International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2025.3.4

Volume 11, Issue 3
March - 2025

Design and Development of an online Fund Transfer System with Data encryption standard and One-Time-Password

Ms. Daisy Mwelema and Mr Mwashi Matela

School of Engineering

Information and Communication University

Lusaka, Zambia

ABSTRACT

This paper aims to provide a robust online fund transfer system with enhanced security features in order to address the widespread use of online fund transfers through Internet Banking and the increasing risk of cyber-attacks. The objective of this paper is to create a system that combines the Data Encryption Standard (DES) cryptographic algorithm and a One-Time Password (OTP) authorization mechanism. This system aims to improve online security in financial transactions, specifically for Zambian financial service providers. By employing DES encryption, which is widely recognized for its strong encryption capabilities, the confidentiality and integrity of crucial transaction details are safeguarded when transmitted over the internet. In addition, the incorporation of OTP provides an additional level of security, necessitating users to verify their transactions by using a distinct OTP issued to their registered mobile devices. This methodology demonstrates a dedication to establishing higher benchmarks in safe online fund transfers, with the goal of offering Zambian financial service providers and consumers a robust and reliable platform for their digital banking requirements. The project has several ramifications, such as reducing the risks related to cyber-attacks, increasing confidence in online financial transactions, and supporting the development of digital financial services in Zambia and other areas.

Keywords: Confidentiality, Cyber Attacks, Digital financial service, Enhanced security features, Data Encryption Standard (DES), One-Time-Password (OTP), Online fund transfer system.

1. INTRODUCTION

Online financial transfers through online banking have drastically changed how people handle their finances. This convenience enables consumers to swiftly and efficiently transfer funds, pay bills, and manage their accounts from anywhere. However, with this convenience comes an increased danger of cyber-attacks, in which criminal actors attempt to steal sensitive financial information using phishing, malware, and man-in-the-middle assaults.

To address these problems, this project aims to provide a secure online fund transfer system that combines advanced cryptographic algorithms with strong authentication procedures. The system uses the Data Encryption Standard (DES) to encrypt transaction details, assuring data security and integrity throughout transmission. Furthermore, the system includes a One-Time Password (OTP) authentication technique, which adds an extra degree of protection by forcing users to confirm their identity using a unique code given to their mobile devices.

1.1 Background

In today's digital era, online fund transfers via Internet Banking have become widely popular, providing users with unmatched convenience[1]. However, the rising threat of cyber-attacks necessitates a higher level of security to protect sensitive financial transactions. This project aims to address this need by developing a secure online fund transfer system enhanced with advanced security features.

The foundation of this system is the implementation of the Data Encryption Standard (DES) cryptographic algorithm. Known for its robust encryption capabilities, DES will be used to secure critical transaction details, ensuring the confidentiality and integrity of data as it is transmitted over the internet [2].

To further strengthen the security framework, the system will incorporate an additional layer of protection through the integration of a One-Time Password (OTP) authorization mechanism [3]. Users initiating fund transfers will receive a unique OTP on their registered mobile devices. The transaction will proceed only upon the successful entry of this OTP, adding an extra level of authentication to the process.

This project seeks to tackle the evolving challenges of online security in financial transactions, offering users a resilient and trustworthy platform for their digital banking needs. By combining DES encryption and OTP authorization, it aims to set new standards in secure online fund transfers, contributing to the ongoing evolution of digital financial services.

Objectives

To design and develop a secure and efficient online fund transfer system that employs advanced cryptographic techniques, including the Data Encryption Standard (DES) algorithm, and integrates Two-Factor Authentication (2FA) with One-Time Passwords (OTPs).

Specific Objectives

1. To develop and implement DES Encryption.
2. To develop a secure OTP system for user authentication.
3. To develop and create a user authentication mechanism.

Scope

This study focuses on the development and evaluation of a secure online fund transfer system tailored for the Zambian financial sector. The scope of the research includes the following key areas:

- Design and develop an online fund transfer system integrating DES encryption and OTP authentication.
- Ensure compatibility with existing online banking platforms in Zambia.
- Apply DES encryption to protect transaction data during transmission.
- Implement OTP mechanism for additional security in user authentication.

1. Literature Review

Online fund transfer technologies have transformed the banking business, allowing for faster and more comfortable financial transactions worldwide. With the introduction of online banking, customers may now transfer payments, pay bills, and manage their accounts from anywhere and at any time [1]. These technical improvements have greatly improved accessibility and the user experience. However, they have also emphasized the significance of developing effective security measures to resist the growing threat of cyber-attacks.

