INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

Assessing the Efficiency of Contemporary Cybersecurity Protocols in Nigeria

[1]Oyetunde Christian Oyedeji., [2]Mubarak A Moronkunbi., [3]Adebayo Adeyinka Victor., [4]Popoola Olusegun Victor

[1]BlueSky Citadel 193 Crayford Rd. London

[2]MuVio Solutions Ltd, Old Lagos Road Ibadan Oyo state Nigeria.

[3]Electrical Department, University of Johannesburg, South Africa

[4]National Institute for Policy and Strategic Studies

DOI: https://doi.org/10.51583/IJLTEMAS.2024.130707

Received: 09 June 2024; Revised: 28 June 2024; Accepted: 02 July 2024; Published: 29 July 2024

Abstract: This study evaluates the effectiveness of contemporary cybersecurity protocols in Nigeria, focusing on their efficiency and application within the local context. Cybersecurity is essential in safeguarding sensitive data against theft and unauthorised access, especially as Nigeria experiences growth in online services such as e-commerce and e-banking. The research examines the usability and economic viability of modern security measures like SSL, TLS, and cryptographic protocols. It highlights the challenges of implementing these protocols in Nigeria due to high operational costs and limited local expertise. The paper also discusses Nigeria's legal framework, including the Cybercrime Act of 2015 and the efforts by governmental bodies like NITDA to enhance cybersecurity. Case studies of recent cyber-attacks illustrate the evolving threat landscape and the critical need for robust cybersecurity strategies. The study concludes with recommendations for improving Nigeria's cybersecurity infrastructure through better regulation, increased awareness, and adopting emerging technologies like blockchain and quantum computing. The research aims to bolster Nigeria's cybersecurity posture and promote safer digital environments by addressing these issues.

I. Introduction

Stealing and intruding on sensitive data are two of the most widespread threats. Secure Sockets Layer (SSL), a web-based secure packet model, and public critical infrastructure with its application in HTTPS were designed for confidential data safety (Dastres & Soori, 2020; Khan et al., 2022; Ibrahim; Kumar et al., 2024). A majority of these modern security measures have safeguards. Stealing and intruding are both avoided by these security measures. Conversely, to thrive in an always-changing digital world of business, the selection of efficient security measures should be continuously analysed. Moreover, there is absolute confidence that investments should not bring specious profits through a waste of operational resources. Hence, contributions have been made by other researchers on the appraisal of these contemporary cybersecurity measures or equivalents by proposing technologies that minimise commercial costs and impacts. This paper presents an open alternative that assesses the efficiency of modern cybersecurity protocols in a graspable manner. Technology has been incorporated into various operations in every part of the globe. These operations often depend on network services to aid data exchange and storage in attaining desired results. Several network security measures were created due to our reliance on these network services. These security measures were produced to halt unauthorised and deceitful activities such as interruption, eavesdropping, misrepresentation, denial of service, and unauthorised access. However, very few of these measures were implemented due to the fear of increasing operational costs. Most known network services resort to applying basic security measures and protocols in performing sensitive operations. The information delivered through the network channel is left open when sending tools to use these unsecured network services to prevent them from being exposed to attacks or compromise (Dastres & Soori, 2020; Khan et al., 2022; Ibrahim; Kumar et al., 2024).

II. Background and Rationale

Efficiency is a concept used in economics to describe the state of an entity making the most use of the resources allocated to it (Ode-Martins, 2021). Efficiency in the use of cybersecurity residency is determined by the fact that funds are being utilised to secure and maintain the security in cyberspace, which is adequate and proportionate to the security provided (O'Brien et al., 2024). So many protocols are available in the open literature that promise to secure cyberspace. However, because of their usability problems, these protocols often deter individual use (Ugbe, 2021). For the efficient and successful deployment of these services, it is paramount to investigate the usability of contemporary security protocols. Because usability is never a priority, these protocols are often constructed to be secure rather than usable, even though it is known that their deployment would involve users (Igbinovia & Ishola, 2023). It is interesting to investigate these interfaces because the return on the investment of implementing a security protocol in terms of user trust and confidence would be diminished if it is not usable during deployment.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

