World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

A two-tier database architecture framework for combating cyber threats

Aleke Francis Alexander Onyibe [1,*], Glory Nosawaru Edegbe [1], Samuel Omaji [1] and Akinola Samson Olayinka [2]

[1] *Department of Computer Science, Edo State University Uzairue, Nigeria.*

[2] *Department of Physics with Electronics, Edo State University Uzairue. Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 24(01), 1700–1705

Publication history: Received on 14 August 2024; revised on 15 October 2024; accepted on 18 October 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.1.2939

Abstract

The 21st century has witnessed a lot of advancements in science and technology. One may not be wrong to assert that the field of Information and Communications Technology (ICT) and its allied disciplines like Artificial Intelligence (AI) and Nanotechnology have taken the lead as we witness new developments in these areas year by year. The products and services we utilize and enjoy are evidence of the usefulness of this advancement in science and technology. It is worthy of note that the interest of many (both good and bad in the discipline of ICT), is being ignited by the fact that ICT finds its applicability virtually in every area of human endeavor. In this study, we propose a two tier database architecture that employs an Object-Oriented Analysis Design Methodology (OOADM) using the Unified Modelling Language (UML). The choice of this methodology is because we need to present every stage of the study from analysis to the design phases. With the help of the chosen methodology, we analyzed the existing frameworks, identified the weaknesses, and as a result, we further surveyed algorithms used for reliable data security. From the results obtained from the survey, we employed the SHA-256 algorithm because of its strength in data security, and the Argon2 hashing algorithm which is one of the best algorithms for securing database credentials. In the end, we provide an enhanced framework made up of the chosen algorithms and a two-dimensional database (2-DDb), which could be implemented to effectively combat attacks on important databases.

Keywords: Cyber threats; Database architecture; Cyberespionage; Nigeria Health data information

1. Introduction

The menace of cybercrime in this era is astoundingly alarming and has continued to be on the rise as individuals and business become more reliant on computers and the internet for their day to day activities (Lawani and Osagie-Obazee, 2019). According to (Petrosan, 2023) 40% of internet users fell victim to cybercrime in the year 2022. In recent years, Nigeria like several other countries have experienced several notable cyber-attacks that have highlighted the country's vulnerabilities in the digital space. One significant incident occurred in 2016 when Nigeria's central bank, the Central Bank of Nigeria (CBN), and several commercial banks were targeted by a cyber-attack known as the "Business Email Compromise" (BEC). This attack involved cybercriminals hacking into email accounts to facilitate fraudulent wire transfers, leading to substantial financial losses. Another major incident was the ransomware attack on the Nigeria Customs Service in 2020, which disrupted the agency's operations and compromised sensitive data. These attacks underscore the need for robust cybersecurity measures and heightened awareness to protect Nigeria's critical digital infrastructure and financial systems. According to Olaigbe (2022), some remarkable cybercrimes in Nigeria include:

- Ransomeware attack on Nigerian betting platform Bet9ja which was carried out by BlakCat in April 2019;
- In May of same year, MoMo Payment Service Bank suffered a breach that reportedly caused a loss of $53 million just few days after launching the platform;

[*] Corresponding author: Aleke Francis Alexander Onyibe

- In a related case, the Lagos Internal Revenue Service (LIRS) was accused of data breach through exposing personal data online on its web portal and was fined the sum of 1 million naira by national information technology development agency (NITDA) in same year;
- In addition, 71 percent of Nigerian organizations were hit by ransomware in the past year, yet some of Nigeria's worst cybersecurity incidents are still not reported (Guardian, 2022).

Previous research into combating cyber threats has explored a wide range of techniques spanning various domains such as network security, artificial intelligence (AI), and behavioral analysis. One traditional approach involves Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which monitor network traffic for suspicious activities and take corrective actions (Wasiu and Acheme, 2024). These systems rely on signature-based detection to identify known threats and anomaly-based detection to spot unusual patterns that may indicate an attack. AI and machine learning are also becomming prominent in cybersecurity research. Machine learning algorithms can analyze vast amounts of data to detect anomalies and predict potential threats based on historical patterns. Techniques such as supervised learning, unsupervised learning, and reinforcement learning are employed to improve the accuracy of threat detection and response. Additionally, natural language processing (NLP) is used to analyze textual data from threat intelligence reports and social media to identify emerging threats Acheme *et. al*., (2024) provided a comprehensive review of various machine learning techniques used for network intrusion prediction.

