British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

IMPROVEMENT ON CYBERSECURITY TECHNIQUES AND RISK MITIGATION OF INFORMATION SYSTEMS USED IN INTERNET BANKING AND MOBILE BANKING

Oladejo Samuel Adetunji[1] and Waheed A. A. (Ph.D.)[2]

[1&2]Department of Computer Science, Faculty of Natural and Applied Science, Lead City University, Ibadan Oyo State, Nigeria.

Email: [1]oladejosa@live.com, [2]waheed.azeez@lcu.edu.ng,

Cite this article:

Oladejo, S. A., Waheed, A. A. (2024), Improvement on Cybersecurity Techniques and Risk Mitigation of Information Systems Used in Internet Banking and Mobile Banking. British Journal of Computer, Networking and Information Technology 7(3), 73-84. DOI: 10.52589/BJCNIT-NDPYWQYV

Manuscript History

Received: 22 May 2024

Accepted: 31 Jul 2024

Published: 9 Aug 2024

ABSTRACT: *Cybercrime committed on financial institutions are rapidly and steadily becoming more sophisticated and more widespread. The rise in occurrence and extent of cyber-attacks can be linked to a number of factors, such as ineffective risk management systems within banking sectors, ICT technological infrastructure and staff competency and awareness about cyber crimes attacks. As a result of the vulnerabilities in the systems, organized criminals take advantage to breach financial institution's systems to steal money. This study makes an effort to look into ways to improve the multi-tier threat and risk management system for internet and mobile banking. The completion of this project marks a significant milestone in the development of a modern banking management application system. The Banking Management Application System, integrated with Flutter, DRF, and MySQL, demonstrates the capabilities of these technologies in building cross-platform mobile applications with an intuitive and visually appealing user interface, robust backend API, and efficient database management. By implementing essential banking functionalities, the system aims to enhance the banking experience for customers, providing convenience, security, and efficiency in managing their accounts and conducting transactions. The successful implementation of the Banking Management Application System with DRF and MySQL confirms the feasibility and effectiveness of this technology stack. The system's architecture, database design, user interface design, and the powerful features of DRF and MySQL contribute to its overall functionality and user satisfaction. Through this project, we have gained valuable insights into software design, system implementation, and the utilization of the Dart-Flutter-DRF-MySQL stack for developing a comprehensive and feature-rich banking management application system.*

KEYWORDS: Multi-tier threat; Risk management system; Internet banking; Mobile banking.

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

INTRODUCTION

Banks are not looted as frequently as they once were because money is now held outside of bank vaults. There is a lot of money in cyberspace, thanks to modern computer technologies and data networks. Banks need to protect themselves against cybercrime while also adjusting to contemporary trends of conducting business electronically. In the year 1820, the first "cybercrime" was officially documented. That is not surprising given that the abacus, which is considered to be the earliest type of a computer, has been used in China, Japan, and Nigeria since 3500 BC. However, it was Charles Babbage's analytical engine that marked the beginning of the contemporary computer era. To date, practically all banks in Nigeria have adopted electronic banking and/or cyber banking in one form or another.

Nigerian financial institutions are adjusting to technological advancements on a global scale, but cybercriminals remain on the prowl. Worldwide, e-banking fraud is a problem that continues to cost both banks and clients' money. Millions of dollars' worth of financial transactions have been made online thanks to e-commerce, online banking, and related technologies, and as banks broaden the range of online services they offer their customers, the risk of internet computer fraud (ICF) rises and the risk environment changes. With the increasing use of e-banking services and its predicted domination in the near future, high-profile attacks with financial motivation have been seen all over the world. Some of the well-known contributing reasons to the pressing security issue need to be addressed[1].

Due to the growing threat that cybercrime poses to the global economy, the Nigerian government planned to enact legislation to reduce it there[2]. There was a need to develop strategies to tackle cybercrime given the threats it posed to the world's economies. Nigeria was experiencing an upsurge in cybercrime incidents, which necessitated research to quantify. Nigeria is becoming more dependent on ICTs, which is a troubling development given the presence of cybercriminals[3]. People cannot define fraud because it has been committed online, and it is also noted that because the majority of cybercrime victims are well-known bank clients, they are reluctant to publicly acknowledge that they have been successfully duped by some cybercriminals[4].

