Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 12. No. 3, 2024 Series

Article Citation Format
Malasowe, B.O. (2024): Fundamentals for Developing a National Database to Address Cyber Security Challenges in Nigeria: A Pilot Study. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 12, No. 3. Pp 23-34. www.isteams.net/digitaljournal. dx.doi.org/10.22624/AIMS/DIGITAL/V12N3P3

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 23rd June, 2024
Review Type: Blind Peer
Final Acceptance:27th August, 2024

Fundamentals for Developing a National Database to Address Cyber Security Challenges in Nigeria: A Pilot Study

Malasowe, Bridget Ogheneovo
Department of Computer Science
University of Delta
Agbor, Delta State, Nigeria
E-mail: bridget.malasowe@unidel.edu.ng
Phone No: +2348027539942

ABSTRACT

This pilot study explores the fundamental requirements for establishing a national database aimed at addressing cyber security challenges in Nigeria. With the increasing frequency and sophistication of cyber threats, the need for a centralized repository of cyber-related data has become critical. This research employs systematic literature review approach to explore the fundamentals for developing a national database to address cyber security challenges in Nigeria. The SLR aims to synthesize existing research, identify gaps in the literature, and provide a robust foundation for the pilot study Findings indicate that a national database could significantly enhance threat intelligence sharing, incident response coordination, and policy formulation. Key imperatives identified include the establishment of robust data governance frameworks, collaboration between public and private sectors, and investment in infrastructure and training. The study concludes with recommendations for policymakers to prioritize the development of this database as a cornerstone of national cyber security strategy, ultimately fostering a more resilient digital environment in Nigeria.

Keywords: National Database, Cyber Security, Challenges, Digital Environment, Nigeria

1. INTRODUCTION

The escalation of cyber threats has positioned cyber security as a paramount concern for nations worldwide, particularly in developing countries like Nigeria. The rapid digitization of services, combined with limited security infrastructure, has rendered many sectors vulnerable to cyber attacks (Olufowobi et al., 2021). According to the National Cyber Security Policy of Nigeria (2014), the country faces significant challenges in addressing the complexities of cyber crime, which include data breaches, financial fraud, and identity theft. The situation has been exacerbated by the increasing reliance on digital technologies, making a proactive approach to cyber security more crucial than ever. One viable strategy for enhancing Nigeria's cyber resilience is the establishment of a national database dedicated to cyber security.

Such a database would serve as a centralized repository for threat intelligence, incident data, and best practices, facilitating collaboration among government agencies, private sector organizations, and international partners (Nduka & Okwuosa, 2021). Research indicates that countries with robust cyber security databases can respond more effectively to incidents and develop informed policies based on real-time data (Lindstrom & Lötjönen, 2019). Despite the clear advantages of implementing a national database, Nigeria faces numerous obstacles.

Challenges include inadequate technological infrastructure, insufficient skilled personnel, and a lack of cohesive strategies across different sectors (Abdulazeez et al., 2019). The fragmented nature of cyber security efforts in Nigeria highlights the urgent need for a unified approach to data collection, sharing, and analysis, which a national database could provide.

This pilot study aims to investigate the essential components required for the successful establishment of a national database to address cyber security challenges in Nigeria. This research seeks to provide a comprehensive understanding of the current state of cyber security in Nigeria and identify critical steps toward the development of an effective national database. The ultimate goal is to contribute to a more robust national cyber security strategy that can safeguard Nigeria's digital landscape.

2. LITERATURE REVIEW

The increasing prevalence of cyber threats in Nigeria underscores the necessity for a national approach to cyber security, particularly through the establishment of a centralized database. This literature review examines existing research on cyber security challenges in Nigeria, the benefits of national databases, and the foundational elements required for their implementation.

> *Cyber Security Challenges in Nigeria: Nigeria faces a myriad of cyber security challenges exacerbated by rapid technological advancements and insufficient infrastructure. According to Ogunseye and Abah (2020), the rise in internet penetration has led to increased cyber crimes, including identity theft, financial fraud, and hacking. The Nigerian Cyber Security Policy (2014) identifies key threats such as phishing attacks and ransomware, indicating a pressing need for enhanced protective measures. Moreover, Olufowobi et al. (2021) highlight that many organizations, particularly SMEs, lack awareness and resources to effectively combat these threats, rendering them more vulnerable to attacks.*

The Role of a National Database

A national cyber security database serves as a critical tool for enhancing threat intelligence sharing and response coordination among various stakeholders. Nduka and Okwuosa (2021) emphasize that such a database can facilitate real-time data collection, enabling better analysis of cyber threats and the development of informed policies. Research by Lindstrom and Lötjönen (2019) supports this notion, indicating that countries with centralized databases exhibit improved incident response capabilities and resilience against cyber threats. -Furthermore, the integration of a national database can aid in the standardization of cyber security practices across sectors, promoting collaboration between governmental bodies, private enterprises, and international organizations (Abdulazeez et al., 2019). This collaborative approach is essential in creating a unified front against cyber threats, enhancing overall national security.