The exponential usage of technology has characterised the 21st century to make life easier. No area of life has profited more from this than ICT's continuous development and deployment. The widespread use of mobile phones and internet services has permeated every facet of human life. Security in deploying and using ICT is often characterised by cybercrime and internet malpractices. Because of unchecked and unregulated usage, the subsequent abuse and illegal use of ICTs has led to the development and deployment of cybersecurity, especially in securing internet-based services. As the usage and industrialisation of ICT continue to be exploited and developed, cybersecurity protocols are also developed to improve security in cyberspace. In Nigeria, online e-commerce and e-banking services are gradually becoming popular. The loss of financial resources and the trust deposited in e-commerce due to illegal access and pilfering of customer data often discourages the use of online e-commerce services. For every successful electronic transaction, the reputation of Nigeria's e-commerce system and the confidence posed in the use of such a system is enhanced. Because of the large amount of data processed and transmitted during an electronic transaction, the subsequent loss when such data is illegally accessed inevitably presents a significant barrier to its widespread usage and development. Individuals and organisations are often unwilling to use services that are not guaranteed.

Research Objectives

To assess secure systems, we aim to hit the sweet spot where the system cannot be breached too quickly, and the cost of managing the system remains low. However, choosing which security solution to adopt for any system is critical to these goals (Adisa, 2023). Opting for a secure solution that comes at a cost much higher than expected is not economical while opting for a security system that can break easily will lead to disaster (Oladipo et al., 2024). This research proposes to answer a fundamental question in cybersecurity: How do we assess a security system? Assessing a security system involves safeguarding the system's integrity, the privacy of its users, and the system resources and considering protocols for remotely accessing and managing the system to deliver on its business case (Daniels, 2023). We believe that the throughput of remotely accessed information systems should not suffer too much because of securing the system; otherwise, the accessed information will not be delivered promptly to users who need to commence actions based on the accessed information (Abrahams et al., 2024). Security efficiency is now taken very seriously as both businesses and governments are getting informed about cyber threats. Countries are lining up to design and implement protocols that will lead to sustained peace from the actions of hacker groups and individuals delving maliciously into the cyber world and causing harm. Nigeria recently moved to the next level of cybersecurity awareness when the Central Bank of Nigeria (CBN) exercised to ensure Nigeria's commercial banks were appropriately secured from attack. Though it is expected that the banks would not be too forthcoming when it comes to their standing in connection to the tests they carried out, the fact that the tests were carried out at the first instance might become a detriment to the ability of attackers to consider our financial sector as a soft target.

Scope and Limitations

This thesis's scope is cybersecurity research, emphasising communication protocols, data exfiltration, and covert and botnet infrastructures (Obono & Tawo, 2022). The goal is to understand the cybercriminal mind, its tools, and how the artefacts work. Such in-depth knowledge is likely to cripple financial benefits, network infrastructure, or access information for more nefarious activities (Heino et al., 2022). The research studies appropriate security protocols, Cisco routers, and possibly redesigning of the Internet for improved performance and increased security (Bang et al., 2022). The report contains the test results, gathered network protocols, network traffic metadata, comprehensive examples, detailed explanations, and sometimes step-wise screenshots (Krishnan et al., 2021). The exponential growth of cybersecurity threats coincides with the provision of required infrastructure and technical expertise. This broad approach examines evolving security, socio-economic, and ethical issues. The human domain has been included, although behaviour-based security is not within the scope of this thesis. This thesis focuses more on technology leadership, innovation, and cybersecurity. The aim is also to increase awareness among policymakers, individuals, and security professionals regarding the evolving threat. The research is conducted to understand policy and security shortcomings so that necessary changes can be made. Formal ethical framework recommendations were beyond the scope of this research. They require more profound ethical implications and further exploration across national and international perspectives. Results also show that different APTs may be able to use a covert channel for C&C and data exfiltration. Networks with suitable network security devices seem to reduce C&C communication.