Behavioral analysis is another significant area of research, focusing on understanding and predicting the actions of both attackers and legitimate users. By studying user behavior, systems can differentiate between normal and suspicious activities, helping to prevent insider threats and unauthorized access. Honeypots and honeynets, which are decoy systems designed to attract and analyze attackers, have also been extensively researched to gather intelligence on attacker methods and improve defensive strategies. Furthermore, cryptographic techniques have been advanced to secure communications and data storage. Research in this field includes the development of more robust encryption algorithms and protocols to protect against increasingly sophisticated attacks. Blockchain technology has also been explored for its potential to provide secure and tamper-proof data management solutions. Overall, the continuous evolution of cyber threats necessitates ongoing research and innovation in these and other areas to enhance cybersecurity defenses.

This study aims to develop an enhanced framework for combating cyber threats on critical national infrastructure using secure two-tier database architecture. With the specific objective to design a framework for Combating Cyberespionage on the Nigeria's health sector through the use of multiple databases incorporating the SHA-256 and Argon2 algorithms for data security and hashing. The study is important in the sense that it would develop a pathway for preventing cyber-related crimes on the Nigeria's electronic health data infrastructure. The outcome of this study would also encourage and improve confidence when performing analytics on the Nigeria's health data.

2. Related Works

Here, the most recent literatures that focus on the problem domain are reviewed. Reasons are to present a clear need for further research in the subject area under study. Research works selected from reliable sources are reviewed to guide through identifying the gaps, which this study intends to fill.

In trying to find solution to curtailing cybercrimes on electronic infrastructures, Kemp (2023) employed Bayesian model averaging on a representative sample of 5,872 businesses from four rounds (2018–2021) of the UK Government's Cyber Security Breaches Survey. Results from the research according to the author, showed that government policies and schemes awareness helps to provide more security against cybercrime, though, the research results do not show that companies who implement the recommended measures are at low risk of cyberattacks.

Shuai et al.(2023) in their research to curb attacks of critical infrastructures; used a novel cybersecurity data set, IP addresses from FireHOL blocklist in addition to Generalized Linear Models (GLMs) to assess the potential influence of various explanatory variables on cybercrime and to identify the most important factors. The researchers further use Structural Equation Modelling (SEM) to examine the causal relationships within the networks of interacting factors in order to distinguish drivers of cybercrime. The authors developed models for identifying causative factors of cybercrime, and regions with the highest cybercrime occurrences but they did not develop and implement a novel system for combating cybercrime.

Notably, Adom et al.(2023) proposed the use of a prototype personal computer (PC) surveillance and monitoring software system for combating cybercrime. Their proposed system is to use the basic and extended features of a spyware for software administrative control, and computer monitoring for illegal and fraudulent usage. The authors posited that the proposed system could be configured to be invisible to unwanted users for recording users' activities and to track the trail of usage of computer applications. However, it is a work in progress.

In other to achieve more robust results, Sheikh et al.(2022) considered the role of machine learning and deep learning in providing security for cyberphysical systems (CPS). The authors identified challenges that underscores the use of machine learning and deep learning. Such challenges include: CPS constraints, the performance of learning models, and security of learning models. The authors further proposed a framework for cyberphysical systems security, and the proposed framework must take into consideration all domain requirements and constraints and past known and future unknown (Zero day) attacks.

Rao et.al (2021) used a hybrid approach made up of the Diffusion based cryptography and Diffie-Hellman key exchange Algorithm for database security. According to the authors, effective security was achieved, however, encryption of information cannot be performed with the help of the Diffie-Hellman algorithm and the diffusion based cryptography is susceptible to insertion and modification once an active interceptor breaks the algorithm.

Arasu et.al (2021) developed a system called 'Fastver' to improve data integrity on databases. Their system is based on a hybrid approach that the strengths of Merkle trees and deferred memory verification. The system showed good performance when compared with the traditional approaches of the constituent methods, however, they noted that the '*Verify ()*' method may fail to detect inconsistencies when collision is found on the cryptographic hash.

Mee et al. (2019) developed a case based reasoning (CBR) decision support methodology for profiling cyberattacks and document hackers' behavioural traits. Their work focused on data-driven analysis of websites defacement, and they recommended cross-data analysis with other various data sources like cybercrime statistics data from law enforcement agencies, threat intelligence data from malware analysis groups, and vulnerability databases. Their work did not provide electronic framework for directly combating cybercrime and cyberespionage.

