Int. j. adv. multidisc. res. stud. 2026; 6(1):459-466

Received: 19-11-2025
Accepted: 29-12-2025

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Secure Online Banking Transaction System with Cryptography

[1] Lombe Masua, [2] Moses Mupeta

[1, 2] Department of Information Security and Computer Forensics, School of Engineering, Information and Communications University, Lusaka, Zambia

Corresponding Author: **Lombe Masua**

Abstract

The rapid adoption of digital financial services has increased the demand for secure, reliable, and efficient online banking platforms. However, the rise in cyber-attacks, identity theft, and unauthorized transactions continues to undermine user trust and expose critical vulnerabilities in existing systems. This study presents the design and development of a secure online banking transaction system that integrates advanced cryptographic techniques to ensure confidentiality, integrity, and authentication of financial data. The system incorporates a hybrid cryptographic model combining symmetric and asymmetric encryption to safeguard transaction processes, user credentials, and communication channels. Multi-factor authentication (MFA) and secure session management are also implemented to strengthen access control and mitigate common attack vectors such as phishing, man-in-the-middle attacks, and brute-force intrusions. A prototype of the system was developed and evaluated through functional testing, security analysis, and performance benchmarking. Results indicate that the proposed solution enhances transactional security while maintaining system efficiency and usability. The study demonstrates that cryptography, when properly integrated into online banking architecture, can significantly improve the resilience of digital financial systems against emerging cybersecurity threats.

Keywords: Online Banking, Cryptography, Hybrid Encryption, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Multi-Factor Authentication (MFA), Cybersecurity, Secure Transactions, Data Integrity, System Security, Authentication Mechanisms, and Session Management

1. Introduction

The rapid digital transformation across industries has made secure computing a foundational necessity, particularly in financial services. Secure computing encompasses technologies, protocols that ensure availability of information systems, and practices that protect digital systems and data from unauthorized access, breaches, and disruptions. In online banking, the risks of cyber-attacks such as identity theft, data leaks, and fraud continue to escalate as more users perform transactions over the internet (ZICTA, 2024) [1].

As cyber threats grow in sophistication, financial institutions are increasingly required to implement advanced data protection mechanisms to ensure trust and compliance with regulatory standards (Deloitte, 2022) [2]. Among the most effective solutions are cryptographic techniques, which provide confidentiality, integrity, and authentication for sensitive data (Check Point Research, 2023a) [3]. This project focuses on developing a secure online banking transaction system that integrates Advanced Encryption Standard (AES) encryption, secure user authentication, and structured database management using Java and MySQL (Paar and Pelzl, 2010; IBM, 2021; Macrium Software, 2023) [4, 5, 6].

1.1 Motivation and Significance of the study

Motivated by increasing threats of financial loss and identity theft, this study explores the necessity of implementing encryption protocols and strong security frameworks in online baking systems to restore user trust and system reliability. The motivation behind the study is to address the high rates of financial fraud, account takeovers, and data theft, and highlights the desire to help banks and customers secure online financial transactions (Rescorla, 2008; Sharma and Bohra, 2017; ZICTA, 2024) [7, 8, 1]. Zambia's vulnerability to cybercrime rose to over 9,500 cases reported in 2023.

The study highlights the importance and potential benefits of the research. It explains how the study positively impact various stakeholders, including customers (protecting their financial data during transactions), businesses (ensuring secure online payment systems), banks, and financial institutions (implementing and maintaining secure digital payment solutions), (Menezes, van Oorschot, and Vanstone, 1996; Macrium Software, 2023) [9, 6].

1.2 Scope of the Study

The study is centered on online payment security, excluding security concerns related to physical transactions (such as cash payments or in-person card transactions). It also contributes to various stakeholders by promoting cybersecurity awareness and helping organizations implement robust security systems (Mavroeidis, Tzovaras, and Strintzis, 2007; Kaspersky, 2022) [10, 11].

- Geographic Scope: Focused on Zambia, with specific reference to AB Bank Zambia and the local cybercrime context (ZICTA, 2024) [1].
- Technological Scope: Utilizes Java for application development, MySQL for database management and secure data storage, AES for data encryption, and SSL/TLS for secure data transmission (IBM, 2021; Oracle, 2021) [5, 12].
- User Scope: Includes customers, banking staff, and administrators involved in online transactions.
- Content Scope: Concentrates on online payment transaction systems, excluding ATM and in-person card systems.
- Evaluation Scope: Testing involves assessing system functionality, performance, usability, resistance to attacks and security effectiveness.
- Exclusions: Excludes non-digital transactions such as cash or Point of Sale transactions, regulatory compliance implementation, and physical security devices.
- Time Frame: Data and trends are drawn from 2022 to 2025 (ZICTA, 2024; Deloitte, 2022) [1, 2].

