AJSTME, Volume. 12, Issue 2. 263-274, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

Intrusion Detection System and Biometric Authentication as Predictors of Cybercrime Mitigation in South-South Nigeria

Ushie Peter Ochiche[1], Ezikeudu, Chukwudi Charles[1], Dr. John T. Okpa[1], Ushie, Hannah Oizamisi[2] & Akpan Emmanuel Mendie*[3]
[1]Department of Criminology and Security Studies, University of Calabar
[2]Department of Education, University of Hull
[3]Department of Educational Foundations, University of Calabar
Corresponding Author: emmanuelakpan9966@gmail.com

Abstract

This study examined intrusion detection systems and biometric authentication as predictors of cybercrime mitigation in the South-South Geopolitical Zone of Nigeria. A cross-sectional research design was adopted, with two research questions and hypotheses guiding the study. The accessible population comprised 18,750 ICT professionals, cybersecurity personnel, system administrators, and digital system users in selected organizations. A sample of 1,200 respondents was determined using Taro Yamane's (1967) formula and selected through stratified random sampling. Data were collected using the Intrusion Detection System and Biometric Authentication on Cybercrime Mitigation Questionnaire (IDSBACMQ), validated by experts and tested for reliability, with Cronbach's Alpha coefficients ranging from .77 to .89. Separate simple linear regression analyses were used for data analysis. Findings showed that intrusion detection systems significantly predicted cybercrime mitigation, while biometric authentication had no significant effect. The study recommends vulnerability assessments, penetration tests and system audit conducted at reasonable intervals will establish if the deployed IDS and Biometric systems is working as expected and whether another measure is required or not.

Keywords: Intrusion Detection System, Biometric Authentication, Cybercrime Mitigation, Information Security, South-South Nigeria.

Introduction

The rapid expansion of digital connectivity across the globe has reshaped how individuals, organizations, and governments interact, particularly through online systems that support communication, financial transactions, and service delivery. In Nigeria, and particularly in the South-South geopolitical zone, due to the digitization of operations, a greater dependence has been placed on network-based system (online platform for education, banking, and governmental, health related services and e- commerce (Laghrissi et al., 2021). The downside of this digitally driven development is the increase in the proliferation of new form of criminal activities, commonly known as cybercrimes, including hacking, identity theft, ransomware, phishing and unauthorized system (accesss)which requires robust and adequate measures (Abbaset al., 2022). The increased reliance on these networked systems necessarily necessitates that organizations must implement an effective defense against these cyberattacks and ensure the continued functioning of their online systems.

Cybercrime mitigation has become an integral element of cybersecurity management. Cybercrime mitigation "is the set of proactive, strategic, policy, technical and process initiatives that aims at thwarting potential and successful malicious incidents against an individual, group or system, mitigating the damage they can cause, and responding effectively to incidents" (Bada, Sasse, and Nurse, 2019). It pertains to endeavors to minimize Unauthorized System Access; prevent compromise of private information, diminish financial and operational damages, and upgrade systems in order to

resist cyber-attack (Craigen, Diakun, &Purse, 2019). Within the context of this study, cybercrime mitigation refers to the extent to which organizations are able to protect against cyber threats, detect a security breach, and keep their online systems and digital resources operational and resilient.

In as much as cyber attacks have become increasingly widespread and advanced, it is an urgent concern for both developed and developing nations of the world though the latter appear more vulnerable with their infrastructure challenges, technical skills shortages and lacking security know-how. Cyber security techniques have led to the emergence of technologies such as intrusion detection systems (IDS). Intrusion detection system is a technology, which continually checks the computer network or electronic device for malicious activity and policy violations.

The device either attempts to or does log, report, and potentially block the identified activity (Laghrissi et al., 2021). Within the study,intrusion detection system refers to the extent which organizations implement online programs designed to monitor and protect network and systems. In today's modern warfare against threats to critical IT assets, machine and artificial intelligence-assisted IDS have been found to effectively discover evolving and complex cyber-attacks more so than traditional solutions do (Hernandez-Ramoset al., 2023). In practice, IDS can aid in maintaining security resilience at the network level by observing traffic, checking unusual patterns, and inhibiting penetration. However, IDS are impacted by factors like an overabundance of false alarms, the inability to respond to the emergence of novel patterns, and the difficulty of integration with the extant systems within an enterprise.