III. Cybersecurity Landscape in Nigeria

Many nations attempt to safeguard their national cyber-territory by crafting and implementing several laws to combat and arrest potential and actual cybercriminals (Izevbuwa & Ngwoke, 2022). These laws contain both fine impositions and prescribed imprisonment terms for managing and deterring criminals from committing crimes. Prosecutions are high. The institutions regulating the Information and Communication Technologies (ICT) industry and sphere are fully functional in all nations, and Nigeria is no exception. The Nigerian Cybercrime Act 2015 is a statutory enactment of the laws against committing all criminal offences within Nigerian cyberspace and against unauthorised access to computer systems and network devices (Obiefuna et al., 2023). The Nigerian Information and Technology Development Agency (NITDA) functions in the promulgation of rules and guidelines that, on the sanction of the Minister of Communication, have the power of law enforcement. The agency is responsible for developing policies that will promote the growth of institutions within the ICT sphere, such as education, health, governance, and other societal structures (Awhefeada & Bernice, 2020).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

The cybersecurity landscape in Nigeria is at a critical stage. As diverse online channels become entrenched in the daily running of businesses, an escalation in cybercrimes arises in response to the crime opportunities these pose to potential cyber attackers. Cybercrimes are not just done for criminal hobbies but for commercial purposes. A successful cybercrime disrupts the victim's activities and provides the criminal with monetisable advantages. Thus, Nigeria is fast becoming one of the more critical cybercrime destinations on the Internet. Due to the ease of perpetrating the criminalities of cyberattacks, there are increasing instances of lone wolves or individuals with more expansive networks of associates getting involved in cyberterrorism. They are both locally based and internationally based. Because most cybercriminals are at large internationally, it is always difficult to apprehend and bring their persons to justice (Eboibi, 2020). However, security architectures are not only being improved but methods of curbing and preventing cyberattacks are also being tackled head-on. Implementing several cybersecurity protocols has sought to combat this myriad of crooks indulging in cybercrime.

Historical Overview

This is why every society puts measures in place to protect its critical information infrastructures (CIIs) (KHAUSTOVA et al., 2023). Several cybersecurity protocols are widely available to address the issue of cybersecurity. These protocols could include firewalls, intrusion detection systems, updated antiviruses, cryptography, biometrics, multifactor authentication, the deployment of demilitarised zones, end-to-end encryption, and many other personal privacy tools (Dawson et al., 2021). In this study, the terms "cybersecurity" and "information security" are used interchangeably, representing the protection of any asset, whether physical or electronic, networked or un-networked, from threats violently or aggressively. Hence, cybersecurity is generally expressed as protection from any intentional disruption or unauthorised actions, such as denial of service, data destruction, corrupted data or software commands, loss of confidentiality, espionage or theft, and computer hacking (Malatji et al., 2022). The word internet is becoming a term to be fearful and wary of due to its connotations with hackers, worms, spyware, and an adversary to one's environment on the information superhighway and even within the home. Though the networked environment is dynamic and an effective means of getting businesses to cut operations and maintenance costs, it remains a jungle where consumers and businesses can quickly lose money, months of high-quality research; work can go up in smoke, and individuals, either at home or work, could quickly become completely incapacitated. Consequently, the fear of attack has led to developing and utilising a "technological fortress" known as cybersecurity. Hence, cybersecurity has become an increasingly important aspect of national security due to the advances in cyberweapons along with the proliferation of more sophisticated cyber-attacks (Viganò et al., 2020). In every society, the failure of the cybersecurity posture brings devastating consequences for a nation's economy and its ability to conduct itself as a leader in the international community.