1.3 Problem Statement

The current online transaction systems suffer from vulnerabilities such as inadequate encryption, weak authentication, absence of secure communication protocols, and susceptibility to cyber threats, including SQL injection and social engineering attacks. According to the Zambia Information and Communications Technology Authority (ZICTA), Zambia reported over 9,500 cases of cybercrime in 2023, with financial fraud accounting to more than 60% of these cases (ZICTA, 2024) [1]. Additionally, a 2022 Deloitte Africa Cyber-security Outlook revealed that 75% of the African financial institutions experienced at least one attempted or successful cyber-attack in the past year, with online banking fraud cited as a major concern (Deloitte, 2022; Check Point Research, 2023a) [2, 3].

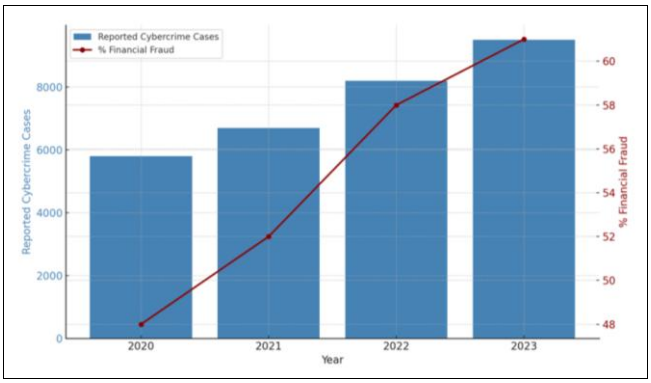
If these issues remain unaddressed, they pose a serious threat to user trust, financial stability, and regulatory compliance, especially as digital financial services expand rapidly in Zambia and across Africa. Without the implementation of secure cryptographic techniques, robust authentication mechanisms, and protected databases, online transaction platforms will continue to experience high rates of fraud, data breaches, and system exploitation.

The reported cybercrime cases are shown in Table 1. and Fig 1. Below.

Table 1.1: Reported Cybercrime cases in Zambia (2020-2023)

Year	Reported Cases	% Financial Fraud
2020	5800	48%
2021	6700	52%
2022	8200	58%
2023	9500	61%

Source: Author (2025)



Source: Author (2025)

Fig 1.1: Rising Cybercrime and Financial Fraud Cases in Zambia (2020-2023)

1.4 General Objective

- To Design and Develop a Secure Online Banking Transaction System with Cryptography.

1.5 Specific Objectives

- To implement AES encryption for secure online transactions.
- To design secure authentication mechanisms to prevent unauthorized access.
- To integrate a robust SQL-injection protected MySQL database for safe data management.

1.6 Research Questions

- How effective is AES encryption in securing online transactions?
- What authentication mechanisms can be implemented to prevent unauthorized access?
- How can the database be strengthened with access control mechanisms?

2. Literature Review

This chapter of the paper presents a comprehensive review of existing literature related to secure online banking systems and the application of cryptographic techniques in safeguarding financial transactions. It examines the evolution of online banking, common security threats faced by digital financial platforms, and the role of cryptography in enhancing data confidentiality, integrity, authentication, and non-repudiation.

The chapter also explores various cryptographic algorithms and security frameworks adopted in modern online banking environments, highlighting their strengths, limitations, and suitability for secure transaction processing. Furthermore, the review analyzes previous research studies, existing online banking models, and technological trends to identify gaps that justify the development of a more robust, cryptography-enhanced system. The aim of this chapter is to provide a theoretical foundation for the study, establish the

context of the proposed solution, and support the design choices made during the system development process.

2.1 Related Works

Several researchers and institutions have developed or analyzed online banking systems that incorporate cryptographic mechanisms to enhance transaction security. Reviewing these systems helps identify existing strengths, limitations, and opportunities for improvement in designing a more secure banking platform. This section presents three related systems frequently referenced in prior studies.

1. Secure Online Banking System Using Two-Factor Authentication (TFA) - (Nair and Thomas, 2020).

Nair and Thomas proposed a secure online banking system that integrates two-factor authentication (TFA) with traditional username and password login. The system uses AES encryption to secure transaction data stored in the database and SSL certificates to encrypt client–server communication. The authors highlight that adding TFA significantly reduces unauthorized access attempts and phishing-related risks.