Another security approach of great importance used for protecting personal information for the purposes of authentication is the biometric authentication . Biometric authentication refers to mechanisms through which each person is checked according to biological or behavioural (physical human or behavioural features) that uniquely differentiate them from other individuals (facial, fingerprint, signature, voice, iris of the eye and behavioral patterns) (Al-Ghamdi et al., 2022). Different from pass word authentication, biometric authentication is based upon biological identity markers that cannot be easily forged or transferred and used as a means to prevent unauthorized user access to any given digital resources (device or network).

In the context of this study, biometric authentication is defined as the degree to which organizations employ biometric identification technology to manage and verify user identities, and grant access privileges to digital devices or network to protect sensitive digital information. Studies show that Biometric Authentication strengthen Cybersecurity because passwords are weak and most users' passwords have not been collectibles from a hacking group or is used twice and is vulnerable to both phishing Attacks and password cracking (Wagata&Teoh, 2022).

Biometric authenticators such as facial recognitions, fingerprints and voices scanners, are readily becoming commonplace in sensitive environments including banks, telecom, schools, and government as they strengthen authentication practices against security threats than passwords can afford. Nonetheless, security and integrity of biometric technology is faced with challenges regarding user privacy and storage and handling of the biometric data, algorithmic inaccuracy and infrastructure availability especially in developing economies. Intrusions detection system and biometric authentication are interrelated because one aims to identify unauthorized accesses and another helps prevent Unauthorized system access, hence they are likely complementary factors contributing to cybercrime Mitigation. Against this background, the study explores intrusion detection systems and biometric authentication as predictors of cybercrime mitigation in South-South Nigeria, with the aim of generating empirical evidence that may support improved cybersecurity strategies in both public and private digital environments

Problem statement

Cybercrime continues to pose a significant security challenge in Nigeria, particularly as individuals, organizations, and government institutions increasingly depend on digital platforms for banking, education, governance, commerce, and service delivery. Increased online activities offer the best opportunities for economic and social growth, but they also lead to risks of unauthorized entry, theft of personal data, email, online fraud, online blackmail and data theft. Increased cyber attacks leads to lack of security and trust in digital systems, as well as financial loss, operation failure and organizational image problems. The increasing rate of cyber-related crime in Nigeria could be seen with reported, investigation, prosecution and recovery by security agencies.

Over 146,000 cybercrime reports were received via the police platform from law Enforcement since the beginning of 2017 to the year 2025 and several billion Naira recovered from cyber

related offences as reported by Nigeria Police Force National Cybercrime Centre (NPF 2025) in it yearly reports. Moreover Nigeria Police Force, in its reports of 2024 reported to have recover over 8.8 billion by it in the investigation of cybercrime as it prosecuted over 751 individuals of crime. Economic and financial crimes commission also mentioned online fraud and other associated crime that leverage the internet are the major financial crime in Nigeria, that leads to significant economy loss by cyber-crime (Economic and Financial Crimes Commission 2024).

Nigeria government has tried to response to cyber-related-issues with various legislatives like the cybercrime prohibition Act 2015, awareness campaigns and adopting some low level of controls, but still cyber-attacks occur. Persistent rise in unauthorized access, email crime, identity-related crime and online fraud proves that the already in-use measures have not been enough to deal with more advance technology. Also several measures have been taken to prevent, detected and combat these kind of threats on technology-driven systems among these the system that drew much interest of many security research works are; Intrusion Detection System (IDS).

The function of intrusion detection system is to continuously monitor network activity and investigate potential activities for unusual behavior and generate alarms when unusual or potential intrusive activities are detected. It's ability to serve as a response to threat at early stage before severe damages occur has lead most studies to evaluate it's performance, (Laghrissi et al., 2021). Biometric Authentication, on the other hand has been regarded as an alternative security measure in the IT systems in recent time; which identify authentic users by checking personal physical & biological characteristic like fingerprints, iris pattern, or face as their unique means of authentication (Al-Ghamdi et al., 2022), reduces the rely on password thereby increases the security and efficiency.

However, there are limited researches providing empirical evidence of either Intrusion Detection System (IDS) or Biometric Authentication oncyber-crime. There seems to be a significant gap in assessing their ability in reducing the cyber-crime rates especially in South-South Geopolitical region in Nigeria, the few research carried out is primarily focused on technical development/performance and general models rather than focusing on assessing the adoption of such technology for crime Reduction in their operational environments; leaving Organizations with the uncertainty of knowing if these measures have yield results for them.

The problem of this study, therefore, lies in the continued prevalence of cybercrime in the South-South geopolitical zone despite existing cybersecurity measures and the limited empirical understanding of how intrusion detection systems and biometric authentication contribute to cybercrime mitigation. This gap necessitates an investigation into whether these cybersecurity technologies significantly predict cybercrime mitigation in the region.

