to potential disruption.

Several efforts have been made to address cybercrime in Nigeria. The introduction of the Cybercrime (Prohibition and Prevention) Act (2015) marked a significant policy step toward combating cyber threats. Government agencies, financial institutions, and private organizations have also implemented various cybersecurity measures, including awareness campaigns, regulatory frameworks, and technological safeguards. Emerging technologies such as blockchain and advanced security systems have been introduced in some sectors with the aim of improving data protection and transaction security. However, these efforts have not produced the expected level of reduction in cybercrime incidents. Reports of breaches and digital fraud continue to rise, suggesting that existing strategies may be insufficient, poorly implemented, or not adequately tailored to the local context.

This situation creates an urgent need for more targeted and evidence-based approaches to cybercrime mitigation. There is a need to move beyond general cybersecurity discussions and examine specific, practical variables that directly influence cybercrime outcomes. In particular, the role of end-point security practices at the user level and the potential of blockchain integration at the system level require closer empirical investigation. While these approaches are widely discussed in global literature, their actual impact within the South-South Nigeria remains unclear.

This study responds to this gap by examining end-point security practices and blockchain integration as predictors of cybercrime mitigation in the South-South geopolitical zone of Nigeria. The study seeks to generate empirical evidence on how these variables relate to cybercrime outcomes and whether strengthening them can reduce the prevalence of cyber threats.

Hypotheses

1. There is no significant impact of the use of end point security on the mitigation of cybercrime in South-South geopolitical zone of Nigeria.
2. There is no significant impact of the use of block chain on the mitigation of cybercrimes in South-South geopolitical zone of Nigeria.

Literature Review

Recent studies show that cybercrime continues to rise due to weak system defenses, especially at the device level where most attacks begin. Researchers now pay closer attention to end-point security because laptops, smartphones, and other user devices often serve as the first entry point for attackers. End-point security refers to the protection of individual devices connected to a network through tools such as antivirus software, firewalls, encryption, access control, and regular system updates. According to Chandel *et al.* (2019), effective endpoint protection systems can detect, isolate, and remediate threats before they spread across networks, thereby reducing insider threats and unauthorized access.

Their study shows that organizations that deploy layered endpoint protection strategies experience fewer successful breaches compared to those relying on single-layer defenses. Supporting this view, Dargahi *et al*. (2019) explained that many cyberattacks, especially ransomware, exploit vulnerabilities at the user-device level, including outdated software and weak authentication systems. These vulnerabilities allow attackers to execute malicious code, steal data, or lock systems for ransom. The authors emphasized that strengthening endpoint

configurations, enforcing patch management, and implementing behavioural monitoring can significantly reduce the success rate of such attacks.

Connolly and Wall (2019) further noted that increasing sophistication of cybercriminals has shifted attention toward technical countermeasures that operate at the endpoint level, particularly in detecting crypto-ransomware before execution. Their findings indicated that proactive endpoint defenses such as real-time monitoring and anomaly detection help organizations respond quickly and limit damage.

In addition, broader cybercrime management frameworks also recognize the importance of endpoint-level defenses. For instance, a cybercrime incident architecture proposed by researchers in Computers and Security stresses that effective mitigation requires identifying attack entry points and aligning preventive controls with specific threat vectors. Since many attacks originate from compromised devices, endpoint security becomes a key control point in this framework.

Empirical evidence also links poor endpoint security practices to wider organizational risks. Studies (CrowdStrike 2024; Verizon 2024) on cyber incidents show that data breaches often begin with compromised endpoints, leading to financial losses, operational disruption, and reputational damage. Organizations with weak endpoint defenses tend to experience higher exposure to such risks. From the reviewed literature, it is clear that endpoint security plays a direct role in cybercrime mitigation. Strong endpoint protection reduces system vulnerabilities, blocks unauthorized access, and limits the spread of malware within networks. However, most of these studies are based on developed economies and corporate environments, with limited focus on regional contexts such as South-South Nigeria. There is still a gap in empirical evidence on how endpoint security practices among individual users and small organizations influence cybercrime outcomes in this region.