Banks recently began offering online banking services to their consumers, but many of them did not feel secure enough to handle their counseling online. However, a lack of security and value knowledge is the main factor in customer concerns. The two most important considerations that may affect the use of web banking services anywhere are security and value[5]. All banks in Nigeria use internet banking, giving their customers the freedom to access their accounts and conduct transactions whenever and wherever they choose. Online banking, in contrast, has made several security dangers known that may jeopardize the usage of such services. This is because customers provide terrible information, and revealing it would have an impact on the customer still because of the bank's relationship with their customers[6].

Banks and financial institutions now face newer varieties of hazards to the privacy and security of data, a vital asset for every organization. In the Internet of Things era, criminal activity and data theft have become more sophisticated and cunning, with criminals increasingly using technology to get over technological barriers within the financial system. Banks must invest in systems and technology that go beyond merely avoiding assaults since bank cyber security threats have low entry barriers[7]. Protecting customer assets is the clear reason why cyber security is important in banking activities. As more individuals go cashless, online checkout

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

pages and physical credit scanners are becoming more prevalent. In both scenarios, customer information may be forwarded to other locations and used maliciously. Additionally, the client is impacted by this. Additionally, it harms the bank significantly as they work to restore the data[8]. If the information is taken, the bank might have to pay hundreds of thousands of dollars to get it back. They consequently lose the trust of their customers and other financial institutions. That is not the only issue that comes when cyber security banking precautions are not taken. The customer must cancel all of their credit cards and start new accounts, maybe with a different bank. Even if the FDIC insures their funds, thieves are still trying to get their personal information[9].

A customer's confidence and faith in the financial service would undoubtedly be impacted if they become a victim of a fraud or experience system access issues. Unplanned system disruptions are a significant contributor to customers' unhappiness with DFS provider services[10]. The inability to transact due to network or service outages was considered as one of the top annoyances and led to reckless behavior that put the users at risk of being cheated, according to research on the attitudes and behaviors of low-income mobile money users. The bad experiences demonstrate that DFS customers are less likely to use mobile money services more frequently and have much less faith in service providers and the entire financial system[11]. The potential fraud and system access mistakes that can arise from a cyber-incident disproportionately affect the poor. They are more prone to use devices and channels that are not intended to offer the security needed for a financial transaction (such as USSD technology), are frequently less knowledgeable about social engineering assaults, and—most importantly—can least afford to lose money. Another issue is that customers in underdeveloped nations frequently face the burden of proving they were the victims or are responsible for any losses related to a cyberincident[12]. 5,220 mobile money users were polled in 2016 by the International Telecommunication Union (ITU) and CGAP. Deceptive 83% of respondents from the Philippines, 56% from Nigeria, and 27% from Ghana reported receiving SMS messages. 17% of mobile money users in the Philippines and Ghana, as well as 12% of those in Nigeria, admitted to having lost money as a result of fraud or a scam. Cyber events and the losses they create can obstruct attempts to increase access to financial services since trust and confidence in financial service providers (FSPs) and payment systems are essential components for sustained financial inclusion[13]. Additionally, these kinds of situations and patrons' bad experiences can spread swiftly through word of mouth and may wind up being covered by the media. It takes a lot of time and work to restore reputations and people's trust after such damage[14].

Cybercrime safety measures include the joint use of security protocols, plans, risk management tools, necessary practices, and competency that may be used to defend the information system[15], according to the worldwide communication authorities. Internet security, computer network security, and electronic system security are all included in the term "cybersecurity." Effective cyber-security measures, such as early detection, deterrent, and systems' capacity to continue operating during and even after attacks, are necessary to prevent the loss of data and retain integrity. These are crucial elements to take into account while developing a plan and minimizing the effects of cybercrime[16].