2. Cryptography-Based E-Banking Security Model Using RSA and SHA-256 - (Kumar and Singh, 2021).

Kumar and Singh developed an e-banking security framework that employs RSA for secure key exchange and SHA-256 hashing for protecting user credentials. Their model ensures that sensitive information such as passwords and transaction details cannot be easily intercepted or altered. The system incorporates a layered security architecture, combining encryption, hashing, and session management.

3. Hybrid Cryptographic Online Banking System Using AES and RSA - (Ahmed *et al*., 2022).

Ahmed and colleagues proposed a hybrid online banking system that combines AES (symmetric) and RSA (asymmetric) encryption to secure both transaction processing and communication channels. The hybrid approach enhances confidentiality and key management efficiency. The system also integrates time-based OTPs to strengthen authentication.

3. Methodology

3.1 Baseline Study

Before the implementation of a secure online banking transaction system, a baseline study was conducted to assess the existing level of an online banking transaction system among the target audience. This baseline study serves as the foundation for evaluating the effectiveness of an online banking transaction system in enhancing cybercrime behavior. It also provides an insight into the strengths' and weaknesses of existing systems, allowing for targeted improvements in the online banking transaction system design.

The baseline study involved conducting interviews and carrying out surveys with banking staffs, systems administrators, and selected customers as these are often the target of cyber threats.

I. Data collection

for the baseline study was carried out through both primary and secondary sources:

Primary Data:

Collected via quantitative data collection method, structured questionnaires and qualitative data collection method, and semi-structured interviews. Questionnaires were distributed to banking customers and staff involved in managing digital banking platforms to assess their experiences with existing online banking systems.

Secondary Data:

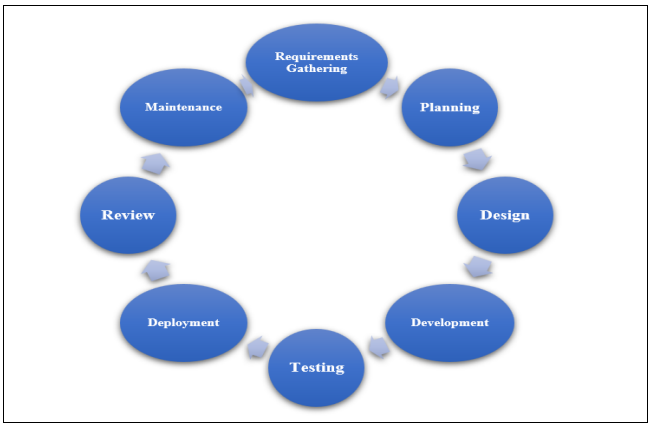
Included a review of the existing literature, cybersecurity reports, and statistics from reliable institutions such as ZICTA, Deloitte, and Check Point Research.

Ethical Considerations

Ethical considerations were of paramount importance in this study. All participants were briefed and given voluntary consent. Data privacy and confidentiality were strictly maintained for anonymity, and participants were given the option to withdraw from the study at any time without consequence.

II. Research Approach

Agile approach is an SDLC model widely used in software engineering to ensure success of the project. In the Agile approach, the whole process of software development is divided into sequential phases. In this Agile model, typically, the outcome of all phases is flexible and cyclic (Dyba and Dingsoyr, 2008) [15].



Source: Author (2025)

Fig 3.1: Agile model

The following are the Agile model phases in practice:

Requirements Gathering Phase

This phase involves identifying the project goals, key functionalities, and requirements from stakeholders, who are banking staff, IT teams, and selected customers.

Planning Phase

From the gathered requirements, the team begins planning sprints stages and assign the sprints to stakeholders.

Design Phase

The system design helps in specifying hardware and system requirements and helps in defining the overall system architecture.

Development Phase

This is the actual coding where each sprint is developed and tested for functionality at the end.

Testing Phase

Unlike Waterfall model, testing is continuous in Agile model and occurs at every sprint.

Deployment Phase
After successful testing, the increment is deployed to production or staging environment. In secure online transaction system, this phase is rolled out in stages (e.g., internal banking staff, limited customers, then full launch).

Review Phase
This phase involves a review team conducting a meeting to demonstrate what was gathered from stakeholders, and provide feedback on security or any other issues and changes to be included to the project backlog for the next sprint.

Maintenance Phase
Due to some issues that come up based on real-world use and new threats, update patches are released, including better versions to enhance the product. Therefore, maintenance is done to deliver these changes in the customer environment.