Cybercrime has continued to evolve with increased reliance on digital systems, especially in financial services, identity management, and data exchange. In response, researchers have examined blockchain technology as a possible tool for reducing cybercrime due to its structure and security features. Blockchain refers to a distributed ledger system that records transactions across multiple nodes in a network. Each transaction is time-stamped, encrypted, and linked to previous records, making it difficult to alter without detection. According to Dylan Yaga *et al* (2019), blockchain systems provide data integrity, transparency, and resistance to unauthorized modification, which are critical in preventing fraud and cyber manipulation. Their report explains that once data is recorded on a blockchain, it becomes practically immutable, reducing the risk of data tampering. Supporting this view, Shermin Voshmgir (2020) noted that blockchain eliminates the need for central intermediaries, which are often targets of cyberattacks. By decentralizing data storage and validation, blockchain reduces single points of failure, thereby limiting opportunities for hackers to exploit centralized systems. This feature is especially relevant in financial transactions where fraud and identity theft are common.

In cybersecurity, Moubarak Alazab *et al* (2020) argued that blockchain can enhance security through cryptographic mechanisms and consensus protocols. These mechanisms ensure that only verified transactions are added to the ledger, making it difficult for attackers to inject malicious data. Their study showed that blockchain-based systems can strengthen authentication processes and reduce risks associated with unauthorized access. Similarly, Khaled Salah et al. (2019) explained that blockchain has strong potential in securing Internet of Things (IoT) environments, where cyber threats are prevalent. By using blockchain to manage device communication and data exchange, systems can prevent spoofing, data breaches, and unauthorized control of devices. This suggests broader applications of blockchain in protecting interconnected digital infrastructures.

Empirical studies also showed that blockchain can reduce financial cybercrime. For instance, Samaniego Mayra and Ralph Deters (2019) demonstrated that blockchain-based transaction systems improve traceability and accountability. Since all transactions are publicly verifiable within the network, it becomes easier to detect suspicious activities and prevent fraud. This level of transparency discourages cybercriminal behaviour. Despite these advantages, some studies caution that blockchain is not a complete solution to cybercrime. Atul Kumar *et al*-(2021) pointed out that while blockchain secures data at rest, vulnerabilities may still exist at user endpoints, interfaces, and application layers. Poor implementation, lack of regulation, and limited user awareness can reduce its effectiveness. This indicated that blockchain must be combined with other cybersecurity measures for better outcomes.

From the reviewed literature, blockchain technology tends to have strong potential in mitigating cybercrime through its decentralized structure, cryptographic security, and data integrity features. It can reduce fraud, improve transaction security, and enhance trust in digital systems. However, most existing studies focus on developed economies, with limited empirical research in regions such as South-South Nigeria. There remains a gap in understanding how blockchain adoption in local financial systems, government services, and small-scale enterprises affects cybercrime mitigation

Methodology

The study was conducted in the South-South geopolitical zone of Nigeria. A cross-sectional research design was adopted for the study because data were collected from respondents at a single point in time to determine the relationship between cybersecurity technologies and cybercrime experiences. The population of the study consisted of 42,859,300 respondents. The sample size of 400 respondents was determined using Taro Yamane's (1967) sample size determination formula at a 5% level of significance. However, to improve representativeness and increase statistical power as well as account for possible non-response, the sample size was increased to 1,200 respondents**.** The respondents were selected using the stratified random sampling technique to ensure adequate representation of different states and relevant respondent categories within the South-South geopolitical zone of Nigeria.

Data were collected using a researcher-developed questionnaire titled "Cyber Security Technologies and Cybercrime Questionnaire (CSTCQ)". The instrument was structured into sections measuring cybersecurity technologies and cybercrime-related outcomes. The items measuring the independent variables (cybersecurity technologies) and dependent variable (cybercrime vulnerability/experiences) were rated using a four-point Likert scale of Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD)**.** The responses were coded as follows: Strongly Agree = 4, Agree = 3, Disagree = 2, and Strongly Disagree = 1. Higher scores indicated greater adoption of cybersecurity technologies and stronger perceptions of cybercrime-related conditions. The reliability of the instrument was established through Cronbach's Alpha reliability analysis, with coefficients ranging from 0.77 to 0.89, indicating acceptable internal consistency among the questionnaire items.