Fidler (2012) highlighted steganalysis for detecting information hidden in an image file. Beginning his work, a possible stego image was processed by a preprocessing network consisting of several convolutional layers and two fresh focus modules, and several enhanced feature maps were output. Then, the resulting enhanced feature maps were fed into both a classification network and a reconstruction network. The classification network identified whether the feature maps came from a stego image or a simple cover image. The reconstruction network, consisting of some layers of convolutional units, pixel shufflers and feedback residual modules, completed the reconstruction of hidden information. The result of his experiment shows that the proposed image steganalysis algorithm can obtain state-of-the-art results in terms of detection rate and hidden information reconstruction compared with classical rich models and several recent deep learning-based methods. However, his work was based on steganography as a way of hiding information in an image, and processing stegano image to reveal its contents. His work did not proffer any electronic solution to all possible means of cyberespionage and cyberwarfare.

3. Methodology

This paper proposes a framework of a two-tiered database architecture that can be implemented for improving security in critical information systems. In figure 1, the diagrammatic illustration of the conceptual framework is presented, it involves breaking down the key components and their interactions in a clear, visual format. It includes elements related to cybersecurity, database architecture, and critical infrastructure protection.

The proposed framework is a 2-tier architecture in DBMS. This refers to a client-server architecture where the user interface and the application logic are separated into two separate components. The client component is typically the user interface and the server component is responsible for handling the data and business logic. In this architecture, the client component communicates directly with the server component to request data and perform actions.

In the proposed framework, the database user initiates a data transaction (which may be storage or retrieval) of data after a successful logon. The request passes through the reference database (RDB) which is the visible database. For data storage, the data is stored in the RDB, the BDB becomes active and an automatic OTP is sent to the DB user and a window opens for the user to supply the OTP sent to a registered phone number. If the OTP is entered within the stipulated time, the data is hashed using the SHA-256 algorithm and stored in the BDB. The state of the BDB changes to 'hidden'. If the OTP entered is not correct, the BDB changes state to 'hidden'. Figure 2 illustrates these processes.

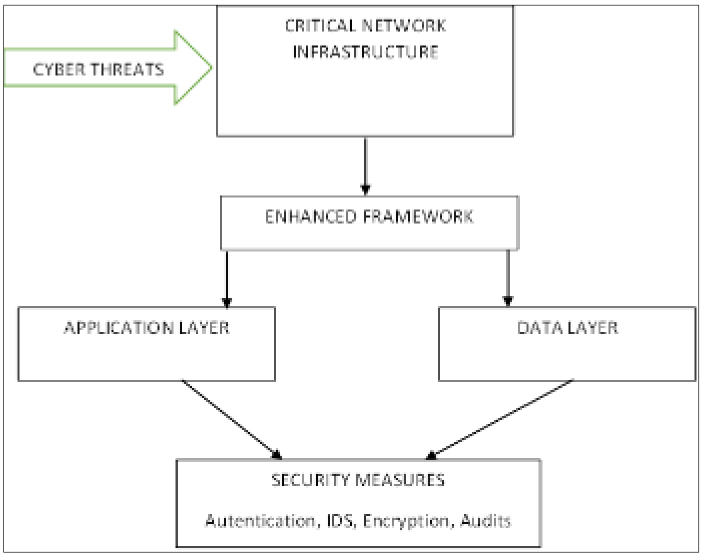

Figure 1 Conceptual Framework

In the course of data retrieval and access which is the major target of most attackers, the BDB prompts the user to enter that user's password as contained in the BDB (different from that of the user's password on the RDB), if the password is correctly entered, an OTP is also sent to complete the retrieval process.

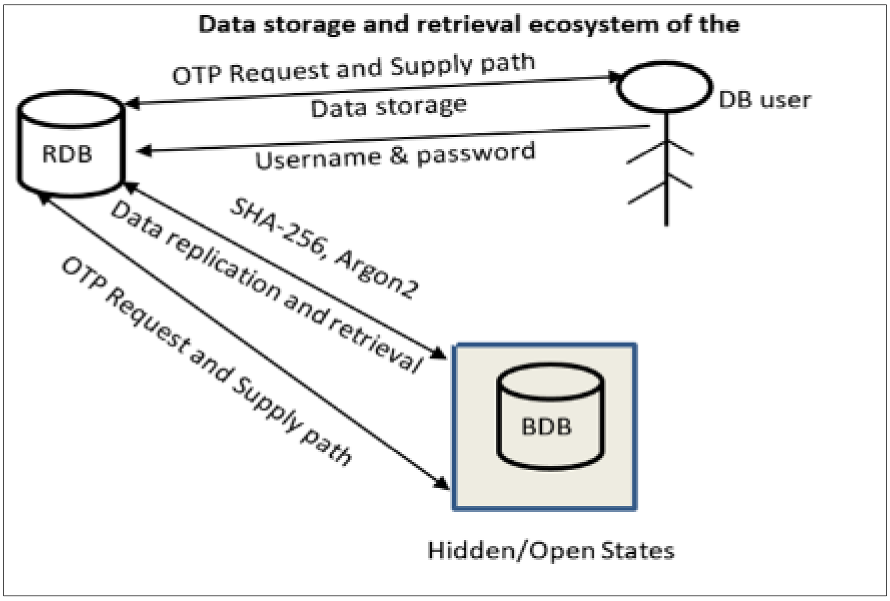
Data storage and retrieval ecosystem of the
OTP Request and Supply path
Data storage
Username & password
DB user
RDB
SHA-256, Argon2
Data replication and retrieval
OTP Request and Supply path
BDB
Hidden/Open States