III. Development of the Application

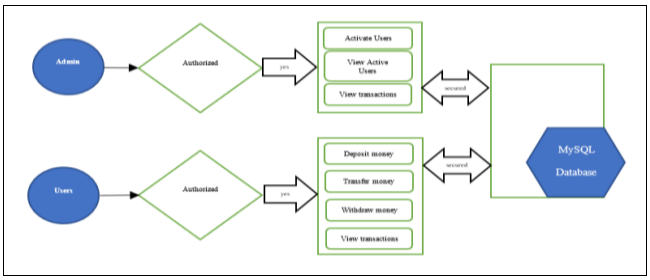
The development of an Online Banking Transaction System followed a structured and iterative approach. The application was developed to address the growing need for secure transmission and actual security of sensitive data being transmitted and stored. The development of the application involves putting the design into functional code. The core functionalities of the system were developed using a combination of the following:

- Front-end development: JavaServer Pages (JSP), HTML, CSS, JavaScript, Bootstrap and Vendor CSS/JS.
- Back-end development: JavaServer Pages supported with Java programming language, and AEScryptography.
- Database: MySQL.
- Data Security: AES encryption.
- Transport security: SSL/TLS – HTTPS.

3.2 System Design

In this study, system design involves the creation of architectural, functional, and data models to visualize and structure the online banking transaction system. The following are the key components:

High Level Architecture
This describes the overall system structure, major components, and interactions.



Source: Author (2025)

Fig 3.2: High level Architecture

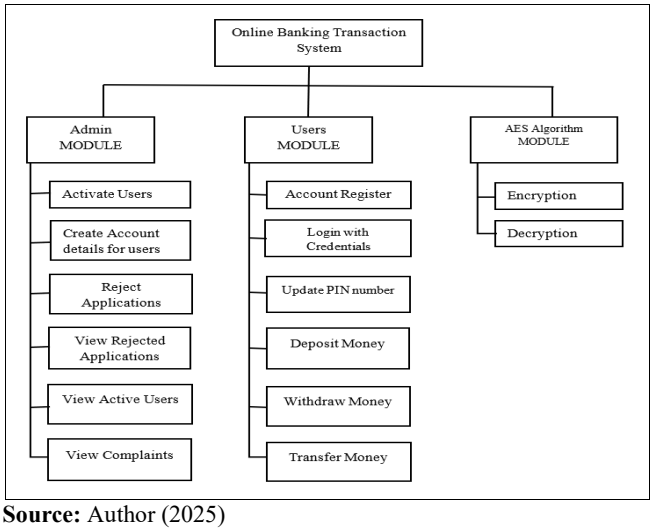
Modular Design of the System Functions
By the word modular, meaning the design of the system is broken down into smaller and manageable components whereby each module addresses a specific function within the system. This promotes separation of work, ease of maintenance, flexibility of the system. These core modules interact with one another through well-defined interfaces, ensuring that the system operates cohesively while allowing for independent updates, testing, and scaling.
Below are the core modules of the system:

Admin Module
The Admin module handles the transaction initiation, verification, and authorization of the system securely. It ensures the confidentiality and integrity of transaction data throughout the process. The Admin module comprises the following sub-modules; Activate Users, Create Account details for Users, Reject Applications, View Rejected Applications, View Active Users, View Transactions, and View Complaints.

Users Module
This module provides a user-friendly interface for users to interact with the system. It includes functionalities such as displaying transaction details, managing user settings, and providing feedback to users regarding the status of their transactions. It consists of the following sub-modules; Account Registration Module, Login with Credentials Module, Update Personal Identification Number (PIN), Deposit Money, Withdraw money, and Transfer Money.

Advanced Encryption Standard Algorithm Module
This robust encryption algorithm involves the encryption and decryption of transactional data. It ensures that sensitive information remains confidential during transmission and storage, and maintains its integrity, protecting it from unauthorized access at any point.

Encryption: This sub-module takes the plaintext data and an encryption key as input and generates encrypted ciphertext, ensuring data confidentiality during transmission and storage.
Decryption: This sub-module takes the encrypted ciphertext and a decryption key as input and gives output to the original plaintext data, allowing authorized users to access and interpret the information securely.



Source: Author (2025)

Fig 3.3: Modular Design of the System Functions

4. Results

This study was conducted through a descriptive survey research design. The study targeted Lusaka district of Lusaka province, Zambia. The study administered highly structured questionnaires up to 120 participants who included customers, IT staff, and System Administrators. A personally administered semi-structured questionnaire was the main tool for data collection. The data was tabulated, and analyzed by use of descriptive.