Questionnaires were administered to the respondents through purposive sampling method. This method requires the researcher to use her own discretion to decide who to administer the questionnaire to in order to ensure that the questionnaires are administered to the right set of respondents with the prerequisite knowledge to provide answer to the questionnaire items. The researcher employed the help of three research assistants to ensure that the entire questionnaires were adequately administered to the target respondents. Adequate measures were taken to ensure that the entire questionnaires were retrieved from the sampled respondents. The data collected were properly scored and coded for statistical analysis. The

data collected were then analyzed using simple linear regression analysis to examine the relationships between the variables.

Results

Demographic Description of the Study Sample

The data for this study were collected from a random sample of 1200 respondents. Their demographic description was done using frequency counts and simple percentages as presented in Table 1.

Table 1: Distribution of respondents by socio-demographic characteristics, N = 1,200

Demographic variables	Category	N	%
Gender	Male	656	54.7
	Female	544	45.3
Age	26-35yrs	472	39.3
	36-45yrs	326	27.2
	46yrs and Above	402	33.5
Educational level		36	3.0
	No formal Education		
	Primary Education	144	12.0
	Secondary Education	180	15.0
	Tertiary Education	840	70.0
location		400	33.3
	Cross River State		
	Rivers State	400	33.3
	Edo State	400	33.3
Marital status	Single	254	21.2
	Married	690	57.5
	Divorced	182	15.2
	Widow/widower	74	6.2

The results in Table 1 show that 656 (54.7%) were males and 544 (45.3%) females. By Age, 472 (39.3%) were 26-35yrs,326 (27.2%) were 36-45yrs and 402 (33.5) 46yrs and above. By Educational level, 36 (3.0%) were those from no formal education, 144 (12.0%) were those from primary education, 180 (15.0%) were those from secondary education and 840 (70.0%) were those that attended tertiary education. By respondents' location, 400 (33.3%) were those from Cross River state, 400 (33.3%) from Rivers State and 400 (33.4%) were those from Edo State. By marital status, 254 (21.2%) were singles, 690 (57.5%) were married, 182 (15.2%) were divorced/divorcees and 74 (6.2%) were widows/widowers. The sample was thus considered heterogeneous enough for the study.

Hypothesis one: *There is no significant impact of the use of end point security on the mitigation of cybercrime in South-South geopolitical zone of Nigeria.*

To test this hypothesis, simple linear regression analysis was applied with end-point security as the independent variable and mitigation of cybercrime as the dependent variable. The F-ratio test was used to determine the significance of the overall regression model, while the t-test was used to determine the significance of the regression constant and coefficient in predicting the dependent variable. The justification for adopting simple linear regression was

based on the objective of the study, which was to determine whether end-point security significantly predicts cybercrime mitigation.

The variables used in the regression analysis were measured using a continuous composite score derived from a four-point Likert scale questionnaire. Although individual questionnaire items were measured at the ordinal level, the summed mean scores used for regression analysis were treated as interval-level measurements, which is common practice in social science research when multiple Likert items are combined to form composite variables.

End-point security (independent variable) was measured using respondents' ratings on questionnaire items assessing the extent of organizational practices and technologies used to protect endpoint devices from cyber threats. The items covered areas such as endpoint protection software, antivirus and anti-malware solutions, device access control, regular security updates, endpoint monitoring, and threat detection mechanisms. Each item was rated on a four-point Likert scale coded as: Strongly Agree (SA) = 4, Agree (A) = 3, Disagree (D) = 2, and Strongly Disagree (SD) = 1. The scores from the items were aggregated to obtain a composite end-point security score, where higher scores indicated stronger endpoint security practices.