Literature Review

With increasing dependency on digital platforms in finance, governance, education and other business operations, concern about cybercrime mitigation has risen more than ever. Unauthorized access, identity theft, phishing, ransomware and fraud perpetrated by cyber criminals continues to challenge organizations because attackers always develop new tactics to bypass security systems in the conventional methods of security implementation. As such, the researcher's attention and that of many others have increasingly shifted towards tech-based solutions such as intrusion detection systems (IDS) and biometrics, as means of cybercrime mitigation. Both techniques, though operating at different levels, share a mutual objective that of enhancing security by detecting threats and granting authorized access.

With regards to the impact of IDS, it receives massive attention for its capability in monitoring networks, detecting anomalous activity, and alarming when such behaviour is detected. Empirical evidence broadly agree that IDS aids in cybercrime mitigation as they improve capacity in detecting threats and response time. For example Buczak and Guven (2016), demonstrated that intelligent IDS improved the detection accuracy of malicious activities by analyzing large volumes of network data and recognizing patterns related to network attacks, while Aljawarneh, Aldwairi, and Yassein (2019) also proved thatIDS was more effective at increasing network visibility and response time. However both works show similarities in the fact that both studies demonstrated the prevention capacity of the IDS technology.

More recently, studies on the role of machine learning in IDS enhancement has been emphasized. Ahmad, Mazzara, and Distefano (2021), asserts that machine learning-based IDS have strong capabilities in detecting complex and unknown attacks by learning from historical data, thus confirming that adaptiveIDS tech are more secure that signature-based systems. However other works has revealed demerits related to intelligentIDS such as raising more False Alarms, lack of adequate data set, weak detection capabilities for zero day attacks etc. Thus

overall there is a lack of conclusive statement regarding how intelligent systems may pose entirely secure environment from unknown cyber threats.

Context of African and Nigerian situation provides another dimension which influences the level at which IDS performs; unlike studies from developed regions that are largely concerned with detection accuracy and efficiency of algorithms, African studies are inclined to institutional factors that influences cybersecurity implementation. From South Africa, Mthembu and Ismail (2021), demonstrated that organizations are well aware of need of cybersecurity technologies butface hurdles such as high costs, poor technical capacity, limited infrastructures etc, while Akinyemi, Adewumi and Alese (2020), identified poor security practices, lack of appropriate infrastructures and poor professional capacity as limiting factors to effective cybercrime mitigation in Nigeria. The findings suggest that security technologies are limited by other factors other than their operational abilities.

In Nigeria, it is evident that the uptake of the cyber security technology is gaining momentum, particularly in sectors like banking and telecommunications and government. Works carried out within the Nigerian banking sector have reported that effective security monitoring mechanisms do increase the chances of detecting suspicious actions and prevent exposure to threats. For instance, Oladayo and Adewole (2021), revealed that cybersecurity technologies have been helpful in preventing online financial fraud and safeguarding information integrity among banking organizations, but most works focused only on the financial institutions in Nigeria, thus the general impact of such tech on other organizations have not been fully explored.

The South-South geopolitical zone of Nigeria in particular has shown increased reliance on the digital world; at the same time, the zone faces the challenge of cybercrime mitigation in different sectors including banking, education, government and business organizations. Works like Okon and Ekanem (2022) shows poor awareness and low security practices contributed to increased cyber vulnerability among users of digital technology in this region, same as Udo and Inyang(2023) which noted that weak capacity and poor investment on digital security infrastructure are challenging Nigerian organizations in addressing cyber threats. Though both works reveal poor cybersecurity in the southern region, the extent at which IDS, for instance, contribute is yet to be fully investigated.

Biometric identity as a tool to strengthen personal verification and unauthorized access remains another critical cyber security solution outside threat detection. It works beyond password systems by using individuals' unique physiological or behavioral characteristics, such as fingerprints, facial images, irises, and voice. Jain, Nandakumar, and Ross (2019) noted that biometrics are robust means of authentication because such traits and characteristics cannot be easily mimicked or shared compared to passwords. Kumar, Zhang, and Eldefrawy (2020) also find biometric technology improve overall access controls.