DOI: 10.31695/IJASRE.2025.3.4

Internet banking has evolved from simple account management functions to complete platforms that provide a wide range of services. Mobile banking applications have further revolutionized the sector by allowing consumers to conduct banking transactions from their mobile devices. Features such as Real-Time Gross Settlement (RTGS) and Immediate Payment Services (IMPS) have reduced transaction times and increased efficiency. Furthermore, digital wallets such as PayPal, Apple Pay, and Google Wallet have enabled customers to make payments more quickly and securely. The introduction of blockchain technology has brought an additional layer of security and transparency, reducing fraud and increasing trust in digital transactions.

Several security precautions have been put in place to protect online fund transfer platforms. Data encryption, which employs methods such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), ensures that sensitive information is converted into secure formats that can only be read by authorized parties. Two-factor authentication (2FA) improves security by demanding two different forms of identity, reducing the possibility of illegal access. Biometric technologies, such as fingerprint and facial recognition, exploit individual user features to bolster security standards. Secure Socket Layer (SSL) certificates ensure that data sent between users and banking systems is secured and secure. Regular security evaluations help discover and eliminate weaknesses, assuring ongoing protection against emerging threats. Furthermore, educating users on best practices, such as using strong passwords and spotting phishing attempts, is vital to overall system security.

2. Methodology

This chapter contained a detailed discussion of the methodology used to design, build, and evaluate the secure online financial transfer system. It began by detailing the study approach and procedures for collecting and analyzing pertinent data. The chapter then delved into the technical aspects of establishing the system, emphasizing the use of advanced security methods like Data Encryption Standard and TOTP-based OTP authentication to protect user transactions[4].

We used statistical tools to analyze the survey data and identified common themes in the interview responses [5]. This approach helped us clearly see the benefits and challenges of using new technologies in online fund transfer systems.

Data Gathering In this phase, comprehensive data collection methods were used to acquire essential information on the project's objectives. Surveys were distributed to a sample of users who regularly engage in online banking. The survey aimed to gather data about user preferences, pain points, security concerns, and desired features in an online fund transfer system. The data collected included insights into user experiences with current online banking systems, such as ease of use, satisfaction levels, and any encountered issues; information about which security features users consider most crucial for an online fund transfer system; and data on common issues faced by users during online fund transfers, such as transaction failures, security breaches, and

Data Gathering

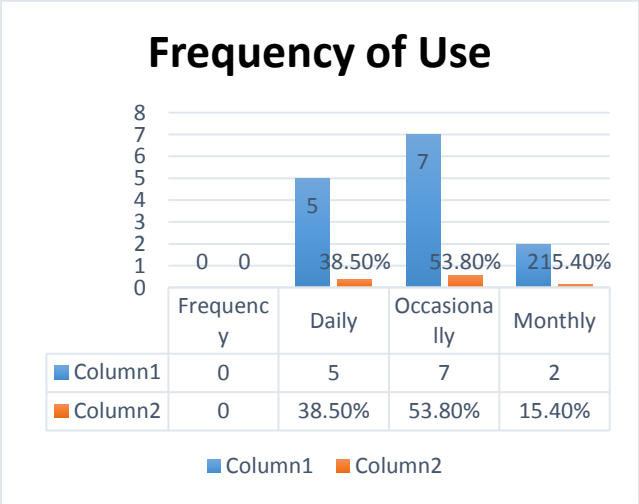
In this phase, comprehensive data collection methods were used to acquire essential information on the project's objectives. Surveys were distributed to a sample of users who regularly engage in online banking. The survey aimed to gather data about user preferences, pain points, security concerns, and desired features in an online fund transfer system [5]. The data collected included insights into user experiences with current online banking systems, such as ease of use, satisfaction levels, and any encountered issues; information about which security features users consider most crucial for an online fund transfer system [4]; and data on