Mitigation of cybercrime (dependent variable) was measured using questionnaire items assessing the extent to which cybersecurity measures reduce cybercrime occurrence and impacts. The items measured indicators such as prevention of unauthorized access, reduction of data breaches, improved detection of cyber threats, reduction of financial losses, and improved organizational response to cyber incidents. The same four-point Likert scale was used: Strongly Agree (SA) = 4, Agree (A) = 3, Disagree (D) = 2, and Strongly Disagree (SD) = 1. The responses were combined to generate a composite cybercrime mitigation score, with higher scores representing stronger perceived effectiveness in mitigating cybercrime. The results obtained from the statistical analysis are summarized and presented in Table 2.

Table 2: Regression of cyber crime mitigation on end point security

R-value = .618			Adjusted R Square = .382		
R Square =.382			Std. Error = 5.92192		
Source of variance	**Sum of Squares**	**df**	**Mean Square**	**F-ratio**	**P-Value**
Regression	25971.122	1	25971.122	740.568	.000
Residual	42012.878	1198	36.069		
Total	67984.000	1199			
Predictor variable	**Unstandardized Coefficient**		**Standardized Coefficient**	**t-test**	**P-Value**
	B	**Std. Error**	**Beta**		
(Constant)	2.770	.856		3.236	.001
End point security	1.543	.073	.618	27.213	.000

*Significant at .05 level P < .05

The results in Table 2 show that an R-value of .618 was obtained, indicating a moderate positive relationship between end-point security and the mitigation of cybercrime. The R-square value of .382 indicates that approximately 38.2% of the variation in the mitigation of cybercrime is explained by end-point security, while the remaining 61.8% is explained by other factors not included in the regression model. The adjusted R-square value of .382 further confirms the explanatory strength of the model.

The F-value of 740.568 with a p-value of .000, which is less than the .05 level of significance, indicates that the overall regression model is statistically significant. Therefore, the null hypothesis was rejected. This means that end-point security significantly predicts the mitigation of cybercrime in the South-South Geopolitical Zone of Nigeria. The regression constant (B = 2.770) indicates the estimated level of cybercrime mitigation when end-point security is held constant or assumed to be zero. When end-point security is introduced into the model, the unstandardized regression coefficient (B = 1.543) indicates that a one-unit increase in end-point security will result in a 1.543-unit increase in the predicted level of cybercrime mitigation.

The standardized regression coefficient (β = .618) shows the relative contribution of end-point security to cybercrime mitigation. The contribution of end-point security was statistically significant (t = 27.213, p = .000 < .05), indicating that stronger end-point security practices significantly improve cybercrime mitigation. This implies that improvements in end-point security are associated with increased effectiveness in mitigating cybercrime.

Hypothesis two: *There is no significant impact of the use of block chain on the mitigation of cybercrimes in South-South geopolitical zone of Nigeria.*

To test this hypothesis, simple linear regression analysis was applied with blockchain technology as the independent variable and mitigation of cybercrimes as the dependent variable. The F-ratio test was used to determine the statistical significance of the overall regression model, while the t-test was used to determine the significance of the regression constant and coefficient in predicting the dependent variable.

The justification for adopting simple linear regression was based on the measurement and purpose of the study. Although the individual questionnaire items were measured at the ordinal level using a four-point Likert scale, the responses were aggregated into composite scores for blockchain technology and mitigation of cybercrimes. The resulting composite scores were treated as interval-level measurements, making them suitable for parametric analysis such as simple linear regression.

Blockchain technology (independent variable) was measured through questionnaire items assessing the extent to which blockchain-based security features are applied for cybersecurity purposes. The indicators included decentralized data storage, transaction transparency, data integrity protection, authentication mechanisms, secure record management, and resistance to unauthorized modification of information. Each item was measured on a four-point Likert scale coded as: Strongly Agree (SA) = 4, Agree (A) = 3, Disagree (D) = 2, and Strongly Disagree (SD) = 1. The scores obtained from the items were summed and averaged to produce a composite blockchain technology score, with higher scores indicating greater application of blockchain security practices.