Current Threat Landscape

Nigeria began its trek into cyberspace in 2001, as with many global cyber regions (Awhefeada & Bernice, 2020). Subsequently, a blueprint for national cybersecurity and critical infrastructure protection policies was announced in 2012. However, these policies were not fortified with the execution of the National Cyber Security Act until 2015. 2018, the Cyber Crime Act was established (Abiodun et al., 2020). However, the free reign of cyber criminals continues to inspire attacks such as cyberterrorism, information thefts (including the activities of advanced persistent threat actors), e-frauds, Internet of Things, and ransomware, among others (Adediran, 2021). Recently, a few persistent victims of ransomware attacks have either shut down or gone underground. The threat landscape has continuously evolved, while defender readiness has remained static. Reports from the Nigerian Communications Commission revealed around 93 million internet users in Nigeria, the highest in Africa. While economies of scale may have a positive impact on the cost of connectivity, the exponential increase in internet users serves as an inducement for cybercriminals due to the poor economic status of the country and the willingness of the populace to explore nonconventional ways of earning a living (Richards & Eboibi, 2021). Nigeria's diverse economy, with internet penetration in every sector, including e-government, e-commerce, and online banking, makes the country a beautiful market for cybercriminals. With poor cybersecurity awareness, most Nigerian cybersecurity issues will likely worsen. Cybersecurity readiness includes nation-states, organisations, entrepreneurs, and individuals' collective efforts to secure information and communication infrastructure and practices. Cybersecurity readiness is the capability of a nation to protect against, detect, and respond to cyber threats and vulnerabilities. Recent studies on cybersecurity threats in Nigeria are pretty limited. This paper reviews the current cybersecurity threats and their significant impacts on Nigeria.

IV. Contemporary Cybersecurity Protocols

Contemporary cybersecurity protocols relate to varying degrees of technologies presently in use. Technologies are emerging daily, standing on the shoulders of existing ones. Some contemporary technologies include blockchain, quantum computing, and mobile systems (Baseri et al., 2024). In this case, emphasis will be laid on blockchain and quantum technologies. However, the authors will not lose sight of traditional methods since they still constitute the leading voices locally. According to Coon, the integration of these three—the current dominant, the emergent, and the traditional—will help organisations attain a better alignment between their cybersecurity risks and investments. To other authors, existing traditional approaches are locked within their frameworks, and the creativity to change the formula and governance that are key to surviving, managing major incidents, and adapting to the changing threat modelling is restricted (Liu et al., 2022). Such a school argues that a paradigm shift has opened the doors to quantum-driven cryptography except for monetary gainers who are disinclined to think otherwise (Oliva del Moral et al., 2024). As already mentioned, enterprise organisations in Nigeria are slow to grow around such evolving paradigms

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

and, as such, safeguard their cyberspaces with what they currently obtain. The objective of this paper, amongst others, is to theoretically explain the point, as best as they could, for the embracing of the shift that leads to the use of quantum computing and blockchain technology in creating modern-use safety systems (Bishnoi, 2020).

Overview of Common Protocols

SSL and TLS are cryptographic protocols that provide communications security over a computer network (Oppliger, 2023). They are used for web browsing, email, instant messaging, and voice-over-Internet protocol (VoIP). They are used to secure network traffic and ensure that data passed from one server to another is not eavesdropped (Sheikh & Tariq, 2021). The transmission control protocol (TCP) is a core component of the internet protocol suite located at the transport layer. It provides reliable, ordered, and error-checked delivery of a stream of incoming data, and it is used to prepare for sending messages in packets over internet protocol (IP) (Sayal et al., 2020). Internet protocols are communication protocols that scientists and developers have designed to facilitate the communication process between two or more computers over the Internet. It is responsible for providing all capabilities for a device to use the network links to send and receive packets of data in an organised path that will enable reaching out to the destination (Kumar et al., 2024). Every networked device has a unique identifier computer scientists assign, called the internet protocol (IP) address. It is figuratively the address where packets are meant to be explicitly delivered. This section overviews some joint and contemporary cybersecurity protocols in organisations and governments. It covers Internet protocols, transmission control protocols, simple network management protocols, transport layer security, secure sockets layer, and password authentication protocols. It also explains the TCP/IP stack used in networks.