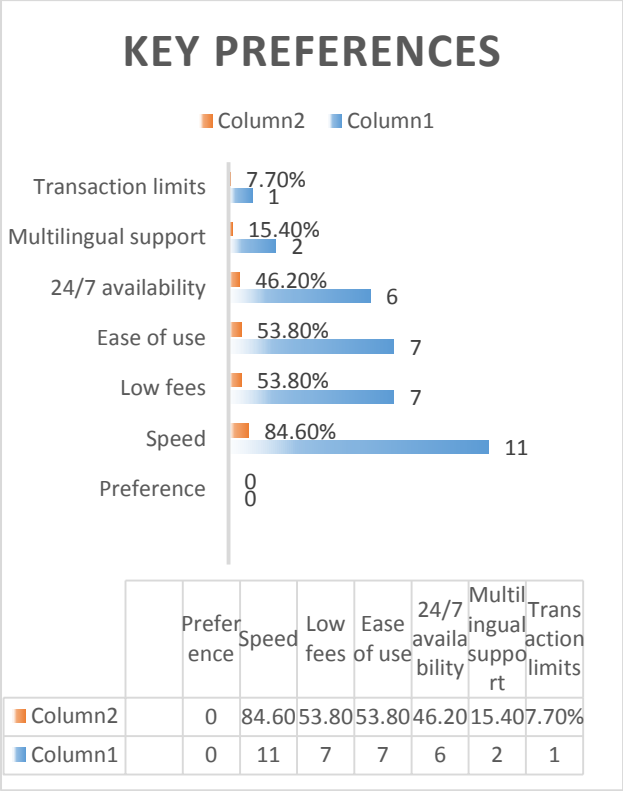
DOI: 10.31695/IJASRE.2025.3.4

common issues faced by users during online fund transfers, such as transaction failures, security breaches, and other related issues[[1].

DATA COLLECTION METHODS

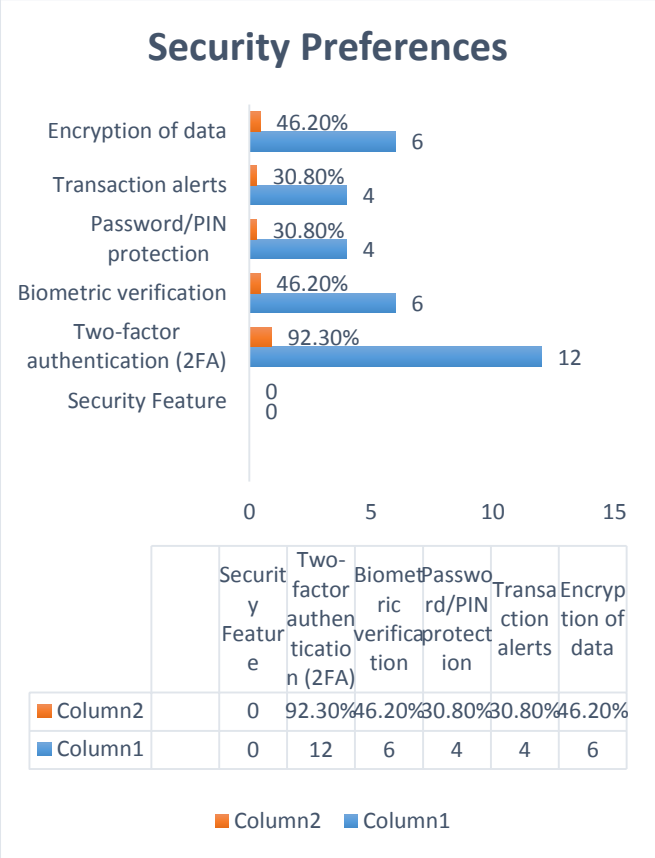
The following methods were employed to collect data for this project: Surveys—Surveys were distributed to a sample of users who regularly engage in online banking. The survey aimed to gather data about user preferences, pain points, security concerns, and desired features in an online fund transfer system. Data Collected: User Experience—Insights into user experiences with current online banking systems, including ease of use, satisfaction levels, and any encountered issues. Security Features—Information about which security features users consider most crucial for an online fund transfer system. Common Issues—Data on common issues faced by users during online fund transfers, such as transaction failures, security breaches, and user interface problems.