Mitigation of cybercrimes (dependent variable) was measured through questionnaire items assessing the effectiveness of cybersecurity measures in reducing cybercrime occurrence and consequences. The indicators included prevention of unauthorized access, reduction of cyber fraud, protection of sensitive information, improved detection of cyber threats, and enhanced response to cyber incidents. The items were also measured using the four-point Likert scale coded as Strongly Agree (SA) = 4, Agree (A) = 3, Disagree (D) = 2, and Strongly Disagree (SD) = 1. Higher composite scores represented greater perceived effectiveness in mitigating cybercrimes.

Therefore, the use of simple linear regression was considered appropriate because the study aimed to determine the extent to which blockchain technology predicts mitigation of cybercrimes. The analysis estimated the contribution of blockchain technology to cybercrime

mitigation by examining the regression coefficient, standardized beta value, t-value, F-value, and significance level. The results obtained from the statistical analysis are summarized and presented in Table 3.

Table 3: Regression of the mitigation of cybercrime on blockchain

R -Value =.209			Adjusted R Square =.043		
R Square = .044			Std. Error = 7.36620		
Source of variance	**Sum of Squares**	**Df**	**Mean Square**	**F-ratio**	**P-Value**
Regression	2979.385	1	2979.285	54.908	.000
Residual	65004.615	1198	54.261		
Total	67984.000	1199			
Predictor variable	**Unstandardized Coefficient**		**Standardized Coefficient.**	**t-test**	**P-Value**
	B	**Std. Error**	**Beta**		
(Constant)	32.942	1.013		32.508	.000
Blockchain	-.522	.070	-.209	-7.410	.000

*Significant at .05 level P< .05

The results in Table 3 show that an R-value of .209 was obtained, indicating a weak negative relationship between blockchain technology and the mitigation of cybercrime. The R-squared value of .044 indicates that approximately 4.4% of the total variation in the mitigation of cybercrime is explained by blockchain technology, while the remaining 95.6% is explained by other factors not included in the regression model. The adjusted R-square value of .043 suggests that the model maintains approximately 4.3% explanatory power after adjusting for the predictor variable.

The F-value of 54.908 with a p-value of .000, which is less than the .05 level of significance, indicates that the overall regression model is statistically significant. Therefore, the null hypothesis was rejected. This means that blockchain technology significantly predicts the mitigation of cybercrime in the South-South Geopolitical Zone of Nigeria.

The regression constant (B = 32.942) indicates the estimated level of cybercrime mitigation when blockchain technology is held constant at zero. The unstandardized regression coefficient for blockchain technology (B = -0.522) indicates that a one-unit increase in blockchain technology is associated with a 0.522-unit decrease in the predicted cybercrime mitigation score. The standardized coefficient (β = -.209) shows the relative contribution of blockchain technology to cybercrime mitigation, indicating a weak negative predictive relationship. The effect of blockchain technology was statistically significant (t = -7.410, p = .000 < .05). This implies that blockchain technology significantly contributes to predicting cybercrime mitigation, although the direction of the relationship is negative in this model.

The result suggests that blockchain technology, as measured in this study, significantly predicts cybercrime mitigation, but its contribution is negative. This may indicate that blockchain technology adoption alone may not sufficiently improve cybercrime mitigation without adequate implementation capacity, cybersecurity expertise, regulatory support, and integration with other security measures.

Discussion

The findings show that end-point security has a strong and significant impact on the mitigation of cybercrime in the South-South Geopolitical Zone of Nigeria. The R^2 value of 0.382 indicates

that end-point security explains 38.2% of the variation in cybercrime mitigation, which reflects a substantial contribution. This result aligns with earlier studies that identify end-user devices as common entry points for cyberattacks. For instance, Moubarak Alazab *et al* (2020) reported that weak device-level protection such as poor password practices and outdated software increases exposure to malware and unauthorized access. The present finding supports this position, suggesting that strengthening end-point security measures such as regular updates, antivirus protection, and access control can significantly reduce cyber threats.

The significance of the regression model further confirms that improvements in end-point security directly influence cybercrime mitigation. This agrees with Khaled Salah *et al* (2019), who emphasize that securing devices connected to networks plays a critical role in preventing system-wide breaches, especially in environments where digital transactions are frequent. In the South-South region, where many users rely on personal devices for financial activities, this finding suggests that user-level security practices remain a key factor in controlling cybercrime. The high t-values for both the constant and coefficient also indicate that end-point security is a reliable predictor within the model.