When systems are not properly protected, they become vulnerable. As a result, hackers will find it simpler to access the system and collect information without authorisation. Therefore, proactive and reactive cyber security measures should constantly be used in the banking industry. If only one preventative measure—such as firewalls and antivirus software—is

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

implemented, cyber theft cannot be properly controlled. More cyber defenses must be implemented for information security. Modern technology should be able to detect, block, and eliminate malware and viruses to prevent them from entering the system.[17]

As a result, a substantial gap still needs to be closed. The goal of this project is to investigate how to enhance the multi-tier threat and risk management system for online and mobile banking.

Statement of the Problem

Financial institutions are increasingly and progressively becoming targets of sophisticated and pervasive cybercrime. Numerous reasons, including ineffective risk management systems within banking sectors, ICT technological infrastructure, staff competency, and staff awareness of cybercrime attacks, might be linked to the increase in the frequency and scope of cyberattacks. Organized criminals take advantage of system weaknesses to hack into financial institutions' systems and steal money. Users of computers continue to be a weak point in online security since their password habits directly affect how secure a system is. Passwords that are not carefully chosen and managed may be more open to potential abuse and exploitation. As a result, even the most advanced security systems are vulnerable if users do not carefully choose and manage their passwords.

Passwords are still the most popular form of authentication even though issues with password security are "conspicuously unsolved," according to the Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance. Newer authentication methods that are supported by technology, such as biometrics and one-time pins, are gaining popularity and actually make the internet a safer place. All users, however, are required to use these technologies in the same way. In other words, differential authentication is not created using user attributes. All users are treated identically when authenticated, regardless of any additional information that may be known or inferred at the time of authentication.

There is a knowledge gap about Multi-Tier Threat and Risk Management System for Internet and Mobile Banking, according to the aforementioned reviews. This research attempted to close this gap. It aimed to enhance Internet and mobile banking multi-tier threat and risk management systems.

Aim and Objectives of the Study

A better multi-tier threat and risk management system for online and mobile banking is what this project aims to create.

The broad objectives are to:

i. create the management system's user interface for internet and mobile banking;

ii. create a multi-tiered framework for risk management for online and mobile banking; and to

iii. put the built system for online and mobile banking to the test and evaluate it.

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

METHODOLOGY AND DESIGN

Choice of Technology

For this study, the following development tools have been carefully selected:

1. Environment for Integrated Development: Programming languages for Microsoft Visual Studio Code: Python, Dart
2. My SQL database engine
3. Git and GitHub are two code repositories.
4. OpenCV, artificial intelligence

Design Method of System

The bottom-up method of controlled design was employed in this study. The basic systems are represented as subsystems of the emergent system since the bottom-up technique involves putting disparate systems together to create more complex systems. A bottom-up method identifies the system's discrete base components in great detail first. These components are then integrated to create bigger subsystems, which are in turn linked, often on several layers, to create a comprehensive toplevel system. The following are a few of the information system's design steps:

- Create a database table to store the information about your clients, and a form to collect (input) that information**.**
- Create a form that will allow users to register for mobile banking (processing) and store their information in a database table.
- Create a login form using the database table's existing client information.
- Create an authenticator to verify user information.
- Create a biometric and face recognition system as an alternative to the account number and password login method.
- Create a reliable report generator that can generate client registration information and transaction history as needed.

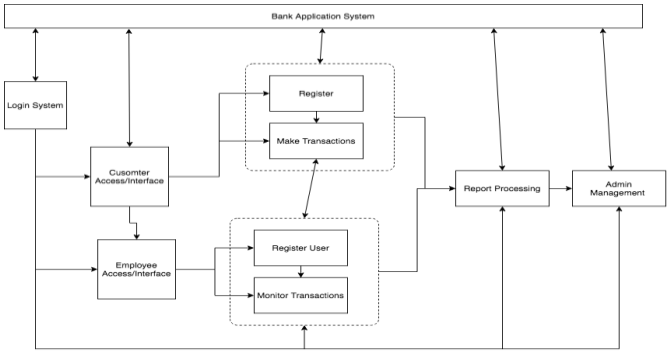

Figure 2.1: BAS's Functional Block Diagram (system flow)