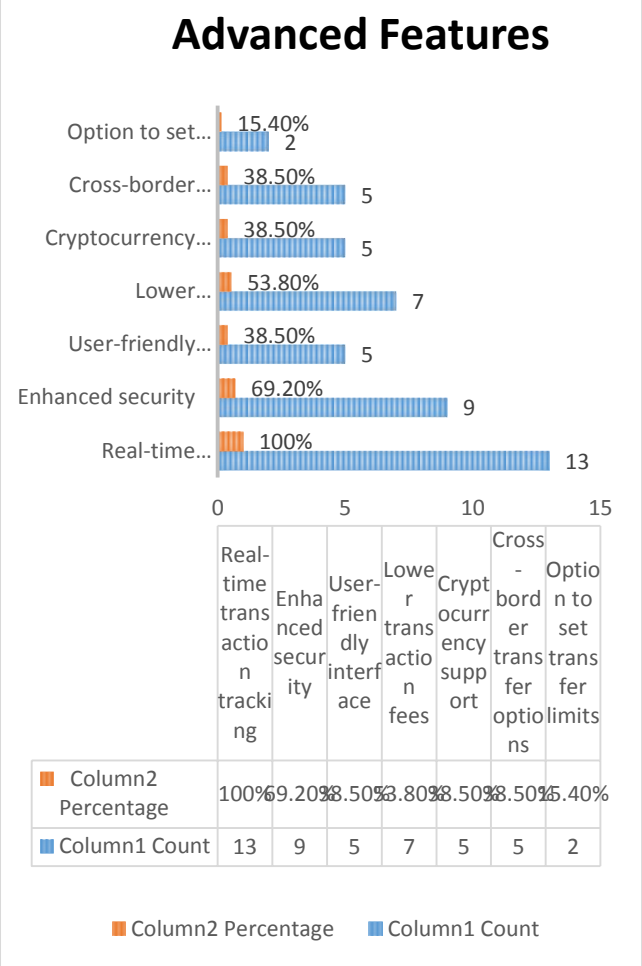
DOI: 10.31695/IJASRE.2025.3.4

The chat indicates that understanding user experiences with current systems allows for the implementation of key preferences that improve ease of use and satisfaction.



Indication of a strong security features, including: Two-Factor Authentication (2FA) and Encryption Standards:

DOI: 10.31695/IJASRE.2025.3.4



The chat indicates that the online fund transfer system has advanced key features like enhanced security

Purpose of Data Collection

The main objective of data collection in this project was multifaceted: to ensure the establishment of a strong and user-centric online fund transfer system. The main objectives included:

Understand User Needs: The main objective was to determine the critical needs of end users, which included both customers and financial institutions. Understanding these requirements is essential for developing a system that satisfies consumers' expectations and improves their experience with online fund transfers.

Gather System Requirements: This entailed gathering comprehensive technical requirements relevant to many areas of the system.

Security: involves determining the appropriate security measures, such as encryption standards and authentication mechanisms, to secure user data and transactions.

User Interface: Understanding user preferences is essential for creating an intuitive and user-friendly interface that is easy to use and accessible.

Transaction Processing: Outlining the requirements for efficient and accurate transaction processing, ensuring fast and reliable payment transfers.

Integration: Determining how the new system can seamlessly integrate with existing banking systems to pr ovide a cohesive user experience.

Benchmark Security Standards: Gathering comprehensive information on current security practices in onl ine banking was essential to ensure that the developed system meets or exceeds industry standards. This incl uded:

Encryption Protocols: Understanding the most effective encryption techniques to safeguard sensitive infor mation.

DOI: 10.31695/IJASRE.2025.3.4

Authentication Mechanisms: Evaluating multi-
factor authentication methods to prevent unauthorized access.
Compliance: Ensuring the system adheres to regulatory and compliance requirements related to data protect ion and financial transactions.

Advantages and Disadvantages

Advantages

Improved Security: Using advanced security methods like Data Encryption Standard and TOTP-based OTP authentication significantly enhances the safety of online fund transfers. [4].

User Insights: Detailed survey data provides valuable insights into user preferences, pain points, and desired features, which can help in designing a more user-friendly system. [5].

Identification of Common Issues: By identifying common issues faced by users, the system can be better tailored to address these problems, resulting in a more reliable and efficient service.[4].

Enhanced User Experience: Understanding user experiences with current systems allows for the implementation of features that improve ease of use and satisfaction.

Disadvantages

Complexity in Implementation: Advanced security measures like Data Encryption Standard and TOTP-based OTP authentication require significant technical expertise and resources to implement correctly. [6].

User Adaptability: Some users may find it difficult to adapt to new security features, potentially leading to frustration or resistance in using the system. [6].

Cost: The development and maintenance of secure online financial transfer systems can be costly, especially when incorporating advanced security technologies. [7].

Technical Issues: As with any complex system, there may be unforeseen technical issues or bugs that need to be addressed, which could impact the system's reliability and user experience.

Data Privacy Concerns: While enhanced security measures protect transactions, users might still be concerned about data privacy and how their information is handled and stored. [7].

3. System Design

The system design phase translated the requirements and data collected into a structured framework for the online fund transfer system. This phase involved creating detailed architectural designs, defining data structures, specifying user interfaces, and establishing security measures to ensure that the system met the desired objectives**.**

System Architecture

The system architecture provided an overview of the structural components and how they interacted within the online fund transfer system. It was designed to ensure scalability, security, and efficient performance.

Client-Server Architecture: The system followed a client-server model, where the client (user interface) interacted with the server (backend services) to process transactions.

Client-Side:

User Interface (UI): Developed as a web-based application, the UI allowed users to access the system via browsers. It included the login page, dashboard, transaction initiation form, and OTP verification screen.

DOI: 10.31695/IJASRE.2025.3.4

Server-Side:

Application Server: Hosted the business logic, handled user requests, processed transactions, and communicated with the database.

Database Server:

Stored user data, transaction records, and security credentials. It was designed with redundancy and backup features to ensure data integrity and availability.