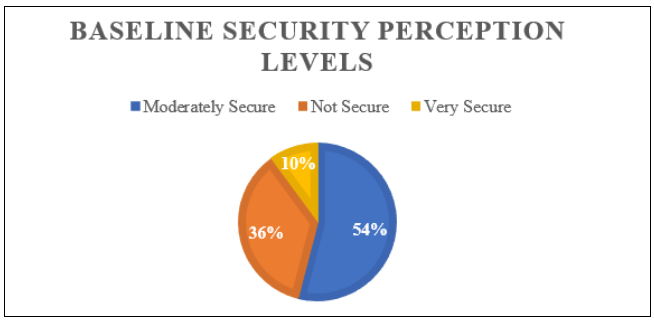
4.1 Baseline Study Results

The baseline study was conducted to observe and understand the current state of the existing system and its vulnerabilities before the development and implementation of the proposed secure online banking transaction system.

4.2 Survey Results and Discussion

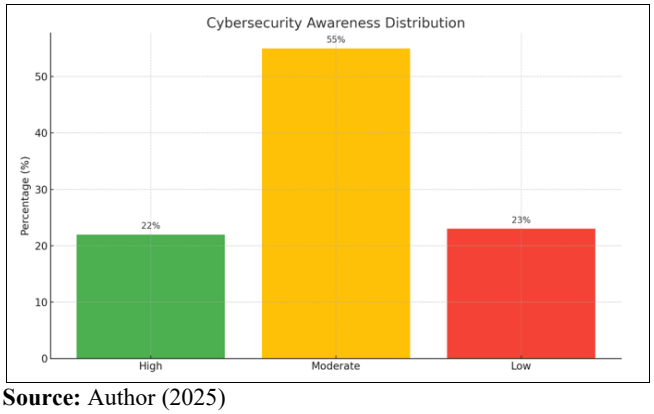
Survey Results:

- **Demographic Information:** From the 120 respondents which are banking staff, IT support, and few selected customers), 67% were from the age group of 25-45 with 46% being female and 54% male. 40% were banking staff, while 25% System administrators, and 35% were customers.
- **Cybersecurity Knowledge:** The cybersecurity knowledge results showed about only 22% of participants had high knowledge with encryption, and phishing prevention. About 55% had moderate knowledge of computer security risks but possessed zero technical knowhow. About 23% had low knowledge of cybersecurity practices.



Source: Author (2025)

Fig 4.1: Baseline Security Perception Levels



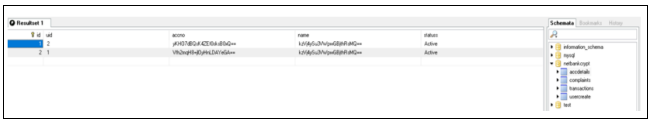
Source: Author (2025)

Fig 4.2: Cybersecurity Awareness Distribution

Discussion

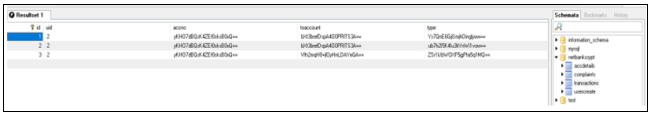
The baseline results show that the use of online banking is high but users lack sufficient cybersecurity awareness. Participants reviewed that the existing system is only moderately secure, with phishing being a top concern. Hence, this justified the inclusion of AES encryption, and session handling.

4.3 System Implementation Results



Source: Author (2025)

Fig 4.3: User account details encrypted with AES



Source: Author (2025)

Fig 4.4: User transaction details encrypted with AES

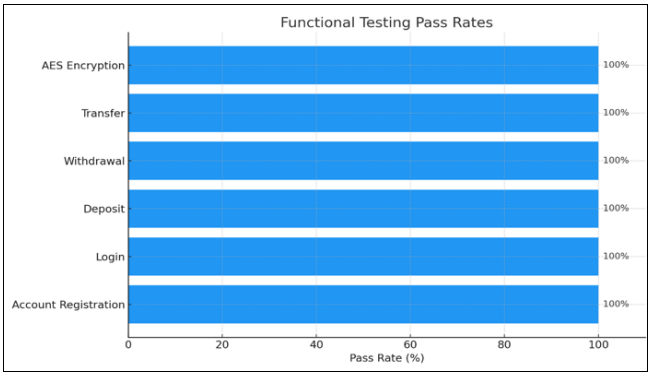
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and a finished product.

Following the Agile-based development and incremental integration, the proposed system was tested under multiple scenarios.