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

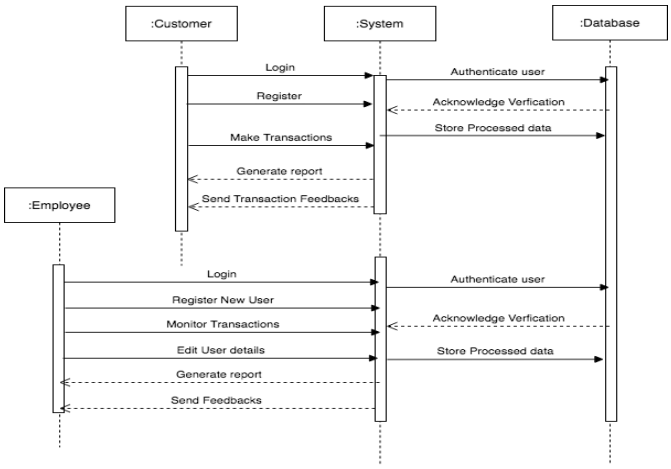

Figure 2.2: BAS's Sequence Diagram

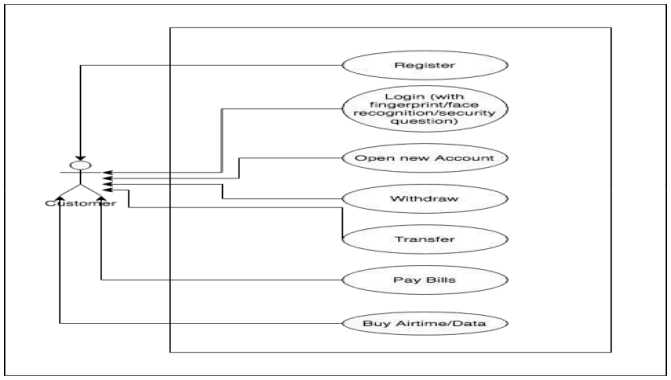

Figure 2.3: Case Diagram Showing Customers

Functionality in the System

System Design and Implementation

Software Design

Software Design

Software design refers to the procedure through which a computer or software engineer develops a specification of a software artifact, intended to achieve goals, utilizing a set of simple components and subject to limitations. Typically, problem-solving and planning for a software solution go into software design. This covers both high-level architecture design and low-level component and algorithm design.

Architectural Design

The suggested system is a banking application system that attempts to raise the multi-tier danger that clients encounter from approved individuals and bankers while using the mobile bank application. A MySQL database was integrated into the Banking Application System to store customer personal information in encrypted format using a cryptographic technique and

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

their transaction details. Additionally, the MySQL stores user security queries in Cipher-Text form. Using an API, or application programming interface, the bank application system communicates with the system directly. It processes all requests and offers a user interface through which users may communicate with the system. Figure 3.1 shows the Bank Application System's architectural layout:

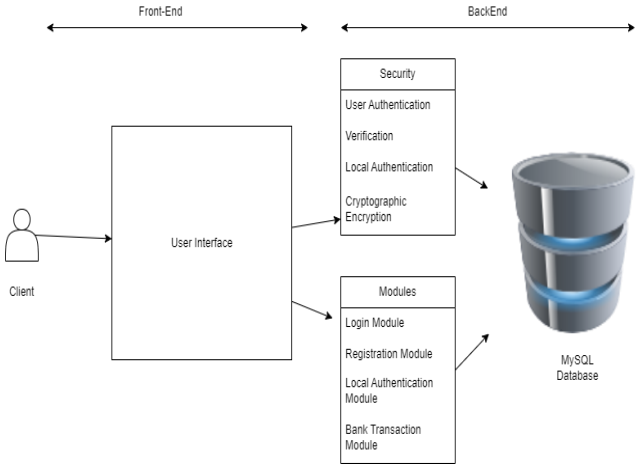

Figure 3.1: Architectural Layout of Bank Application

System

EER DIAGRAM

An EER (Enhanced Entity-Relationship) diagram is a form of conceptual data model used in software engineering to represent the structure of a database system. The EntityRelationship (ER) model serves as the foundation for the EER diagram, which expands its capabilities by introducing new ideas and features. The entities (or objects), their properties, and the connections between entities in a database system are represented by an EER diagram. It offers a visual representation of the relationships between various elements and their interactions inside the system.