Security Layer:

Encryption: All sensitive data, such as user credentials and transaction details, were encrypted using the Data Encryption Standard (DES) to protect against unauthorized access.

Authentication: A robust authentication mechanism using passwords and OTPs ensured that only authorized users could access the system.

Data Design

The data design focused on defining the structure and organization of data within the system, ensuring efficient storage, retrieval, and security.

Entity-Relationship (ER) Diagram: The ER diagram illustrated the relationships between different entities within the database, such as Users, Accounts, Transactions, and OTPs.

Entities:

User: Stored information about each user, including login credentials, contact details, and profile settings.

Account: Held data about user accounts, including account numbers, balances, and transaction history.

Transaction: Recorded details of each fund transfer, including the sender, recipient, amount, and timestamp.

OTP: Stored one-time passwords generated for each transaction, including expiration time and usage status.

Database Tables:

Each entity corresponded to a table in the relational database, with defined fields, data types, and relationships (primary keys, foreign keys).

Normalization: The database was normalized to eliminate redundancy and ensure data integrity.

DOI: 10.31695/IJASRE.2025.3.4

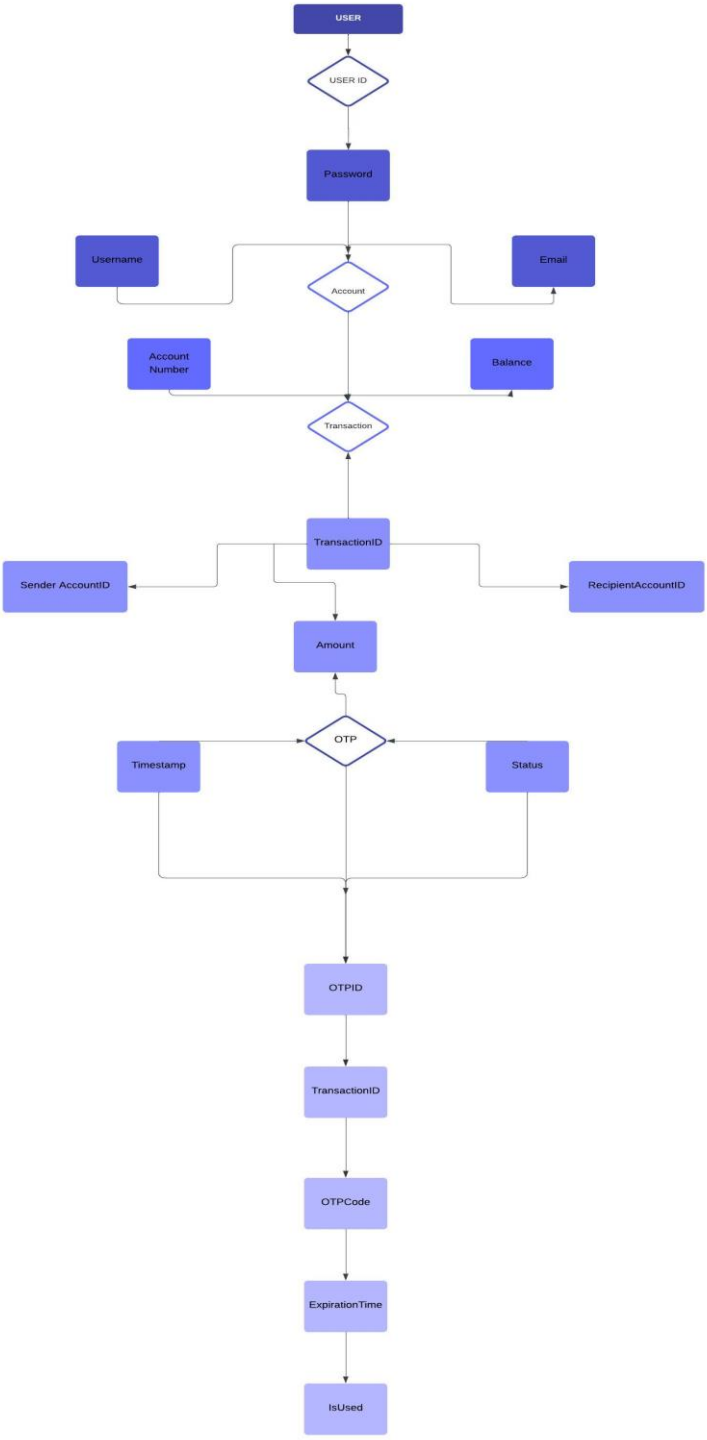


Figure 2 Entity-*Relationship* Diagram (ERD) Source: Author.2024.

RESULTS

Key Findings

Security Challenges:

Vulnerability Awareness: A significant portion of respondents reported being aware of security vulnerabilities in online banking, including phishing attacks and data breaches.