Existing studies have also revealed hybrid approaches between biometrics and other security elements. Yang, Wang, and Ren (2019), demonstrates that the synergy effect between biometrics and other access control mechanisms enhances the overall security in detecting an attacker. This finding confirms the literature which claims effective crime prevention does not rest on security measures but on different security technological devices. However, issues such as privacy, protection of biometric identity, and spoofing attacks remain a challenge for biometric technology implementation. Akhtar and Micheloni (2021) demonstrated that in many cases, attackers have been successful in spoofing the biometric modality, for example through presentation attacks and synthetic biometric traces.

For the Nigerian situation, adoption of biometrics technology is on the increase particularly in the banking sector and telecommunications. The Bank Verification Number (BVN) system used for all financial services is probably the single most widely implemented biometric security system in Nigeria for reducing cyber crime; Adewumi and Akinyemi (2021), reports that biometric systems are helpful in authentication and have helped reduce some forms of digital fraud in Nigeria, but acknowledge weak institutional framework, data protection and infrastructure challenges in Nigeria compared to developed nations.

Comparison of all these studies suggests that while bothIDS and biometric authentication provide different routes of contribution toward cybercrime mitigation, there exists disagreement within the literature on their respective capacities in reducing cybercrime with studies abroad focusing on technology performance, while studies from developing regions (including Nigeria) highlight challenges such as insufficient infrastructure and poor institutional framework. This discrepancy within the body of literature indicates that the existence of the technology alone does not equate to its effectiveness in crime mitigation.

Previous studies are obvious; most of the studies conducted overseas regarding IDS and

biometrics involve experimentation and simulation or evaluate their performances based on statistical metrics, which may not be practical in organizational context. The Nigerian studies adopt predominantly descriptive survey designs and have mostly looked into specific sectors such as the banking industry and telecommunications. None, apart from this research, has investigated various categories of organizations across geopolitical zones using predictive statistical methods to understand the contribution of security technologies on cybercrime mitigation.

Despite growing evidence on the importance of intrusion detection systems and biometric authentication, empirical knowledge remains limited regarding their predictive influence on cybercrime mitigation in the South-South geopolitical zone of Nigeria. Existing studies have not sufficiently examined whether these technologies significantly contribute to reducing cybercrime within the operational realities of organizations in the region. This gap provides justification for investigating intrusion detection systems and biometric authentication as predictors of cybercrime mitigation in South-South Nigeria.

Hypotheses

i. There is no significant impact of the intrusion detection systems on the mitigation of cybercrimes in the study area.

iv. There is no significant impact of the use of biometric authentication on the mitigation of cybercrimes in South-South Geopolitical Zone of Nigeria.

Methodology

The study was conducted in South-South Geopolitical Zone of Nigeria. The research design adopted for the study was cross sectional research design. The target population of the study comprised 18,750 ICT professionals, cybersecurity personnel, system administrators, network administrators, information technology staff, and digital system users in selected organizations across the South-South Geopolitical Zone of Nigeria**.** The organizations included financial institutions, government establishments, telecommunications companies, educational institutions, and business organizations that utilize digital technologies and cybersecurity measures such as intrusion detection systems and biometric authentication.

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.

A 22 item 4 point Likert scale questionnaire titled "Intrusion Detection System and Biometric Authentication on Cybercrime Mitigation Questionnaire (IDSBACMQ)" developed by the researcher was used for data collection. The instrument was face validated and content validated by cybersecurity, ICT and research measurement experts from relevant university departments. The reliability of the instrument was confirmed through Cronbach's Alpha, yielding coefficients ranging from .77 to .89, which were considered satisfactory. The researcher employed the help of three research assistants to ensure that the entire questionnaires were adequately administered to the target respondents. Data were collected systematically to ensures that the response obtained from the selected respondents are correct and that complete information were obtained from the entire respondents. Necessary permit to conduct the survey were obtained from the pertinent administrative bodies and chief executives of each of the targeted organization or institution. A cover letter containing details on the purpose of the research work were sent through appropriate medium, to each and every respondents from the selected sample through their institutions/organizations.

The structured and self-administered questionnaire and was administered personally by the researcher with help of research assistants. The respondent was made to understand the objective of the study, that, their participation is voluntary and cannot either, refuse to respond to questionnaire or with draw their responses at any point, in without any form of penalty, or detriment to their service or position. In addition they were assured of confidentiality of the information's so gathered and solely used for research purpose. The total data collection for the study was for a duration of 4weeks. The Researcher managed and monitored the research team throughout the data collection, collection and return of instrument to minimize the missing data to reasonable extent.