Strengths and Weaknesses

It is argued that it is only through involvement and endorsement by everyone with a valuable stake in the matters and important issues impacting security and availability of global infrastructure that possible effective and stable cybersecurity policies can be achieved (Möller, 2023). An attempt to compensate for the weaknesses identified in the contemporary cybersecurity frameworks is the Cyber Security Consensus Initiative. It argues for the establishment of a round table to include all the essential players in the security debate, including governments, anti-spam, network providers (high cost of implementing DDoS filtering operations), and other non-spam, non-attack impacted sub-segments of the internet (Syafrizal et al., 2020). However, the strategies and frameworks say very little about addressing the reaction, particularly the compensation of legitimate users impacted by aggressive DDoS filtering (Markopoulou & Papakonstantinou, 2021). The strength of protocols and strategies for cybercrime reduction in Nigeria is that they have now gone a long way in spelling out what governments and organisations should do to control the malicious practice of cybercriminality. However, these did not spell out the steps that network providers' services must take to prevent the network from being exploited by hostile users' intent to launch attacks on other sites (Chidukwani et al., 2022).

V. Case Studies

Superimposing Western ideas on Nigerian problems could compound the issues (Daniels, 2023). Would it not be productive and valuable to compare the situation then? This could have been justified in the past because there was no national interest or people in power did not have access to what the internet could bring. However, with the ongoing national debates on life in virtual communities such as the internet, it can be seen that national values and open participation in a global network are essential after all (Idowu). Many Nigerian first-time internet users are just that and do not have the same feel for the West as the older generation. Therefore, the emotional feelings on technological issues such as borderless crimes are not there yet. However, the biggest problem here is the lack of national infrastructure for detecting cyber fraud and, if detected, enforcing the law (Onumo, 2020). Since it has been argued within this dissertation that contemporary cybersecurity protocols appear not to work as they should because they were developed in the West to suit Western needs, then one way of examining this would be to assess the situation in a country where these protocols are assumed to work problem-free (Adewopo et al., 2024). This approach would provide a comparative perspective that could highlight the mismatches and gaps in applying Western-developed cybersecurity protocols in the Nigerian context, ultimately guiding the development of more locally tailored solutions.

Recent Cyber Attacks in Nigeria

The significant increase in the number of cyber-attacks, including phishing, spam, and cyber-crime, combined with the increasing evolution in the tactics, techniques, and procedures (TTPs) of cybercriminals, necessitates the creation of a scalable, homegrown, and effective cyber threat intelligence architecture that will work on providing accurate, consistent, and timely cyber threat information (Chidume et al., 2021). To do this, we propose the development of a domain-specific language/threat modelling declarative Mission Command System Cyber Threat intelligence platform designed to help respond to cyber incidents. A Mission Command System is defined as a military decision-making process that guides a commander in exercising his role; it is based on a philosophy that empowers subordinates to exercise disciplined initiative in decision-making and the execution of dynamically updated plans (N. Okeke, 2021).

The developed architecture will be structured to succeed by distinguishing, in advance, a set of operations or activities for detecting, informing, and responding to cases of internet-born and network systems incidents. In 2019, Nigeria rose to the cyber-aurora status of the country. This is besides the fact that, since 2011, cyber-attacks in Nigeria have continued to escalate. Some significant instances that made the news include the cyber-attack on the Nigeria Stock Exchange (NSE) in 2011, the United States

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

Federal Bureau of Investigation (FBI) cybercrime bust involving several Nigerians-from Oluwatunmise Obadare led fraud organisation that involved $6 million losses and 17 convictions over Business Email Compromise (BEC) related cyber-attacks in 2019 (D. Chechet et al., 2022). Additionally, 2,804 cybercrime-related cases involving small and medium-sized enterprises (SMEs) were reported, verifying a growing pattern of an increase in cybercriminal activities against SMEs. These incidents made the Small and Medium-sized Enterprise Development Agency of Nigeria (SMEDAN) focus on developing small and medium-scale businesses' cybersecurity resilience capabilities (Agbeyangi et al., 2024).