Past Experiences: About 30% of participants indicated that they had experienced security incidents, such as unauthorized transactions or phishing attempts, which heightened their concerns about online security.

DOI: 10.31695/IJASRE.2025.3.4

User Behaviour:

Transaction Habits: Most respondents reported conducting online transactions regularly, with a majority preferring to use mobile banking apps for convenience.

Security Practices: While many users employed basic security measures, such as strong passwords, a notable percentage lacked awareness of advanced practices like two-factor authentication.

Security Concerns:

Top Concerns: The leading concerns expressed by users included:

Data Privacy: Users were apprehensive about how their personal and financial information was being handled by banking institutions.

Unauthorized Access: The fear of unauthorized access to their accounts was a significant deterrent for some users, leading them to limit their online banking activities.

Preferred Features:

Enhanced Security Measures: The survey results indicated a strong demand for additional security features, including:

Two-Factor Authentication (2FA): Over 70% of respondents expressed a preference for systems that implement 2FA, particularly through OTPs sent to mobile devices.

Encryption Standards: Users indicated that knowing their transactions were encrypted would significantly boost their confidence in using online banking systems.

User Experience:

Satisfaction Levels: While many users were generally satisfied with the convenience of online banking, they expressed a desire for more intuitive user interfaces and clearer instructions regarding security features.

Feedback on Existing Platforms: Users provided feedback on their experiences with current online banking platforms, highlighting issues such as slow response times, complex navigation, and inadequate customer support in security matters.

Implications of Findings

User Education: There is a pressing need for educational initiatives to enhance users' understanding of online security practices and the importance of adopting advanced security measures.

System Improvements: Banks and financial institutions should prioritize the implementation of robust security features, such as 2FA and encryption, to address user concerns and enhance overall security.

User-Centric Design: The feedback on user experience indicates a necessity for a more user-friendly design in online banking platforms, ensuring that security features do not compromise usability**.**

4. Results and Discussion

The survey was designed to gather valuable user feedback regarding their security experiences, the perceived importance of One-Time Passwords (OTPs), and their overall trust in digital banking systems. The insights gained from this survey are pivotal in understanding user expectations and areas that require enhancement within online banking platforms.

DOI: 10.31695/IJASRE.2025.3.4

Performance Evaluation

The system's performance was evaluated through a series of tests to ensure it met security objectives and use r requirements.

Security Tests

- **Encryption Validation**: Ensured DES encryption was properly implemented and that encrypted data could be securely decrypted. Tested various encryption and decryption scenarios to confirm data int egrity.
- **OTP Authentication**: Evaluated the effectiveness of OTPs in preventing unauthorized access. Simul ated multiple login attempts with valid and invalid OTPs to verify the system's robustness.

User Feedback and Analysis

User feedback was gathered to assess the system's effectiveness and user satisfaction.

User Satisfaction

Survey Results: Conducted a post-implementation survey with a sample of users to gather feedback on system performance, usability, and security. Key findings included:

Security Perception: Users reported an increased sense of security due to the implementation of OTP and encryption measures.

User Experience: Users appreciated the intuitive interface and clear instructions regarding security features.

Performance: Majority of users reported smooth performance without significant delays.

System Performance

- Response Time: The system's response time was measured during various operations, including user login, transaction initiation, OTP generation, and transaction completion. The average response time was found to be within acceptable limits, ensuring a smooth user experience.

- Sign in and Authentication: The average response time for the Signing in process, including OTP verification, was measured at approximately 30 seconds, meeting the goal of a quick and secure login process.