Training were carried out for research assistants with respect to research objectives and plan, questionnaire introduction, explanation of response, ethical considerations and method of response by non-interview question's so as to ensure consistencies. Questionnaire forms with missing variables or response were retrieved with immediate scrutiny. Missing data was resolved by direct follow-up with the respondents where it was found justifiable. The filled and completed questionnaires were subsequently coded, scored, sorted organized

and then analyzed statistically. The data collected were then analyzed using separate simple linear regression analyses to test the predictive influence of intrusion detection system and biometric authentication on the mitigation of cybercrime

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
Demographic description of study sample

Demographic variables	Category	N	%
Gender	Male	656	54.7
	Female	544	45.3
	Total	1200	100.0
Age	26-35yrs	472	39.3
	36-45yrs	326	27.2
	46yrs and Above	402	33.5
	Total	1200	100.0
Educational level	No formal Education	36	3.0
	Primary Education	144	12.0
	Secondary Education	180	15.0
	Tertiary Education	840	70.0
	Total	1200	100.0
location	Cross River State	400	33.3
	Rivers State	400	33.3
	Edo State	400	33.3
	Total	1200	100.0
Marital status	Single	254	21.2
	Married	690	57.5
	Divorced	182	15.2
	Widow/widower	74	6.2
	Total	1200	100.0

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 intrusion detection system on the mitigation of cybercrimes in the study area. To test this hypothesis, the procedure used in testing hypothesis one and two was adopted with intrusion detection system as independent variable and the mitigation of cybercrime as dependent variable. The results are presented in Table 2.

Table 2: Regression of the mitigation of cybercrime on intrusion detection system

R-value =.484			Adjusted R Square = .232		
R Square = .234			Std. Error = 6.59187		
Source of variance	Sum of Squares	Df	Mean Square	F-ratio	p-value
Regression	15927.646	1	15927.646	366.551	.000
Residual	52056.354	1198	43.453		
Total	67984.000	1199			
Predictor variable	Unstandardized Coeff.		Standardized Coeff.	t-test	p-value
	B	Std. Error	Beta		
(Constant)	13.916	.639		21.770	.000
Intrusion detection system	.764	.040	.484	19.146	.000

significant at .05 level P< .05

The results in Table 2 show that an R-value of .484 was obtained, indicating a moderate positive relationship between intrusion detection system and the mitigation of cybercrime. The R-square value of .234 indicates that approximately 23.4% of the variation in the mitigation of cybercrime is explained by intrusion detection system**,** while the remaining 76.6% is explained by other factors not included in the regression model. The adjusted R-square value of .232 further confirms the explanatory strength of the model. The F-value of 366.551 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 intrusion detection system significantly predicts the mitigation of cybercrime in the study area**.**

The regression constant (B = 13.916) indicates the estimated level of cybercrime mitigation when intrusion detection system is held constant or assumed to be zero. When intrusion detection system is introduced into the model, the unstandardized regression coefficient (B = .764) indicates that a one-unit increase in intrusion detection system will result in a 0.764-unit increase in the predicted level of cybercrime mitigation**.**

The standardized regression coefficient (β = .484) shows the relative contribution of intrusion detection system to cybercrime mitigation. The contribution of intrusion detection system was statistically significant (t = 19.146, p = .000 < .05), indicating that the intrusion detection systems significantly improves cybercrime mitigation. This implies that increased deployment and effective utilization of intrusion detection systems are associated with improved capacity to detect, prevent, and reduce cybercrime incidents in the study area.

Hypothesis two: There is no significant impact of the use of biometric authentication on the mitigation of cybercrimes in South-South Geopolitical Zone of Nigeria. To test this hypothesis, the procedure used in testing hypothesis one and two was adopted with biometric authentication as independent variable and the mitigation of cybercrime as dependent variable. The results are presented in Table 3.

Table 3: Regression of the mitigation of cybercrime on biometric authentication

R-value = .011			Adjusted R Square = -.001		
R Square = .000			Std. Error = 7.53270		
Source of variance	Sum of Squares	Df	Mean Square	F-ratio	p-value
Regression	7.667	1	7.667	.135	.713
Residual	67976.333	1198	56.742		
Total	67984.000	1199			
Predictor variable	Unstandardized Coeff.		Standardized Coeff.	t-test	p-value
	B	Std. Error	Beta		
(Constant)	26.219	1.699		15.433	.000
Biometric authentication	-.039	.106	-.011	-368	.713

significant at .05 level P< .05

The results in Table 3 show that an R-value of .011 was obtained, indicating a very weak negative relationship between biometric authentication and the mitigation of cybercrime. The R-square value of .000 indicates that approximately 0.0% of the variation in the mitigation of cybercrime is explained by biometric authentication, while the remaining variation is explained by other factors not included in the regression model. The adjusted R-square value of -.001 further indicates that biometric authentication has no meaningful explanatory contribution to the prediction of cybercrime mitigation in the model.