> *Foundational Elements for Implementation: To successfully develop a national database for cyber security in Nigeria, several fundamental components must be considered. First, robust technological infrastructure is essential. As highlighted by Afolabi et al. (2020), investment in state-of-the-art technology will facilitate the effective storage, analysis, and dissemination of data related to cyber incidents. Second, human capital development is critical. The lack of skilled personnel in cyber security roles is a significant barrier to effective implementation (Akinyemi & Abereijo, 2021). Training programs and educational initiatives must be established to build a workforce capable of managing and utilizing the national database. Lastly, a clear governance framework is necessary to ensure data privacy, security, and compliance with legal standards. Abdulazeez et al. (2019) advocate for the establishment of policies that outline the roles and responsibilities of stakeholders involved in managing the database, thereby fostering accountability and trust.*

The establishment of a national database to address cyber security challenges in Nigeria is not only feasible but essential. By understanding the current landscape of cyber threats and the benefits of centralized data collection, Nigeria can take significant steps toward enhancing its cyber resilience. Future research should focus on developing a comprehensive implementation strategy that incorporates technological, human, and governance considerations.

Table 1 is the findings of researchers on Cyber Security Challenges in Nigeria, table presents case studies of established database to mitigate cybersecurity issues. Table 3, identified cyber security issues experienced and mitigation approaches taken. Also, table 4 states cybersecurity issues in the banking sector.

Table 1: Identified Cyber Security Challenges in Nigeria

Study	Authors	Year	Purpose	Key Findings	Relevance
Cyber Security Challenges in Nigeria	Abdulazeez, A., Adetunji, A., & Alabi, A.	2019	To provide an overview of cyber security issues facing Nigeria.	Identified major threats, including inadequate infrastructure and lack of awareness.	Highlights the urgent need for a national response.
Cyber Security Frameworks	Afolabi, A., Olorunfemi, F., & Afolabi, S.	2020	To analyze existing cyber security frameworks in Nigeria.	Discussed the weaknesses in current frameworks and suggested integration of a national database for improved data management.	Provides a framework for proposing a national database.
National Cyber Security Policy	Nduka, U., & Okwuosa, I.	2021	To evaluate the impact of Nigeria's cyber security policies.	Found that existing policies lack enforcement mechanisms and comprehensive data strategies.	Points to gaps that a national database could address.
Awareness and Practices	Ogunseye, O. J., & Abah, A.	2020	To assess cyber security awareness among university students in Nigeria.	Revealed low levels of awareness and inconsistent practices in cyber hygiene among students.	Underlines the need for education and a centralized database.
Impact of Cyber Security Policies	Olufowobi, A., Tofade, T., & Olokede, O.	2021	To analyze the effectiveness of cyber security policies in Nigeria.	Suggested that lack of coordination among agencies hinders effective implementation of policies.	Reinforces the necessity for a coordinated national database.

Table 2: Case Studies: National Database to Address Cyber Security Challenges in Nigeria

Case Study	Authors	Year	Objective	Key Insights	Relevance
National Cyber Security Strategy	Federal Government of Nigeria	2014	To establish a framework for enhancing national cyber security.	Emphasized the need for a centralized database for incident reporting and data sharing among agencies.	Highlights the necessity of a national database.
Nigerian Cybercrime Reporting System	National Information Technology Development Agency (NITDA)	2018	To create a system for reporting and analyzing cyber incidents.	Implemented an online platform that collects data on cyber incidents, but lacked comprehensive integration.	Demonstrates the groundwork for a national database.
Cyber Security Capacity Building	African Union	2020	To enhance regional cooperation in cyber security efforts.	Recommended establishing national databases as part of a broader strategy to combat cyber threats.	Supports the idea of a national database in Nigeria.
Cyber Security Policy Review	NITDA	2021	To evaluate the effectiveness of existing cyber security policies.	Found that inadequate data collection methods hinder policy effectiveness, calling for a national database.	Identifies gaps that can be filled by a national database.
National Cyber Security Awareness	Nigerian Communications Commission	2023	To improve public awareness of cyber security issues.	Suggested creating a national database to track public awareness initiatives and their effectiveness.	Reinforces the need for data collection and analysis.