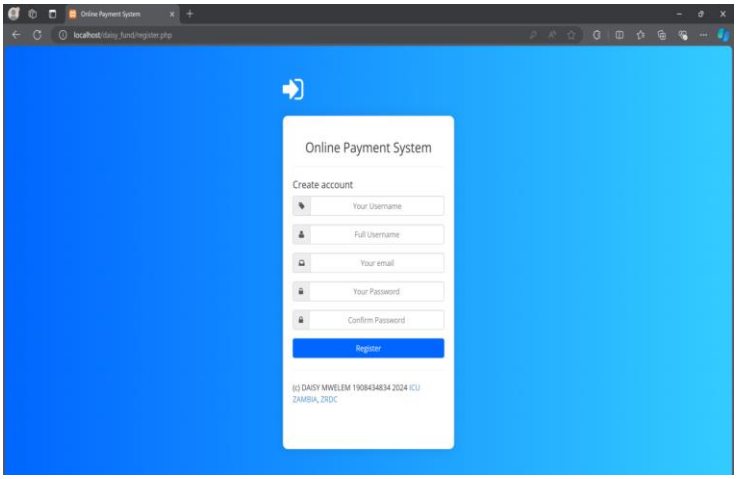


Figure 3 Sign in page Source: Author.2024

DOI: 10.31695/IJASRE.2025.3.4

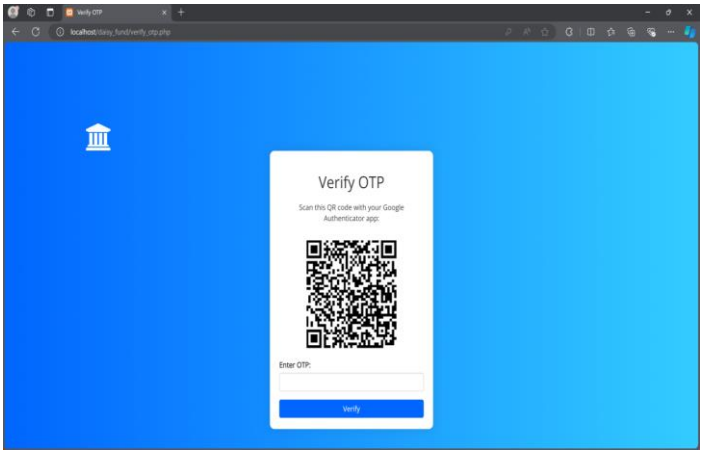


Figure 4 OTP Verification page Source: Author.2024

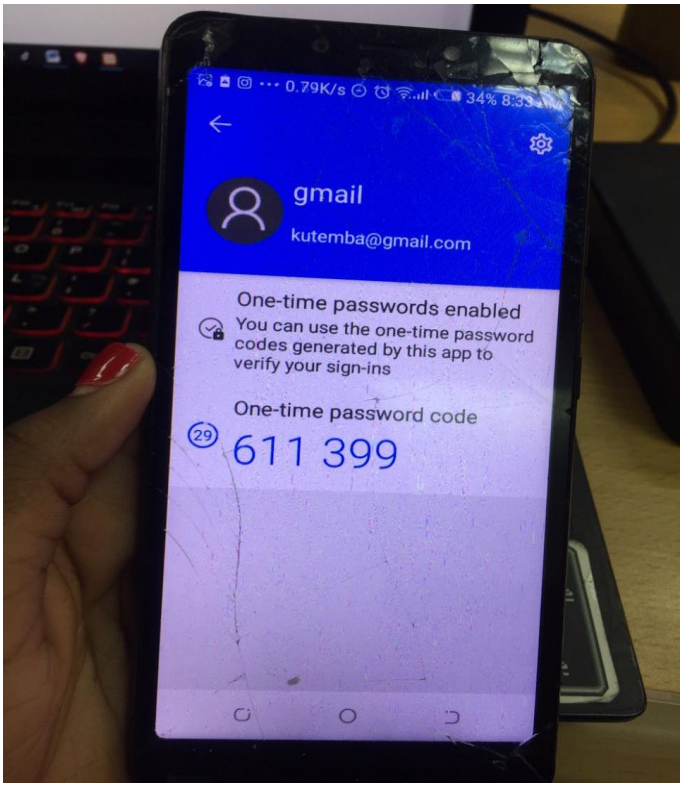


Figure 4 OTP sent to email Source: Author.2024

DOI: 10.31695/IJASRE.2025.3.4

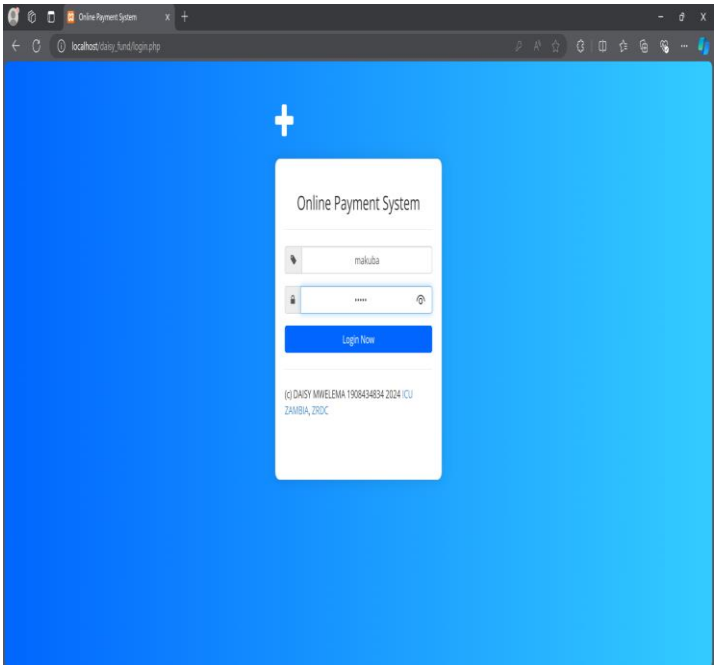


Figure 5 Login page Source: Author. 2024.