Test Results:

Underlisted are tests that the system under-went which are, functional testing, usability testing, security testing, and performance testing:

Functional Testing: This testing focuses on validations such as identified classes of valid input must be accepted, identified classes of invalid input must be rejected, identified functions and classes of application outputs must be exercised. The results showed that all modules executed successfully. Other results showed that AES encryption and decryption consistently secured transaction data without failure, and no duplicate accounts allowed, and input validation worked as intended. All functional test cases were 100%.



Source: Author (2025)

Fig 4.5: Functional Testing Pass Rates

- **Usability Testing:** A group of 15 users participated in user testing (5 banking staff, 5 IT administrators, and 5 customers) were asked to navigate through the system. Most users found the system intuitive and easy to use. Users rated the system components out of a scale of 5.

- Ease of navigation: 4.6
- Mobile responsiveness: 4.4
- Transaction clarity: 4.5
- Overall satisfaction: 4.7

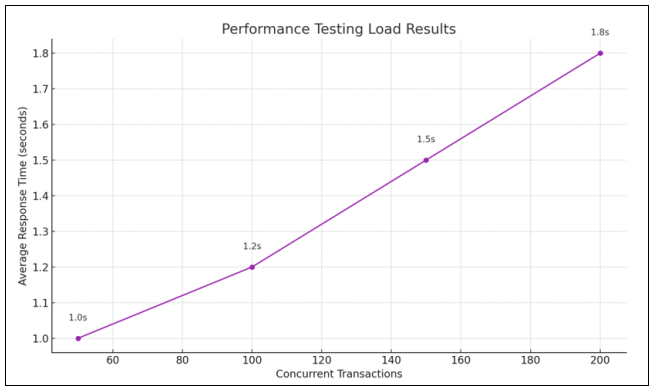
However, some users confirmed that the system interface was clean, and had fast response time but further suggested that the navigation to have dark mode, and integrate biometric authentication.

Performance Testing: This testing shows how well the system handled multiple users simultaneously. The processing speed for the system combining average encryption and transaction time was 1.2 seconds, which was also able to handle approximately 200 concurrent transactions in 1.8 seconds as average response time. During system uptime test, 99.8% was an error rate in less than 0.5%. It was observed that the system maintained stable performance under heavy load.

Table 4.1: Performance Testing Load Results

Current Transactions	Average Response Time (s)
50	1.0 Seconds
100	1.2 Seconds
150	1.5 Seconds
200	1.8 Seconds

Source: Author (2025)



Source: Author (2025)

Fig 4.6: Performance Testing Load Results

- **Security Testing:** Functional, usability, and performance testing are complemented by security testing which focuses on threats, and vulnerabilities. Security testing involves techniques such as penetration testing, and vulnerability scanning to counter data breaches and other threats.

4.4 Data Analysis

The data analysis section presents an evaluation of the results obtained from both the baseline study and the implementation tests. The purpose of this analysis is to interpret and validate the results of both the baseline study and the system implementation tests, showing; whether the proposed solution meets the research objectives, how the solution addresses the gaps identified in the baseline study, and evaluation of the system's effectiveness.

Analysis of Baseline Study Results:

The baseline study showed the existing system exhibited significant gaps in regard to end-user awareness. This validated the need for a robust encryption-based security framework combined with user education.

Analysis of System Implementation Results:

The system's functional, usability, performance, and security tests demonstrated that the developed system met its core objectives which are secure transactions, improved usability, and resilience under high load. Role-Based Access Control (RBAC) effectively limited to admin-only operations. During penetration testing, AES implementation prevented unauthorized access to data.

5. Discussion and Conclusion

5.1 The Baseline Study

The document reviews various existing approaches for online transaction systems. The shortcomings of these methods, such as lack data integrity and security, poor authentication techniques, and lack of a user-friendly interface, are highlighted as the baseline against which the new system is compared. The project is yet and the system has to be fully developed to counter the henceforth mentioned problems in encryption and security vulnerabilities.

5.2 Use of Technology

The utilized technologies were Java, MySQL and AES encryption. The application will be accessed through a browser interface with internet connection, where the interface would be viewed. The software would prove compatibility, scalability, and high performance on all browsers.

5.3 Development of the System as a Solution

The development process followed the Agile methodology, which allowed iterative testing and refinement of key components, including user registration, authentication, encryption, and transaction modules. Functional testing results showed 100% success across all core operations; registration, deposit, withdrawal, transfer, and AES encryption demonstrated that the system achieved its intended objectives.

Performance testing revealed that 99.8% uptime was achieved with over 200 simultaneous transactions in average response time 1.2 seconds which uproars the system to scalability and reliability.

The effectiveness of the system showed that integrating Java with MySQL and AES encryption mitigates data breaches, theft identity, and SQL injection.