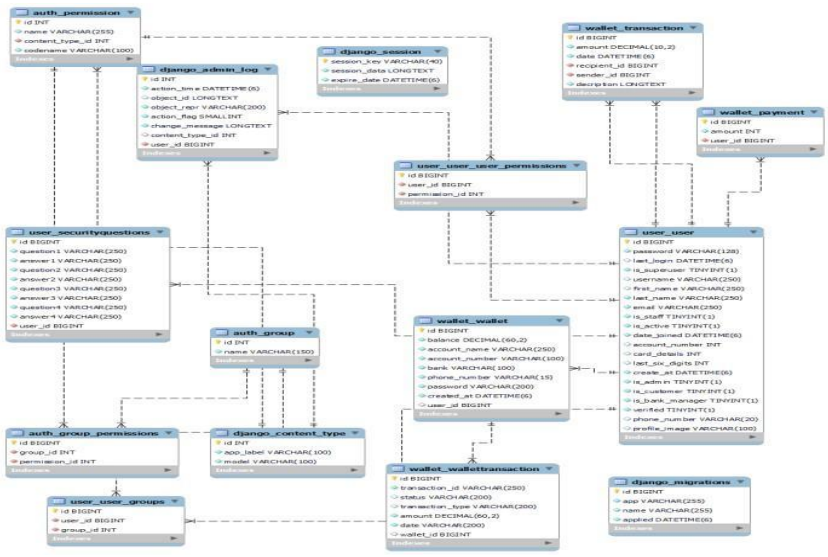

Figure 3.2: Enhanced Entity Relation Diagram of Bank

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

Application System

Input Interfaces and Procedures

The implemented system adheres to the UI/UX (User Interface/User Experience) paradigm, seeking to familiarize and address user issues rather than only impressing the user with its user interface. User ID (Account number for clients, username for bank personnel, and password for system administrator) and Password are required to use the system. The user is given access to the system once this is checked against the data kept in the system's database.

Figure 3.3: Customers Onboarding Screen

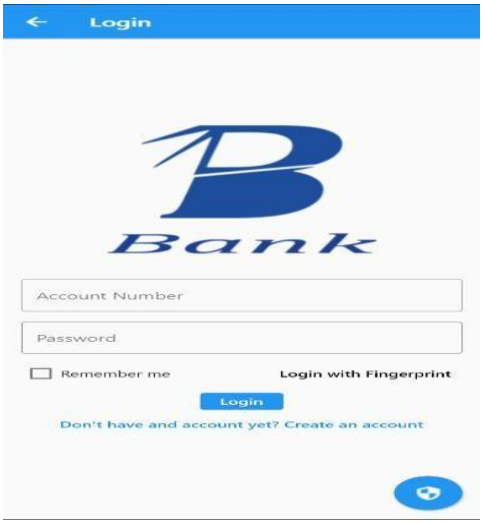

Figure 3.4: Customers login screen

Figure 3.5: Security Questions

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 3, 2024 (pp. 73-84)
www.abjournals.org