Figure 2 A simple database storage and retrieval system

To show clearly the distinction between the existing framework and the proposed framework, the propose framework is analyzed using the use case diagram. Figure 3.3 shows the use case analysis of the proposed framework.

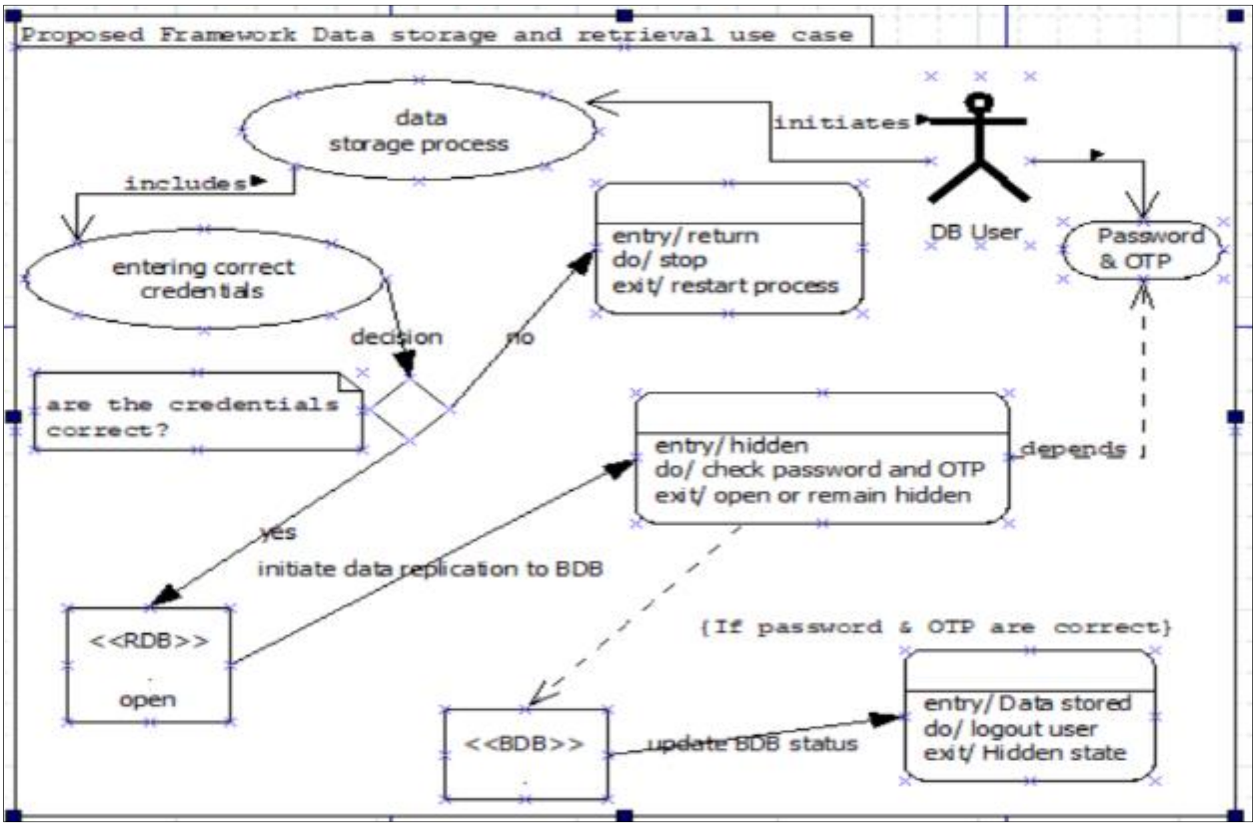
Proposed Framework Data storage and retrieval use case
data storage process
initiates
DB User
includes
entering correct credentials
entry/ return
do/ stop
exit/ restart process
Password & OTP
decision
no
are the credentials correct?
entry/ hidden
do/ check password and OTP
exit/ open or remain hidden
depends
yes
initiate data replication to BDB
<<RDB>>
open
{If password & OTP are correct}
<<BDB>>
update BDB status
entry/ Data stored
do/ logout user
exit/ Hidden state