Table 3: Cyber Security Issues in Nigerian Databases

Database Name	Cyber Security Issues	Mitigation Measures	References
Nigerian Cybercrime Reporting System (NCRS)	- Data breaches - Inadequate security protocols - Public awareness deficiencies	- Implement strong encryption - Regular security audits - Awareness campaigns	Abdulazeez, A., Adetunji, A., & Alabi, A. (2019).
National Identity Database (NID)	- Identity theft - Insufficient data protection	- Biometric verification - Collaboration with cybersecurity agencies - Regular infrastructure updates	Afolabi, A., Olorunfemi, F., & Afolabi, S. (2020).

Database Name	Cyber Security Issues	Mitigation Measures	References
Bank Verification Number (BVN) Database	- Phishing attacks - Insecure transactions	- Two-factor authentication - Continuous monitoring - Public education on phishing	Nduka, U., & Okwuosa, I. (2021).

Table 4: Cyber Security Issues in Nigerian Bank Databases

Database Name	Cyber Security Issues	Mitigation Measures	References
Bank Verification Number (BVN) Database	- Identity theft - Phishing attacks - Insecure transactions	- Implementation of two-factor authentication - Continuous monitoring of transactions - Public awareness campaigns on cyber hygiene	Abdulazeez, A., Adetunji, A., & Alabi, A. (2019).
Automated Teller Machine (ATM) Database	- Skimming attacks - Data breaches	- Use of EMV chip technology - Regular software updates - Customer education on ATM safety	Afolabi, A., Olorunfemi, F., & Afolabi, S. (2020).
Core Banking System (CBS)	- Insider threats - Malware attacks	- Regular security training for staff - Deployment of anti-malware solutions - Incident response plans	Nduka, U., & Okwuosa, I. (2021).

3. METHODOLOGY

This section outlines the systematic literature review (SLR) methodology employed to explore the fundamentals for developing a national database to address cyber security challenges in Nigeria. The SLR aims to synthesize existing research, identify gaps in the literature, and provide a robust foundation for the pilot study. The primary objectives of the SLR are: To identify and analyze existing literature related to cyber security challenges in Nigeria. To examine studies focusing on the establishment of national databases for cyber security.To synthesize findings that inform the development of a national database specific to the Nigerian context.

3.1. Inclusion and Exclusion Criteria

The following criteria were established to guide the selection of literature:

- **Inclusion Criteria:** Peer-reviewed journal articles, conference papers, and government reports published from 2000 to 2024.
- Studies addressing cyber security issues in Nigeria or relevant case studies from similar contexts.
- Research focusing on the development or implementation of national databases for cyber security.

- **Exclusion Criteria:**

- Articles not available in English.
- Non-peer-reviewed sources, such as blogs or opinion pieces.
- Studies that do not provide empirical evidence or relevant theoretical frameworks.

3.2. Search Strategy

A comprehensive search strategy was developed to identify relevant literature. The following steps were undertaken:

- **Database Selection:** Multiple academic databases were searched, including Google Scholar, JSTOR, IEEE Xplore, Scopus, and PubMed.
- **Keyword Selection:** A combination of keywords and phrases was used, such as "cyber security challenges in Nigeria," "national database for cyber security," "data protection in Nigeria," and "cyber security frameworks."
- **Search Execution:** Searches were conducted using Boolean operators (AND, OR) to refine results, and the search was limited to publications from 2000 to 2024.

3. 3 Data Extraction

Following the initial search, the relevant articles were screened based on the inclusion and exclusion criteria. The remaining studies underwent a detailed data extraction process, which involved:

- **Bibliographic Information:** Recording details such as authors, publication year, title, and source.
- **Study Characteristics:** Summarizing key aspects such as study objectives, methodology, findings, and relevance to the research topic.
- **Thematic Analysis:** Identifying themes and patterns in the literature related to cyber security challenges and the establishment of national databases.

3.4. Quality Assessment

To ensure the reliability and validity of the included studies, a quality assessment was performed using established criteria. This involved evaluating:

- **Research Design:** Assessing the appropriateness of the research design used in the studies.
- **Methodological Rigour:** Evaluating the robustness of the methods employed for data collection and analysis.
- **Relevance and Contribution:** Determining the significance of the study's findings to the broader field of cyber security in Nigeria.

The systematic literature review methodology deployed for this research topic provides a structured approach to gather and synthesize existing knowledge on cyber security challenges and the potential for a national database in Nigeria. By following a rigorous process, this SLR aims to contribute valuable insights that can inform the development of an effective cyber security framework in the Nigerian context.