In contrast, blockchain technology shows a statistically significant but weak contribution to cybercrime mitigation, with an R^2 value of 0.044. This means that blockchain explains only 4.4% of the variation in cybercrime mitigation. Although the result is significant, the low explanatory power suggests that blockchain adoption is still limited in its practical impact within the study area. This outcome is consistent with the observations of Dylan Yaga *et al*. (2019), who note that while blockchain offers strong data integrity and resistance to tampering, its effectiveness depends on the level of implementation and integration into existing systems.

The finding also supports Atul Kumar *et al*. (2021), who argued that blockchain alone cannot fully address cybersecurity challenges, especially when vulnerabilities exist at the user or application level. The negative regression coefficient observed in the study may reflect issues such as poor implementation, low awareness, or limited infrastructure supporting blockchain technology in the region. It may also suggest that, in practice, blockchain systems have not yet matured enough locally to produce strong positive outcomes in cybercrime mitigation.

However, the statistical significance of blockchain indicates that it still has potential. This aligns with Shermin Voshmgir (2020), who explained that blockchain's decentralized and transparent nature can reduce fraud and improve transaction security when properly implemented. The implication is that while blockchain is relevant, its current impact in the South-South region remains minimal compared to more immediate and practical measures such as end-point security. The findings suggest that cybercrime mitigation in the study area depends more on practical, user-level security measures than on emerging technologies. End-point security appears to offer immediate and measurable benefits, while blockchain represents a developing solution with future potential. This reinforces the need for a balanced cybersecurity approach that combines strong device-level protection with gradual adoption of advanced technologies.

The findings reveal that blockchain technology has a statistically significant impact on the mitigation of cybercrimes in the South-South Geopolitical Zone of Nigeria. However, the strength of this impact is relatively weak, as indicated by the R^2 value of 0.044. This means that blockchain accounts for only 4.4% of the variation in cybercrime mitigation. While the null hypothesis was rejected due to statistical significance, the low explanatory power suggests that blockchain is not yet a major driver of cybercrime control in the study area.

This outcome reflects the current stage of blockchain adoption in many developing contexts. Studies have shown that blockchain's effectiveness depends largely on the extent of

its integration into existing digital systems. For example, Dylan Yaga*et al*(2019) explained that blockchain improves data integrity and reduces the risk of record tampering through its distributed ledger structure. In theory, this should help reduce cybercrimes such as fraud and unauthorized data manipulation. The present finding supports this theoretical relevance but shows that the practical impact remains limited.

The significant F-value and p-value indicate that blockchain still contributes meaningfully to cybercrime mitigation, even if the effect size is small. This aligns with Shermin Voshmgir (2020), who argued that blockchain systems can enhance transparency and trust in digital transactions. In financial systems, for instance, blockchain can make it difficult to alter transaction records without detection. This feature is particularly relevant in addressing cybercrimes such as financial fraud and identity theft.

Despite these advantages, the negative regression coefficient observed in the study suggests possible challenges in the application of blockchain within the region. This finding may be linked to issues such as low technical capacity, limited infrastructure, poor regulatory frameworks, and lack of awareness among users and institutions. Atul Kumar *et al* (2021) noted that the benefits of blockchain are often undermined when supporting systems are weak or when implementation is incomplete. In such cases, blockchain may not deliver the expected security outcomes.

The weak contribution of blockchain in this study also supports the argument that emerging technologies alone cannot address cybercrime without strong foundational security practices. While blockchain can secure transaction records, it does not prevent attacks that originate from compromised devices or poor user behavior. This explains why its impact is lower compared to end-point security, which directly addresses common entry points for cyber threats.

In practical terms, the finding suggests that blockchain should not be seen as a standalone solution to cybercrime in the South-South region. Instead, its role should be complementary. With increased investment, proper implementation, and supportive policies, blockchain could play a stronger role in the future. For now, its contribution remains limited but significant, indicating early-stage adoption with potential for growth.