5.4 Comparison with other similar Works

In comparing the developed system with other works, similarities were observed:

- Sharma and Bohra (2017) [8] proposed a cryptographic hybrid model to explicitly combine AES and RSA for encryption of data but did not implement it due competent reliable live systems.
- Mambo and Odhiambo (2019) [16] developed machine learning system for enhanced fraud detection. This study provided an easy to use all in one system that could detect credit-card fraudulent transactions and accounts marked for fraudulent activities. Through this combination of cutting-edge machine learning algorithms and rule-based approach, the system effectively differentiated between legitimate and fraudulent in a financial ecosystem, at the same time lacked data encryption integration.

- V. Reddy and T. Anusha (2015) [17] proposed a payment system for online shopping by combining text-based steganography and visual cryptography that provided customer data privacy and prevented misuse of data at the merchandiser's side. The computing implicated only with the prevention of identity theft and customer data security. The system only focused on AES for speed and efficiency.
- A. M. Aburbeian and M. Fernandez-Veiga (2024) [18] proposed a framework that combines multi-factor authentication and machine learning to increase the safety of online financial transactions, address usability, efficacy, and the dynamic nature of various e-commerce platform features. The system achieved about 97% accuracy in fraud prevention.

5.5 Possible Applications

Secure Online Banking Transaction system can be deployed in financial institutions such as commercial banks, E-Commerce platforms, Water utility systems, Electricity utility systems, Government bus systems, and Academic training institution systems. The system secures user authentication, encrypts data, and protect funds during transmission using AES encryption algorithm. Its architecture supports tax revenue, and driver's license renewals. It can also serve as a teaching model for cyber-security and cryptographic courses that focuses on real world encryption system design.

5.6 Summary

The study was successful in design development and testing an online banking transaction using Java technology and AES encryption algorithm. The studies baseline showed weak encryption but the developed system revealed an achievement of 100% performance in functionality and user satisfaction. It also revealed that combining and integrating AES with Java technology mitigates the risk of fraud and data breach.

5.7 Conclusion

The encryption computational models were chosen in this project after extensive research, and the successful testing results confirmed that the choices made by the researcher were reliable. The current online transaction system with AES encryption did not meet the banking standard accuracy of over 98%, due to the limited number of bits used for cryptographic transformation.

This system was tested under robust conditions and it envisaged that real-world performance will be more accurate, proving its security and user-friendliness. The front view online banking system displayed virtually perfect accuracy and in the researcher's opinion further work need not be conducted in this area.

The primary goal of this project, developing a secure, robust, and user-friendly online banking system was achieved through the implementation of AES encryption which demonstrated significant improvement in enhanced data security.

The system not only met all the stated objectives but also contributed to addressing the cybersecurity challenges faced by financial institutions in Zambia and similar contexts. This study underscores the importance of integrating encryption and secure communication technologies into financial systems to combat modern cyber threats and enhance system user trust in online transactions.

5.8 Future Works

The achieved its goal and met the required objectives. Therefore, future improvements can include the following:

- Biometric Authentication: Incorporating the use of physical characteristics of an individual such as facial features, iris scans or fingerprints to verify their identity before granting access to sensitive data or systems (Jain, Ross and Nandakumar, 2019; Ratha, Connell and Bolle, 2020) [19, 20].
- Blockchain Integration: Powerful technology which creates an immutable record of transactions that can be used to optimize business processes, enhance security, and maintain trust between stakeholders. It reduces costs by removing middlemen and ensuring that transactions are quickly and accurately fulfilled (Yaga *et al*., 2019; Casino, Dasaklis and Patsakis, 2020) [21, 22].
- Artificial Intelligence-based Fraud Detection: Implementing machine learning algorithms to mitigate fraudulent activities. By analyzing datasets, AI models can learn to recognize the difference between suspicious activities and legitimate transactions, and they can help identify possible fraud risks to prevent financial crime, or even catching trends that a human agent might miss (Bahnsen *et al*., 2019; Dal Pozzolo *et al*., 2021) [23, 24].
- Cybersecurity Awareness Programs: Developing cybersecurity features within the system that increases the users understanding of cyber threats empowering them to be safer and more secure online (Parsons *et al*., 2019; ENISA, 2023) [25, 26].
- Elliptic Curve Cryptography (ECC): Combining ECC with AES to enable stronger security with smaller key sizes compared to other methods (NIST, 2018; Hankerson, Menezes and Vanstone, 2020) [27, 28].
- Post-Quantum Cryptography (PQC): Classical cryptography relies on the difficulty of specific mathematical problems, such as factoring large numbers or solving discrete logarithms which quantum computers can efficiently solve. PQC combined with AES can withstand quantum capabilities much better (Chen *et al*., 2019; NIST, 2023) [29, 30].