The F-value of .135 with a p-value of .713, which is greater than the .05 level of significance, indicates that the overall regression model is not statistically significant. Therefore, the null hypothesis was retained. This means that biometric authentication does not significantly predict the mitigation of cybercrime in the study area. The regression constant (B = 26.219) indicates the estimated level of cybercrime mitigation when biometric authentication is held constant or assumed to be zero. When biometric authentication is introduced into the model, the unstandardized regression coefficient (B = -.039) indicates that a one-unit increase in biometric authentication will result in a 0.039-unit decrease in the predicted level of cybercrime mitigation.

The standardized regression coefficient (β = -.011) shows the relative contribution of biometric authentication to cybercrime mitigation. However, the contribution of biometric authentication was not statistically significant (t = -.368, p = .713 > .05), indicating that biometric authentication does not significantly influence cybercrime mitigation in the study area. This implies that, although biometric authentication shows a negative relationship with cybercrime mitigation in the regression model, the effect is too weak to establish a meaningful predictive relationship. Therefore, variations in biometric authentication practices do not significantly explain changes in the mitigation of cybercrime within the study area.

Discussion

The result of the first analysis showed that intrusion detection system(s) had a statistically significant contribution toward the mitigation of cybercrimes in the South-South Geopolitical Zone of Nigeria. From the result, R value indicates that there is a minimal (weak) positive relationship between intrusion detection system(s)and cybercrime mitigation .i.e., R=0.234 and there is a significant relationship between intrusion detection system(s)and cybercrime mitigation, i.e., R-squared(0.055)=0.055which means that23.4% variation in cybercrime mitigation is due to intrusion detection system(s). The overall regression model was also significant, as testified by F=366.551;P<.05.

This implies that organisations that effectively develop and deploy the usage of Intrusion Detection Systems are much capable of mitigating against cyber crimes. The result of this study supports the proposition of Sommer and Paxson (2019) that IDS improve security by providing increased system visibilty and by increasing system detection of

malicious activity that could cause harm to an organization's data. Through sustained monitoring of network and system activities IDS allows for earlier detection of threats and appropriate counteraction before actual harm is incurred. The significant finding on the prediction of intrusion detection system on cybercrimes should therefore implies to the organisations in South-South Geopolitcal Zone to strengthen and effectively utilise IT services towards improving monitoring and threatening detection tools. In support is a recent study which established the efficacy of IDS in detecting malicious threats, the authors opined that: Data mining and machnie learninnng-enhanced Intrusion Detection Systems have shown substantial promise in Detecting Intricate and Complex cyber security threats (Buczak and guven, 2016); This can also be corroborated with the work of Khraisat et al. (2019), who stressed that one of the most dominant and crucial tools to defend systems against any form of malacious activity which may arise as result of internet compromise and misuse was the Intrustion Detection Systems.

It was revealed that intrusion systemare significant, they do help in detecting unauthorised users within an organisation's internal networks as well as unauthorized access and system compromise. Likewise, Sarker et al.(2020) argues that proactive cyber-security strategies such as the application of threat detection intelligent systems, would ultimately help in detecting threats early enough by enabling individuals to identify weaknesses that could lead to exploitation before or at the initial stage. It is crucial to acknowledge that although intrusion detection system have established a security function of an IT service(s), the contribution of the intrusion detection system as identified in this finding ought to be seen within the perspective of organisational preparation stage. For instance, intrusion detection systems are helpful but require adequate system configuration, installation, network resources and skilled operators to maximize their benefits(Buczak & guven,2016) Hence the overall cyber crime prevention may be facilitated through effective system planning and installation in the South-South Geopolitcal Zone of Nigeria and other parts.

The result of the second analysis showed that biometric authentication had not significant effect and predictor toward the reduction of cyber crime in the South-South Geopolitcal Zone of Nigeria. This conclusion was reached as a result of the very slight negative relationship between biometric authentication and cybercrime mitigation where r= -.000 meaning it contributed for 0.0% in explained variation in the independent variables in cybercrime. Also, an independent analysis showed that biometric authentication had very weak and not statistically significance impact on the prediction of the cybercrimes, ($F = 0.135$; $p > .05$) of the whole model.