Conclusion

This study examined how end-point security and blockchain technology influence the mitigation of cybercrimes in the South-South Geopolitical Zone of Nigeria. The findings show that both variables have statistically significant effects on cybercrime mitigation, though their levels of impact differ.

End-point security emerged as a strong predictor, accounting for a substantial proportion of the variation in cybercrime mitigation. This confirms that securing user devices such as laptops, smartphones, and point-of-sale systems plays a direct role in reducing cyber threats. Blockchain technology also showed a significant effect, but its contribution was relatively small. This suggests that while blockchain has useful features such as data immutability and transparency, its practical impact in the study area remains limited. The low explanatory power points to early-stage adoption, limited infrastructure, and gaps in technical capacity, which may restrict its effectiveness in addressing cybercrime.

The study concludes that cybercrime mitigation in the region depends more on immediate, user-level security practices than on emerging technologies that are not yet fully integrated. However, blockchain still holds promise as a complementary tool if properly implemented and supported by policy, infrastructure, and user awareness.

Recommendations

1. Government agencies, banks, schools, and private organizations should enforce strict end-point security standards. This includes mandatory use of updated antivirus software, regular system patching, strong password policies, and multi-factor authentication.
2. Regular training should be organised for staff, students, and digital service users. The focus should be on safe device usage, phishing awareness, password management, and recognizing suspicious activities.
3. Blockchain should be introduced in phases, starting with sectors where data integrity is critical, such as financial transactions, identity management, and record keeping.
4. Government and private stakeholders should invest in reliable digital infrastructure and clear regulatory frameworks.
5. A coordinated cybersecurity framework should be developed for the South-South region. This framework should combine end-point security standards with emerging technologies like blockchain, ensuring that both preventive and advanced systems work together.
6. Universities, ICT firms, and government agencies should work together to develop locally relevant cybersecurity solutions. This will help bridge the gap between research findings and real-world implementation in Nigeria's digital environment.

REFERENCES

Aga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain Technology Overview*. National Institute of Standards and Technology (NIST).

Alazab, M., Alhyari, S., Awajan, A., & Abdallah, M. (2020). Blockchain technology in cybersecurity: Applications and challenges. *IEEE Access, 8*, 101827–101844.

Behl, A., & Behl, K. (2017). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Capgemini Research Institute. (2023). *World Payments Report 2023: Where is the cash? Accelerate corporate cash management transformation to build value***.** Capgemini.

Campbell, J. L., et al. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis, 65*, 101386.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. *Telecommunications Systems*, 71(2), 1–32.

Chandel, S., Yu, S., Yitian, T., & Zhili, Z. (2019). *Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat*. Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

Choo, K. K. R., et al. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security, 83*, 22–37.

CrowdStrike. (2024). *2024 Global threat report*. CrowdStrike, Inc. https://www.crowdstrike.com/global-threat-report/

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security, 87*, 101568.

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., & Bianchi, G. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques, 15*(4), 277–305.

Gupta, R. A. & Khan, M. A. (2024). Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; 779–786.

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. *Springer*.

Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68–72.

Kumar, A., Liu, R., & Shan, Z. (2021). Is blockchain a silver bullet for cybersecurity? A review. *Journal of Information Security and Applications, 57*, 102646.

Kumar, S., & Somani, A. K. (2018). Security challenges in end-point computing devices. *Journal of Information Security*, 9(3), 145–156.

Lewis, J. A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for IoT security and privacy: The case study of a smart home. *IEEE Access, 7*, 132706–132717.

Samaniego, M., & Deters, R. (2019). Blockchain as a service for IoT. *IEEE International Conference on Internet of Things*.

Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.

Verizon. (2024). *2024 data breach investigations report (DBIR)*. Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir/

Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

Voshmgir, S. (2020). *Token Economy: How Blockchain and Smart Contracts Revolutionize the Economy*. BlockchainHub Berlin.

Yassine M. & Mouna B. (2024). Financial technology investments and their impact on economic growth. *Modern Management Review*. 29(4),55-69

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375.