Response and Mitigation Efforts

A common mechanism to mitigate these threats instead of merely responding to the incidents involves proactive measures. For all private and public organisations in Nigeria, the national cybersecurity policy and strategy have recognised the risks of using cyberspace and the responsibilities of protecting sensitive information (AlDaajeh et al., 2022). This strategy suggests means for improving the existing security policies, strategic and operational security planning, security enhancement of organisational infrastructure, and minimising the exposure, illegal presence, and risk to Nigeria's integrity and national security on networks. It emphasises ensuring the apparatus of awareness, education, and training, independent audit and certification of security, and regular and appropriate participation and adherence to standard international standards and practices (Shopina et al., 2020).

To pursue the cybersecurity strategic goals and national policies, collaborating with other nations and governmental organisations, reviewing and enforcing compliance with laws, standards, and best practices—security and legal measures are essential (Lilli, 2020). Since managing all the identified score requirements is less practicable, the proposed security measures are to be cost-effective, balanced, and determined. It aims to share and execute its national security objectives through cooperative action with other countries with shared values, objectives, and purposes. This involves aligning with the national interests of our allies and the principles of national law. Should statutes for cybersecurity only be used when assessed through global policy exchange and coordination of developed frameworks? Using established, legally mandated cybersecurity authorities and capabilities as a basis, new international agreements can be reached, with the flexibility to grow and adjust to dynamic technology and operations (Roshanaei, 2021).

Several cybersecurity policies, strategies, and frameworks are designed and implemented for the country. The 2014 revision of the national cybersecurity policy and strategy recognises the importance of the cyber threats that result from the impact of using modern technology and the global Internet. It maps out a line of action/commitment to address many of the cybersecurity events occurring in the country. A summary of the developed cybersecurity policy and strategy includes the "Draft National Cybersecurity Strategy 2021-2025, National Cybersecurity Policy and Strategy, National Critical Information Infrastructure Protection, Cloud Computing Guideline, Biometric Data Capture Standard, Guidelines for Data Centre and Disaster Recovery, National Information Security Policy and Guideline, and Information System Audit and Certification Guideline." These security measures are planned and deployed to ensure the safe use of cyberspace in the country.

Recommendations and Future Directions

The study has recommended that Nigeria's existing Internet Service Providers (ISPs) should be better regulated. They should be monitored based on speed, connectivity, cost, and response time to service complaints (Ofodile et al., 2024). In addition, the tax regime on ISPs should be reviewed downwards to encourage more entrepreneurs to enter the business (Ololade, 2024). To minimise cybercrime activities during BECE and WASSCE, NECO and WAEC must deploy secure applications suitable for the examination well in advance. When students these days are not fully exposed to the basics of Information Security training, the implication is that they will be prone to risk. This could be facilitated by training trainers and rallying the relevant stakeholders in education, especially teachers, parents, schools, and regulatory agencies, to make basic information security the watchword and control of access and impact of the Web a priority in the educational value system (Olujobi, 2020).

In universities and other higher institutions, these recommendations should be implemented to improve awareness of the significance of information security policies and user compliance with information security and organisational policy within the Nigerian context. The implication of this is increased ICT use by various sectors of the economy in tandem with the objectives of Vision 2020, which aims to move Nigeria from merely being a part of the Telecommunication or Information Technology age to an economy deeply integrated with Information and Communication Technology.

a) All organisations connected to Information Systems and Computer Networks should have an ICT/IS policy. b) The ICT/IS policy should be known to all information systems and computer network users. c) Information security awareness training conducted regularly.

The security architecture of any organisation's ICT is a function of its policy. It encompasses the appropriate organisational guidance and directions to ensure organisational mission and business processes are implemented more effectively using ICT security. As such, institutions should formulate an acceptable ICT/IS policy with provisions for technological and procedural infrastructure facilities within the standard guidelines and procedures that would meet their operational needs without hurdles. To this end, it is therefore recommended that:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

References:

1. Dastres, R., & Soori, M. (2020). Network and web security use a secure socket layer (SSL). International Journal of Computer and Information Engineering, 14(10), 330-333. hal. science
2. Khan, N. A., Khan, A. S., Kar, H. A., Ahmad, Z., Tarmizi, S., & Julaihi, A. A. (2022, May). Employing public key infrastructure to encapsulate messages during transport layer security handshake procedure. In 2022 Applied Informatics International Conference (AiIC) (pp. 126-130). IEEE. researchgate.net
3. Ibrahim, A. (). Secure Socket Layer: Fundamentals and Certificate Verification. engrxiv.org. engrxiv.org
4. Kumar, D. D., Mukharzee, J. D., Reddy, C. V. D., & Rajagopal, S. M. (2024, March). Safe and Secure Communication Using SSL/TLS. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1–6). IEEE. [HTML]
5. Ode-Martins, O. (2021). Challenges of Biometrics Technology in Nigeria to Enhance Information Security: A Qualitative Exploratory Case Study. [HTML]
6. Igbinovia, M. O. & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. Digital Library Perspectives. [HTML]
7. Ugbe, U. M. (2021). Exploring the Security Measures to Reduce Cyberattacks within the Nigerian Banking Sector: A Qualitative Inquiry. [HTML]
8. O'Brien, N., Crespo, R. F., O'Driscoll, F., Prendergast, M., Chana, D., Darzi, A., & Ghafur, S. (2024). Usability and Feasibility Evaluation of a Web-Based and Offline Cybersecurity Resource for Health Care Organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed Methods Study. JMIR Formative Research, 8(1), e50968. jmir.org
9. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security. cuni.cz
10. Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape. International Journal of Science and Research Archive, 11(1), 1959-1967. ijsra.net
11. Daniels, O. (2023). National Cybersecurity Policy and Strategy of Nigeria: A Case Study. [HTML]
12. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. Computer Science & IT Research Journal, 5(1), 1-25. fepbl.com
13. Obono, O. F. E. M., & Tawo, B. P. (2022). Improving Security in A Virtual Local Area Network. Journal of Theoretical and Applied Information Technology, 100(10). jatit.org
14. Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. Cybersecurity. springer.com
15. Bang, A. O., Rao, U. P., Visconti, A., Brighente, A., & Conti, M. (2022). An iot inventory before deployment: a survey on iot protocols, communication technologies, vulnerabilities, attacks, and future research directions. Computers & Security. [HTML]
16. Krishnan, P., Jain, K., Buyya, R., Vijayakumar, P., Nayyar, A., Bilal, M., & Song, H. (2021). MUD-based behavioral profiling security framework for software-defined IoT networks. IEEE Internet of Things Journal, 9(9), 6611-6622. academia.edu
17. Izevbuwa, O. G. & Ngwoke, R. A. (2022). Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations. JL Pol'y & Globalization. academia.edu
18. Obiefuna, O. C., Adibe, E., & Osuagwu, A. (2023). Nigeria's Cybercrime (Prohibition, Prevention, etc) Act 2015 at Eight: Class Act or the New Normal? IRLJ. nigerianjournalsonline.com
19. Awhefeada, U. V. & Bernice, O. O. (2020). Appraising the laws governing the control of cybercrime in Nigeria. Journal of Law and Criminal Justice. researchgate.net
20. Eboibi, F. E. (2020). Cybercriminals and Nigerian Cybercrimes Act 2015: Conceptualising Computers for Cybercrime Justice. JACL. uwc.ac.za
21. KHAUSTOVA, V., TIRLEA, M. R., DANDARA, L., TRUSHKINA, N., & BIRCA, I. (2023). DEVELOPMENT OF CRITICAL INFRASTRUCTURE FROM THE POINT OF VIEW OF INFORMATION SECURITY. Univers strategic, 53(1). idsi. md
22. Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1), 69-75. sciendo.com
23. Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255-279. [HTML]
24. Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. The Ethics of Cybersecurity. oapen.org
25. Abiodun, T. F., Oloyede, A. O., Ademola, O. E., Abah, O., & Kehinde, O. S. (2020). Unlawful killings of civilians by officers of the special anti-robbery squad (SARS) unit of the Nigerian police in southwest Nigeria: implications for national security. African Journal of Law, Political Research and Administration, 3(1), 49–64. abjournals.org