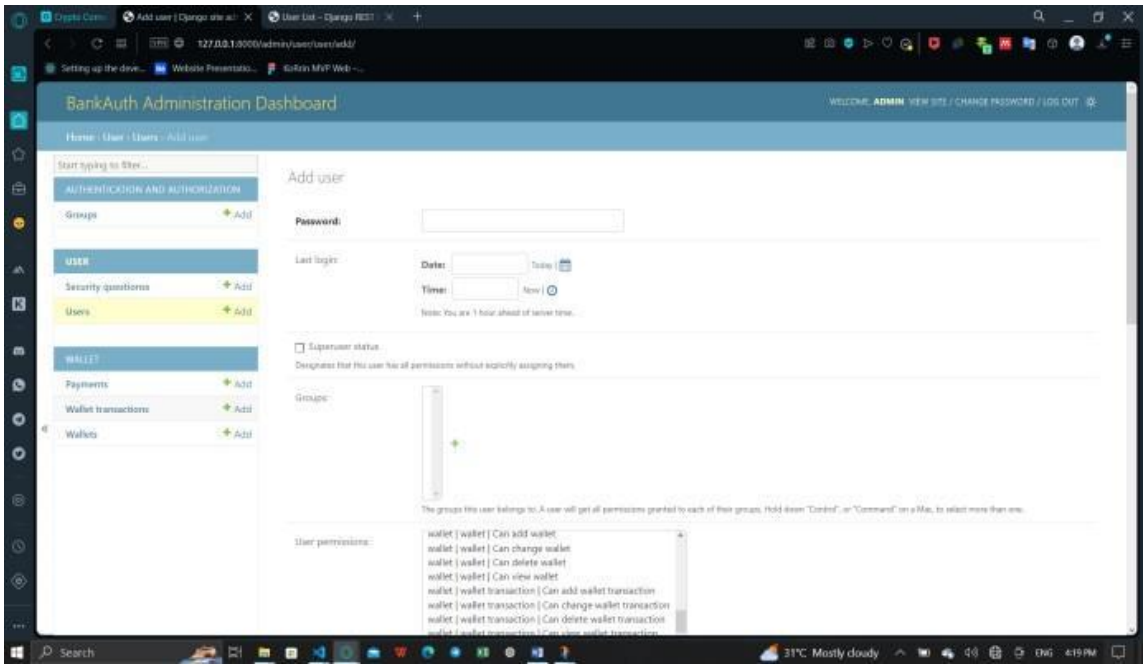

Figure 3.6: System Administrator's User Management

Output Interfaces and Procedures

1. **User Dashboard:** Users are shown a personalized dashboard after successfully logging in, which includes pertinent data such as account balances, recent transactions, and notifications.

2. **Transaction Receipts:** The system creates receipts that contain information about transactions, such as transaction IDs, dates, and amounts, when users carry out operations like fund transfers, bill payments, or account enquiries.

3. **Account Statements:** Users have the option to get account statements that list their transactions for a given time period. For record-keeping purposes, you can download these statements as PDF files or view them online.

4. **Alerts and Notifications:** The system notifies users of significant account actions, such as low balance alerts, transaction confirmations, or account updates, by sending them alerts and notifications. Email, SMS, and in-app notifications are all options for getting these notifications.

5. **Error Messages:** If any difficulties or problems are detected while the system is in use, the proper error messages are presented to users, offering aid and information in troubleshooting the issue.

Module Functionalities

The following are the main modules and their functions: User authentication is handled by this module, which also verifies user credentials and grants access to authorized users in accordance with their responsibilities (client, bank employee, or system administrator).

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

1. **Account management:** Users can manage their accounts through this module, which includes viewing balances, making deposits and withdrawals, starting fund transfers, and managing beneficiaries.

2. Various transactions, including bill payments, loan applications, financial transfers between accounts, and account enquiries are processed by this module. It guarantees the transactions' security and accuracy.

3. **Security and encryption:** This module provides security methods to safeguard user data, such as password security, encryption of sensitive data, and the usage of authentication protocols (such as face or fingerprint ID).

4. **Reporting and Analytics:** This module offers reporting features, producing reports on account activities, transaction histories, client demographics, and other pertinent data. Additionally, it has analytics tools for analyzing user behavior and finding patterns.

5. **System Administration:** With the help of this module, system administrators can control user roles and permissions, system updates, and database upkeep activities.

CONCLUSION

The completion of this project marks a significant milestone in the development of a modern banking management application system. The Banking Management Application System, integrated with Flutter, DRF, and MySQL, demonstrates the capabilities of these technologies in building cross-platform mobile applications with an intuitive and visually appealing user interface, robust backend API, and efficient database management. By implementing essential banking functionalities, the system aims to enhance the banking experience for customers, providing convenience, security, and efficiency in managing their accounts and conducting transactions.

The successful implementation of the Banking Management Application System with DRF and MySQL confirms the feasibility and effectiveness of this technology stack. The system's architecture, database design, user interface design, and the powerful features of DRF and MySQL contribute to its overall functionality and user satisfaction. Through this project, valuable insights have been gained into software design, system implementation, and the utilization of the Dart-Flutter-DRF-MySQL stack for developing a comprehensive and feature-rich banking management application system.