The result of this finding is contrary to earlier studies which highlighted biometric technology's benefits in strengthening security and authenticity. Jian, Nandakumar, and Ross (2019), assert that 'because their unique characteristics are harder to counterfeit than passwords'. Similarly Ratha, Connell and Bolle (2020) reported that technology-centred approaches such as biometrics which offers enhanced authentication mechanism for better defence, would make internet safe and secure. The non-significant influence of biometric on the cyberspace should be linked to specific contexts within which such technology was deployed in the study locations. The theoretical promise of biometric authenticity is, no doubt valid; however, the level of deployment and infrastructure to support its secure usage, is of critical relevance.

If the systems are not properly deployed, or maintained; are inadequately supported, or perhaps are not well integrated with the other IT security infrastructure, then the capacity for biometrics to contribute meaningfully to cyberspace security and thus effectively reducing cybercrimes will be minimal. This corroborates the fact that biometric sysytemare always attacked by spoofing, theft and disclosure (Meng et al.,2021). As distinct from the change of password following its stolen, the physiological and behavioural characteristics like eyes, voice, and signature of individuals that could constitute biometric identity cannot be change or cancel if already stolen (Meng et al.,2021), The explanation also aligned with the views of Li and jain, who opined that stronger internet security needs the integration of technology that integrates identity through physiological means into systems with the security mechanisms that provide further layers of defense, such as intrusion detection Systems (IDS). Henceforth The application of some additional defensive layer is required to boost the effective protection of cyberspace using biometrics as part of comprehensive security solution within an organisations that could lead to a significant influence or reduction in crime within the South-South Geopolitical Zone Nigeria and others.

Conclusion

The study investigated the predictive power of Intrusion Detection Systems and Biometrics Security in mitigating the problem of cybercrime in the South-South Geopolitical Zone of Nigeria. From the result, Intrusion Detection Systems, positively predicted cybercrime mitigation within study

environs. This implies that adequate adoption and use of IDS has a tendency to enhance the ability to detect, monitor and response to cyber threats. On the other hand, there was no significant prediction result from the biometrics security.

Despite providing better means to verify identities and can possibly lead to restricted unauthorized access, biometrics systems was found not to significantly predict cybercrime mitigation in the area. Factors like non-integration of the technology, inadequate infrastructure, use and the management practices adopted, may be a cause of non significance. The finding concludes that effective cybercrime mitigation in the region must take account of holistic cyber security architecture using not just the technology but as well as effective management, in the area of security as Intrusion Detection Systems is an effective security device that improves response and prevention, while Biometrics should be enhanced by integrating it with complementary measures, like the use of encryption technology, endpoint security, multi factor authentication and continuous surveillance. The study is therefore beneficial in that it offers an addition to cyber security knowledge in offering empirical findings concerning the predictive strength of some technologies in the region, where the literature is still quite limited, with a proof that not every security technology offers the same results in different context.

Recommendations

1. Considering that IDS has predicted cybercrime mitigation so well, organizations should endeavor to have sound IDS solutions that is managed by skilled cybersecurity individuals whose function will be to manage alerts, analyze threats and respond immediately to any security incidents detected.
2. Despite the fact that biometric authentication did not predict cybercrime mitigation remarkably well in the study area, an improvement on identity assurance role of Biometric systems can be ensured by combining its usage with other security approaches including; multi factor authentication, encryption, data security/access controls.
3. Regular cybersecurity awareness trainings should be conducted to the IT personnel/system administrator on security system implementation, administration and maintenance.
4. Vulnerability assessments, penetration tests and system audit conducted at reasonable intervals will establish if the deployed IDS and Biometric systems is working as expected and whether another measure is required or not.
5. Security awareness agencies and all cybercrime stakeholders must also come up with relevant policies, guides, and awareness measures for organizations, emphasizing on responsible deployment of security technologies, improved compliance with security standards and effective inter-organizational collaboration for cybercrime prevention.
6. Organizations must ensure a comprehensive cyber security strategy is in place where by Intrusion detection Systems will be combined with Biometric Authentication.

References

Adewumi, A. O., &Akinyemi, I. O. (2021). Biometric systems and financial security in Nigeria. *Journal of Information Security and Applications*, *58*, 102712.

Ahmad, Z., Mazzara, M., &Distefano, S. (2021). Intrusion detection systems for Internet of Things: A survey. *Future Generation Computer Systems*, *123*, 247–263.

Akhtar, Z., &Micheloni, C. (2021). Biometric spoofing attacks and countermeasures: A review. *IEEE Access*, *9*, 164245–164265.