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

26. Adediran, A. O. (2021). Cyberbullying in Nigeria: Examining the adequacy of legal responses. International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 34(4), 965-984. [HTML]
27. Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: Wherein lies the rule of law? International Review of Law, Computers & Technology, 35(2), 131–161. [HTML]
28. Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating Quantum Security Risks in Networked Environments: A Comprehensive Study of Quantum-Safe Network Protocols. [PDF]
29. Liu, Q., Huang, Y., Du, Y., Zhao, Z., Geng, M., Zhang, Z., & Wei, K. (2022). Advances in Chip-Based Quantum Key Distribution. ncbi.nlm.nih.gov
30. Oliva del Moral, J., deMarti iOlius, A., Vidal, G., M. Crespo, P., & Etxezarreta Martinez, J. (2024). Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. [PDF]
31. Bishnoi, B. (2020). Quantum Computation. [PDF]
32. Sayal, M. A., Alameady, M. H., & Albermany, S. A. (2020). Using SSL and TLS Protocols in Providing a Secure Environment for e-commerce Sites. Webology. webology.org
33. Oppliger, R. (2023). SSL and TLS: Theory and Practice. [HTML]
34. Sheikh, S. A., & Tariq Banday, M. (2021). Secure E-mail Communications Through Cryptographic Techniques—A Study. Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2019, 219-235. [HTML]
35. Möller, D. P. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 231-271). Cham: Springer Nature Switzerland. [HTML]
36. Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12(3), 417-432. academia.edu
37. Markopoulou, D. & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The …. Computer law & security review. sciencedirect.com
38. Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access. ieee.org
39. Idowu, O. A. (). Cybercrimes and Challenges of Cyber-Security in Nigeria. academia.edu. academia.edu
40. Onumo, A. O. (2020). A Behavioural Compliance Framework for Effective Cybersecurity Governance and Practice. brad.ac.uk
41. Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). A Comprehensive Analytical Review on Cybercrime in West Africa. arXiv preprint arXiv:2402.01649. [PDF]
42. Chidume, C. G., Oko-Otu, C. N., & Aro, G. C. (2021). State Fragility and Covid-19 pandemic: Implications on the political economy of Nigeria. ncbi.nlm.nih.gov
43. N. Okeke, E. (2021). Pan[dem]ic! Rational Risk Avoidance During a Health Pandemic. ncbi.nlm.nih.gov
44. D Chechet, G., K P Kwaga, J., Yahaya, J., Noyes, H., MacLeod, A., & E Adamson, W. (2022). SARS-CoV-2 seroprevalence at urban and rural sites in Kaduna State, Nigeria, during October/November 2021, immediately prior to detection of the Omicron variant. ncbi.nlm.nih.gov
45. Agbeyangi, A., Makinde, A., & Odun-Ayo, I. (2024). Nigeria's ICT and Economic Sustainability in the Digital Age. [PDF]
46. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. unil.ch
47. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS. Journal of Security & Sustainability Issues, 9(3). lvduvs.edu.ua
48. Lilli, E. (2020). President Obama and US cyber security policy. Journal of Cyber Policy. [HTML]
49. Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. Journal of Computer and Communications. scirp.org
50. Ofodile, O. C., Odeyemi, O., Okoye, C. C., Addy, W. A., Oyewole, A. T., Adeoye, O. B., & Ololade, Y. J. (2024). Digital banking regulations: a comparative review between Nigeria and the USA. Finance & Accounting Research Journal, 6(3), 347-371. fepbl.com
51. Ololade, Y. J. (2024). SME financing through fintech: an analytical study of trends in Nigeria and the USA. International Journal of Management & Entrepreneurship Research, 6(4), 1078-1102. fepbl.com
52. Olujobi, O. J. (2020). Analysis of the legal framework governing gas flaring in Nigeria's upstream petroleum sector and the need for overhauling. Social Sciences. elizadeuniversity.edu.ng