4. RESEARCH FINDINGS

The findings of this pilot study are as outlined below:

1. **Need for Centralized Data Management:** The study identified a significant need for a centralized national database to streamline data management across various sectors, enhancing coordination and response to cyber security threats.
2. **Current Gaps in Cyber Security Frameworks:** Existing cyber security frameworks in Nigeria were found to be fragmented and inconsistent, resulting in vulnerabilities that can be exploited by cybercriminals.
3. **Public Awareness and Education Deficiencies:** Findings indicated a lack of awareness and education regarding cyber security best practices among the general public and within organizations, leading to increased susceptibility to cyber threats.
4. **Integration of Advanced Technologies:** The necessity for integrating advanced technologies such as artificial intelligence and machine learning into the national database was highlighted to enhance threat detection and response capabilities.
5. **Collaboration Among Stakeholders:** Effective collaboration between government agencies, private sector entities, and civil society organizations emerged as a critical factor in the successful implementation of the national database.
6. **Regulatory and Compliance Issues:** The research pointed out challenges related to regulatory compliance, emphasizing the need for clear policies and guidelines to govern the operation of the national database.
7. **Resource Allocation and Investment:** Adequate funding and resource allocation were identified as essential for the successful development and maintenance of the national database, ensuring it remains robust against evolving cyber threats.
8. **Data Privacy and Ethical Considerations:** The importance of incorporating data privacy measures and ethical considerations into the design of the national database was underscored to build public trust and encourage participation.

The pilot study concludes that a national database is fundamental for addressing cyber security challenges in Nigeria. By centralizing data management, enhancing public awareness, and fostering collaboration, Nigeria can improve its resilience against cyber threats. Additionally, integrating advanced technologies and ensuring regulatory compliance will be critical for the successful implementation of the database.

5. DISCUSSIONS

The findings of the pilot study underscore the critical importance of establishing a national database specifically designed to combat cyber security challenges in Nigeria. A c**entralized Database Management** is paramount for enhancing coordination among various governmental and private sector entities. A centralized system would facilitate data sharing and improve the efficiency of cyber threat responses. Currently, fragmented data management hinders effective communication and collaboration, resulting in slower responses to emerging threats.

The study highlighted significant gaps in Nigeria's current cyber security frameworks. Many organizations operate without cohesive strategies, leading to vulnerabilities. This lack of a unified approach complicates efforts to protect sensitive data and respond to incidents. Establishing a national database could standardize practices, enabling all stakeholders to adhere to best practices in data security. One of the most pressing issues identified is the lack of public awareness regarding cyber security. Many individuals and organizations are unaware of the risks associated with cyber threats and the measures they can take to protect themselves. Educational campaigns that focus on cyber hygiene and best practices will be essential in fostering a culture of security awareness.

A national database can serve as a central repository for resources and training materials. Technological Integration of advanced technologies such as artificial intelligence (AI) and machine learning into the national database is crucial for enhancing its effectiveness. These technologies can facilitate real-time monitoring, threat detection, and analysis of patterns, enabling proactive measures against potential cyber attacks. However, this requires significant investment in both technology and skilled personnel. Collaboration among various stakeholders is vital for the success of the national database. Government agencies, private sector companies, and civil society organizations must work together to share information, resources, and expertise. This collaborative approach can help build a more resilient cyber security environment, where insights and strategies are shared to combat cyber threats effectively.

The study revealed challenges related to regulatory compliance, emphasizing the need for clear policies governing the national database. Establishing robust legal frameworks will ensure data protection and privacy, fostering public trust. Additionally, compliance with international standards can enhance Nigeria's standing in the global cyber security landscape. Adequate funding and resource allocation are critical for the establishment and maintenance of the national database. The Nigerian government must prioritize investment in cyber security infrastructure to ensure the database is equipped to handle evolving threats. This includes not only technological investments but also training and capacity-building initiatives for personnel. Public trust is essential for the successful implementation of any national database. Incorporating data privacy measures into the design and operation of the database will be necessary to encourage participation and compliance from the public.

6. CONCLUSION

This study emphasizes the foundational role of a national database in addressing cyber security challenges in Nigeria. By centralizing data management, enhancing public awareness, fostering collaboration, and ensuring regulatory compliance, Nigeria can significantly improve its cyber security posture. Addressing the identified challenges and implementing the proposed strategies will be crucial for the successful development and sustainability of the national database.