Akinyemi, B., Adewumi, A. O., & Alese, B. K. (2020). Cybersecurity challenges and solutions in Nigeria: A review. *Journal of Cyber Security Technology*, *4*(4), 245–263.

Al-Ghamdi, A. S., Abdelkader, G. B., & Boudraa, M. (2022). Biometric authentication systems: A review of current technologies, challenges, and future directions. *IEEE Access*, *10*, 119502–119523.

Aljawarneh, S., Aldwairi, M., &Yassein, M. B. (2019). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152–160.

Asiegbu, B. C., Ikerionwu, C. O., &Ajanwachuku, N. C. (2019). *An intrusion detection system using support vector machine and infinite latent feature selection approach*. African Journal of Computing & ICT, 12(3), 74–84.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 1–10.

Barros, A., Resque, P., Almeida, J., Mota, R., Oliveira, H., Rosário, D., &Cerqueira, E. (2020). *Data improvement model based on ECG biometric for user authentication and identification*. Sensors, 20(10), 2920. https://doi.org/10.3390/s20102920

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21. https://doi.org/10.22215/timreview/835

Economic and Financial Crimes Commission. (2024). *EFCC highlights growing threat of cybercrime and internet fraud in Nigeria*. Economic and Financial Crimes Commission.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Gehrmann, C., Rodan, M., &Jönsson, N. (2019). *Metadata filtering for user-friendly centralized biometric authentication*. EURASIP Journal on Information Security, 2019(7)

Giełczyk, A., Choraś, M., Varadarajan, V., Kommers, P., Piuri, V., &Subramaniyaswamy, V. (2020). *Intelligent human-centred mobile authentication system based on palmprints*. Journal of Intelligent & Fuzzy Systems, 39(6). https://doi.org/10.3233/JIFS-189142

Hernandez-Ramos, J. L., Oliveira, A., & Bernabe, J. B. (2023). Machine learning approaches for intrusion detection systems: Challenges and opportunities in cybersecurity. *Computers & Security, 127*, Article 103098.

Jain, A. K., Nandakumar, K., & Ross, A. (2019). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters, 79*, 80–105.

Kumar, N., Zhang, Y., &Eldefrawy, M. (2020). Biometric authentication for secure communication systems. *IEEE Communications Magazine, 58*(3), 76–82.

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing, 22*, 949–961. https://doi.org/10.1007/s10586-017-1117-8

Laghrissi, F. E., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data, 8*, Article 65. https://doi.org/10.1186/s40537-021-00448-4

Laghrissi, F. E., Douzi, S., Douzi, K., &Hssina, B. (2021). *Intrusion detection systems using deep learning approaches*. Journal of Big Data, 8(65). https://doi.org/10.1186/s40537-021-00448-4

Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., & others. (2021). Deep learning-based intrusion detection systems: A systematic review. *IEEE Access, 9*, 101574–101599. https://doi.org/10.1109/ACCESS.2021.3097247

Leevy, J. L., &Khoshgoftaar, T. M. (2020). *A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 big data*. Journal of Big Data, 7(104).

Nigeria Police Force National Cybercrime Centre. (2024). *National Cybercrime Centre e-reporting portal: Cybercrime reporting and enforcement statistics*. Nigeria Police Force.

Nigeria Police Force. (2025). *NPF cybercrime unit recovers N8 billion, recognized as best in Africa*. Nigeria Police Force.

Ratha, N. K., Connell, J. H., &Bolle, R. M. (2020). Biometric authentication: Security and privacy considerations. *IEEE Security & Privacy, 18*(2), 56–64.

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2019). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50.

Singh, A., & Singh, K. (2020). Role of biometric authentication in securing critical infrastructure. *International Journal of Critical Infrastructure Protection, 28*, 100341.

Sommer, R., &Paxson, V. (2020). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.

Tolosana, R., Gomez-Barrero, M., Busch, C., & Ortega-Garcia, J. (2020). *Biometric presentation attack detection: Beyond the visible spectrum*. IEEE Transactions on Information Forensics and Security, 15, 1261–1275. https://doi.org/10.1109/TIFS.2019.2934867

Wagata, T., & Teoh, A. B. J. (2022). Biometric authentication: Recent advances, challenges, and future perspectives. *IEEE Access, 10*, 105374–105390.

Yang, W., Wang, S., & Ren, J. (2019). Enhancing security through multi-factor biometric authentication systems. *Future Generation Computer Systems, 92*, 512–525.

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2019). *Building an efficient intrusion detection system based on feature selection and ensemble classifier*. arXiv preprint arXiv:1904.01352.