6. Acknowledgements

First and foremost, I would like to thank Jehovah God for the gift of life, strength sustenance and good health he has rendered to me during the course of doing my project. I would like to thank my project supervisor and inspiration Mr. Moses Mupeta for his guidance throughout this research.

I would also like to thank the management of the University for according me the chance to pursue my studies. I would also like to acknowledge all the lecturers from the School of Engineering.

7. References

1. Zambia Information and Communications Technology Authority (ZICTA). Annual cybersecurity report 2023/2024. Mobile Banking Security, 2024, 45-53. Retrieved from: www.zicta.zm. [Accessed 9 May. 2025].
2. Deloitte. Cyber security outlook–Africa edition. Financial Institutions Under Attack, 2022, 10-18. Retrieved from: www.deloitte.com. [Accessed 9 May.

2025].
3. Check Point Research. Network security trends and applications. In A study on the existing cybersecurity policies Zambia, 2023a, 5-15.
4. Paar C, Pelzl J. Understanding cryptography: A textbook for students and practitioners. Springer, 2010, 97-140.
5. IBM. Encryption and AES Best Practices. Data Protection for Enterprises. AES Implementation Guidelines, 2021, 4-9.
6. Macrium Software. What is the Advanced Encryption Standard (AES)? AES Overview, 2023, 2-6.
7. Rescorla E. SSL and TLS: Designing and building secure systems. Addison-Wesley, 2008, 89-115.
8. Sharma N, Bohra B. Enhancing online banking transaction using hybrid cryptographic method. In IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), India, 2017, 1-6.
9. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. CRC Press, 1996, 235-270.
10. Mavroeidis V, Tzovaras D, Strintzis MG. An overview of internet security and its applications. IEEE Signal Processing Magazine. 2007; 24(6):64-78.
11. Kaspersky. Online Transaction in Financial Services. Threat Landscape, 2022, 12-20.
12. Oracle. MySQL 8.0 Secure Development Guide. Security Encryption, 2021, 30-38.
13. Khairnair S, Kharat R. Online Fraud Transaction Prevention System using Extended Visual Cryptography and QR Code. IEEE-ICCUBEA, 2016, 85-90.
14. Sasikumar K, Nagarajan S. Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques, 2022.
15. Dyba T, Dingsoyr T. Empirical studies of agile software development: A systematic review. Information and Software Technology. 2008; 50:833-859.
16. Mambo J, Odhiambo C. Anomaly detection in financial transactions using machine learning: A case study of East African banks. African Journal of Information Systems. 2019; 11(3):121-147.
17. Reddy VL, Anusha T. Combine use of steganography and visual cryptography for online payment system. International Journal of Computer Applications. 2015; 124(6):22-29.
18. Aburbeian AM, Fernandez-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI. 2024; 5(1):177-194.
19. Jain AK, Ross A, Nandakumar K. Introduction to biometrics. New York: Springer, 2019.
20. Ratha NK, Connell JH, Bolle RM. Biometrics: Concepts and applications. New York: Springer, 2020.
21. Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology, 2019.
22. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telecommunications Systems. 2020; 74(2):163-180.
23. Bahnsen AC, Torroba R, Buzeto F, Vilalta R. Cost-sensitive decision trees for fraud detection. Expert Systems with Applications. 2019; 132:274-283.
24. Dal Pozzolo A, Bontempi G, Snoeck M, Snoeck M. Adversarial drift detection for fraud prevention. IEEE Transactions on Neural Networks and Learning Systems. 2021; 32(9):4033-4045.
25. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. The design of phishing studies: Challenges for researchers. Computers & Security. 2019; 79:180-191.
26. ENISA. Cybersecurity awareness and training for organizations. European Union Agency for Cybersecurity, 2023.
27. NIST. Digital Signature Standard (DSS). FIPS PUB 186-4. Gaithersburg, MD: National Institute of Standards and Technology, 2018.
28. Hankerson D, Menezes A, Vanstone S. Guide to elliptic curve cryptography. 2nd edn. Cham: Springer, 2020.
29. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, *et al*. Report on post-quantum cryptography. NISTIR 8105. Gaithersburg, MD: National Institute of Standards and Technology, 2019.
30. NIST. Post-quantum cryptography standardization. Gaithersburg, MD: National Institute of Standards and Technology, 2023.