The findings from this pilot study illustrate the urgent need for a comprehensive national database to effectively tackle cyber security challenges in Nigeria. Establishing such a database will serve as a critical foundation for enhancing data management, streamlining communication among stakeholders, and improving the nation's overall cyber resilience. The key conclusions drawn from the study include:

1. **Centralization is Essential:** A national database will facilitate centralized data management, which is crucial for coordinated responses to cyber threats. This centralization will help eliminate fragmentation in current practices, ensuring that relevant data is readily available to authorized entities.
2. **Awareness and Education are Crucial:** The study highlights a significant gap in public awareness regarding cyber security risks. Implementing educational initiatives will be essential to equip citizens and organizations with the knowledge needed to safeguard their data and respond effectively to threats.
3. **Technological Advancements are Necessary:** Incorporating advanced technologies, such as artificial intelligence and machine learning, into the national database will enhance threat detection and response capabilities. Investment in technology and skilled personnel is vital for the effectiveness of the database.
4. **Collaboration is Key:** Effective collaboration among government agencies, private sector stakeholders, and civil society is critical. A multi-faceted approach will enable the sharing of information, resources, and best practices, thereby strengthening the national cyber security framework.
5. **Regulatory Frameworks Must be Established:** Clear regulatory policies governing the operation of the national database are essential for ensuring data privacy and security. Establishing these frameworks will foster public trust and compliance with national and international standards.
6. **Resource Allocation is Imperative:** Adequate funding and resource allocation must be prioritized to develop and maintain the national database. The government's commitment to investing in cyber security infrastructure is necessary to mitigate emerging threats effectively.
7. **Ethical Considerations Cannot be Overlooked:** Addressing ethical concerns surrounding data privacy and protection is critical to building public trust in the national database. Ensuring that ethical considerations are integrated into the database's design and operation will encourage greater participation from citizens.

This research have revealed that the establishment of a national database is fundamental to addressing the complex cyber security challenges facing Nigeria. By centralizing data management, enhancing public awareness, fostering collaboration, and ensuring robust regulatory frameworks, Nigeria can significantly enhance its cyber security posture and resilience. This pilot study serves as a foundational step towards realizing these objectives and safeguarding the nation's digital landscape.

REFERENCES

1. Abdulazeez, A., Adetunji, A., & Alabi, A. (2019). Cyber security challenges in Nigeria: An overview. International Journal of Computer Applications, 182(16), 1-6. https://doi.org/10.5120/ijca2019919667
2. Afolabi, A., Olorunfemi, F., & Afolabi, S. (2020). The impact of technology on cyber security: A Nigerian perspective. African Journal of Cyber Security and Digital Forensics, 1(1), 45-58. https://doi.org/10.1016/j.ajcsdf.2020.06.003
3. Akinyemi, A. & Abereijo, I. (2021). Human capital development and cyber security: A critical review. International Journal of Cyber Security and Digital Forensics, 10(4), 385-398. https://doi.org/10.17781/P001110
4. Lindstrom, H., & Lötjönen, J. (2019). The importance of cyber security databases in national defense. Journal of Cyber Security and Privacy, 1(3), 234-245. https://doi.org/10.3390/jcsp1030017
5. Lindstrom, H., & Lötjönen, J. (2019). The importance of cyber security databases in national defense. Journal of Cyber Security and Privacy, 1(3), 234-245. https://doi.org/10.3390/jcsp1030017
6. Nduka, U., & Okwuosa, I. (2021). Building a resilient cyber security framework for Nigeria: The role of a national database. Journal of Cyber Security and Privacy, 1(2), 123-140. https://doi.org/10.3390/jcsp1020009
7. Olufowobi, A., Tofade, T., & Olokede, O. (2021). Assessing the impact of cyber security policies in Nigeria: A critical analysis. International Journal of Information Management, 58, 102-114. https://doi.org/10.1016/j.ijinfomgt.2021.102314
8. National Information Technology Development Agency. (2021). Cyber security policy review report. Retrieved from NITDA website
9. Nigerian Communications Commission. (2023). National cyber security awareness campaign. Retrieved from NCC website
10. National Information Technology Development Agency. (2018). Nigerian cybercrime reporting system. Retrieved from NITDA website
11. Ogunseye, O. J., & Abah, A. (2020). Cyber security awareness and practices among students in Nigerian universities. Journal of Information Security and Applications, 54, 102-110. https://doi.org/10.1016/j.jisa.2020.102110

12. Olufowobi, A., Tofade, T., & Olokede, O. (2021). Assessing the impact of cyber security policies in Nigeria: A critical analysis. International Journal of Information Management, 58, 102-114. https://doi.org/10.1016/j.ijinfomgt.2021.102314
13. Federal Government of Nigeria. (2014). National cyber security strategy. Retrieved from NITDA website
14. African Union. (2020). Cyber security capacity building: A roadmap for Africa. Retrieved from AU website