Figure 3 Use case Analysis of the Proposed Framework

In Figure 3.3, the database user initiates an action to store or retrieve data from the database. The data storage process passes through the RDB where data is first stored on entering the correct credentials as stored against that user in the RDB. Subsequently, data replication process is automatically triggered and the user is asked to input password for the BDB and OTP sent to the user’s phone. If the password and the OTP are correct, the state of the BDB is changed to allow data storage. After the storage succeeds, the state of the BDB is updated to ‘Hidden’ and the user is logged out of the BDB. For data retrieval, access to the BDB is required through the use of password and OTP. If the password and OTP are supplied correctly, the requested data is compared with what is contained in the RDB. If any difference is identified, the BDB shuts down the request as an attack on the RDB is suspected. The RDB and BDB database administrators will have to perform some integrity checks before normal workflow is restored.

4. Conclusion

Security of information remains a critical task for many organizations especially in the health sector which requires the highest forms of confidentiality. This research work presented a framework made up of the chosen algorithms and a two-dimensional database (2-DDb), which could be implemented to effectively combat attacks on important databases. The key components of the framework is the incorporation of the SHA-256 algorithm because of its strength in data security, and the Argon2 hashing algorithm which is one of the best algorithms for securing database credentials.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adom, W., Ping, Z., & Frederick, A. A. (2023). Combating Cybercrime using a Prototype PC Surveillance and Monitoring Software System. *International Journal of Computer Applications, 185(9), 34-39*.

[2] Arasu, A., Chandramouli, B., Gehrke, J., Ghosh, E. et.al (2021). Fastver: Making data integrity a commodity. In Proceedings of the 2021 International Conference on Management of Data, 89-101.

[3] Fidler, D. P. (2012). Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think. *International Journal of Critical Infrastructure Protection*, *Vol.1*(Iss.1). https://doi.org/https://doi.org/10.1016/j.ijcip.2011.12.001

[4] Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. Computers & Security. *Computers & Security*, *Volume 127*(ISSN 0167-4048). https://doi.org/https://doi.org/10.1016/j.cose.2022.103089

[5] Lawani, C. & Osagie-Obazee, G. (2019). Alarming Rate of "Yahoo Plus" and Human Insecurity Dilemma in Nigeria: Implication for Counselling. European Scientific Journal, 15(13) ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431.

[6] Mee, L. H., Byung, I. K., & Huy, K. K. (2019). CBR-Based Decision Support Methodology for Cybercrime Investigation: Focused on the Data-Driven Website Defacement Analysis. *Security and Communication Networks*, *Volume 201*. https://doi.org/DOI:10.1155/2019/1901548

[7] Olaigbe, O. (2022). *The Deep Roots of Nigeria's Cybersecurity Problem*. Wired. https://www.wired.com/story/nigeria-cybersecurity-issues/

[8] Petrosan, A. (2023). *Percentage of internet users in selected countries who have ever experienced any cybercrime as of December 2022*. Statista: The Statistics Portal. https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

[9] Rao,M.S., Rao, K.V. & Prasad,M.H.M.K. (2021). Hybrid Security Approach for Database Security using Diffusion based cryptography and Diffie-Hellman key exchange Algorithm. 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, 1608-1612, doi: 10.1109/I-SMAC52330.2021.9640762

[10] Sheikh, Z. A., Singh, Y., Singh, P. K., & Ghafoor, K. Z. (2022). Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. *Computer Communications*, *193*, 302–331. https://doi.org/10.1016/J.COMCOM.2022.07.007

[11] Shuai, C., Mengmeng, H., Fangyu, D., Dong, J., Jiping, D., Shize, Z., Qiquan, G., & Chundong, G. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*. *Vol.10, Iss.71.* https://doi.org/https://doi.org/10.1057/s41599-023-01560-x

[12] WASIU, A. A., & ACHEME, I. D. (2024). A Comparative Study of Machine Learning Algorithms Used for Network Intrusion Detection. IRE Journals Volume 8 Issue 1.

[13] Acheme, I. D., Wasiu, A. A., & Edegbe, G. N. (2024). A network intrusion prediction model using Bayesian network. World Journal of Advanced Research and Reviews, 23(1), 2813-2821.