RECOMMENDATION

Based on the findings of this study, the following are recommended:

1. Platform enlargement increases the system's interoperability with iOS devices to expand its user base and guarantee a consistent user experience across all platforms.

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

2. Enhanced security measures: To keep up with changing security threats, security systems must be updated and improved on a regular basis. Use more sophisticated authentication techniques, such biometric authentication, to give users higher security and convenience.

3. Connecting to banking systems: Work together with financial institutions to integrate the system with current banking platforms so that consumers can access a wider choice of services and receive real-time account information.

4. Performance improvement: Constantly assess and improve the system's performance to guarantee a responsive and fluid user experience—even when there is a lot of traffic.

REFERENCES

1. E. F. Ampratwum. Advance Fee Fraud "419" & Investor Confidence in the Economies of Sub-Saharan Africa (SSA), **Journal of Financial Crime**. 16 (1), 2019, 1-11
2. A. G. Singh. An Explorative Study of Satisfaction Level of Cyber-crime Victims with Respect to EServices of Banks, **Journal of Internet Banking and Commerce**. Vol. 17(3), 2012
3. M. L. Bhatt. Cyber Attacks & Defense Strategies in Nigeria: An Empirical Assessment of Banking Sector, **International Journal of Cyber Criminology**. 7(1). 2018
4. B. L. Sheridon. Credit Card Fraud: Awareness and Prevention, **Journal of Financial Crime.** 15(4), 2021, 21-29
5. BITS. Fraud Prevention Strategies for Internet Banking, A Publication of the BITS Fraud Reduction Steering Committee, www.BITSINFO.ORG. 2017
6. G. H. Olumide. Cybercrime & Criminality in Ghana, **Journal of Information Technology Impact**, 11(2), 2011, 80-100
7. J. J. Olumide. An Analysis of Advance Fee Fraud on the Internet, Journal of Financial Crime, Vol.15 No. 1. 2018,
8. T. K. Dube Adoption and use of Internet Banking in Nigeria: **An Exploratory Study, Journal of Internet Banking and Commerce**, 14(1). 2019
9. D. V. Geeta. Online Identity Theft-In Nigerian Perspective, **Journal of Financial Crime**. **Emerald Group Publishing Ltd.,** 18(3), 2021, 235-246
10. U. K. Gercke. Understanding Cybercrime: A Guide for Developing Countries. ICT Applications and Cybersecurity Division. **Policies and Strategies Department. ITU Telecommunications Development**. 2019
11. K. E. Shalom. A Framework for Cyber Security in Africa. **Journal of Information Assurance and Cybersecurity,** 2012 (2012), Article ID 322399. 2018
12. S. T. Marshall. Computer Fraud – What Can Be Done About It? T**he CPA Journal; May 1995; 65, 5; Accounting & Tax.** 2019
13. M. S. McGuire. Cybercrime: A Review of the Evidence, **Cyber-enabled crimes-fraud & theft, Home Office Research Report** 75. 2018
14. M. P. Owor. Workshop Report on Effective Cybercrime Legislation in Eastern Africa, Dar Es Salaam. 2019
15. K., Njanike, T. Dube & E Mashanyanye., The Effectiveness of Forensic Auditing in Detecting, Investigating and Preventing Bank Frauds, **Journal of Sustainable Development in Africa,** 10 (4), 2009, 405-425

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV

16. H.Y. Prabowo. Building Our Defense Against Credit Card Fraud: A Strategic View, **Journal of Money Laundering Control, 14(4), Emerald Group Publishing Ltd**. 2021
17. M. L. Potter. Internet Banking and Fraud: Making Business Less Risky, **Community Banker** 9 No.7 JI 2000. 2019
18. PWC. Cybercrime: Protecting Against the Growing Threat. **Global Economic Crime Survey, www.pwc.com/crimesurvey.** 2019

Article DOI: 10.52589/BJCNIT-NDPYWQYV
DOI URL: https://doi.org/10.52589/BJCNIT-NDPYWQYV