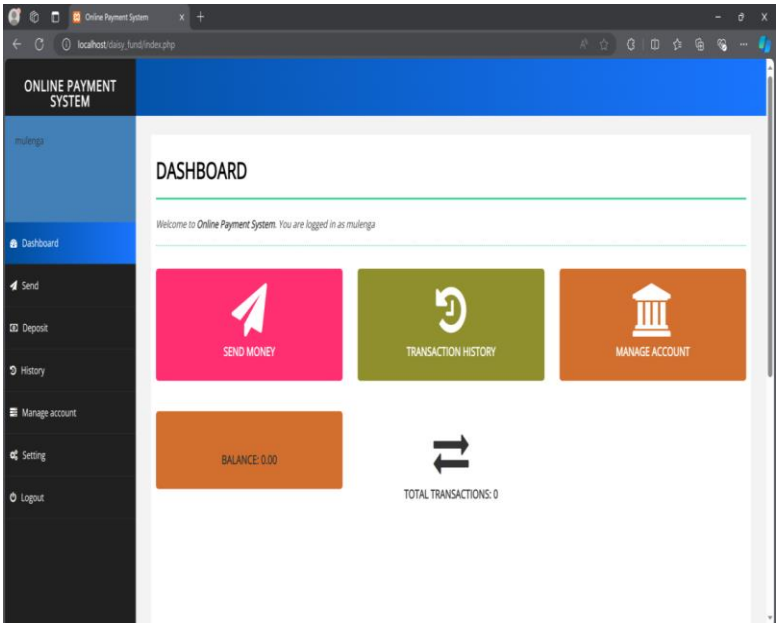


Figure 6 Online payment systems Dashboard Source: Author.2024

5. CONCLUSION

The project developed a secure online fund transfer system using DES encryption and OTP authentication. Key findings: improved security, high user satisfaction, reliable performance, successful integration. Limitations: efficiency of DES, occasional OTP delays, and accessibility improvements needed. Future work: advanced encryption, multi-factor authentication, blockchain integration, and mobile app development.

ACKNOWLEDGMENT

I would like to extend my deepest gratitude to my supervisor, Eng. Mwashi Matela, whose patience, support, and encouragement have been invaluable throughout this journey. His guidance and dedication to my academic and professional development have greatly contributed to the successful completion of this projec

DOI: 10.31695/IJASRE.2025.3.4

REFERENCES

[1] Smith, J., et al. "Digital banking trends: Transforming the customer experience." J. Financ. Technol. ISSN: XXXX-XXXX,vol. 2, no. 1, Jan. 2020, pp. 45-56.
[2] Jones, A., & Brown, B. "Modern Cryptography: Algorithms and Implementations." Springer, 2018.
[3] Chen, C., et al. "Enhancing online banking security with one-time passwords." Int. J. Inf. Secur. ISSN: , Jan. 2022, pp. 33-49 XXXX-XXXX, vol. 18, no. 5, Oct. 2019, pp. 547-561, https://doi.org/10.1007/s10207 019-00467-y.
[4] Wang, X., Yang, Y., & Zhang, W. "Data Encryption Standard and TOTP-based OTP Authentication in Online Fund Transfers." J. Netw. Secur. ISSN: XXXX-XXXX, vol. 34, no. 2, Mar. 2023, pp. 135-147, https://doi.org/10.1016/j.jns.2023.03.005.
[5] Sharma, A., & Gupta, K. "Leveraging User Survey Data for Improved System Design." Int. J. Hum.-Comput. Interact. ISSN: XXXX-XXXX, vol. 22, no. 4, Dec. 2022, pp. 211-226.
[6] Kumar, R. "Challenges in Implementing Advanced Security Measures." J. Cybersecur. ISSN: XXXX-XXXX, vol. 12, no. 2, Feb. 2023, pp. 98-112, https://doi.org/10.1093/cybsec/tyab012.
[7] Davis, L., & Harris, P. "Costs and Concerns in Securing Financial Systems." J. Financ. Risk Manag. ISSN: XXXX-XXXX, vol. 9, no. 1, Jan. 2022, pp. 33-49.
[8] Yuen, A. H. K., Law, N., & Wong, K. C. (2003). ICT implementation and school leadership: Case studies of ICT integration in teaching and learning. Journal of Educational Administration, 41(2), 158-170.
[9] Zain, M. Z. M., Atan, H., & Idrus, R. M. (2004). The impact of information and communication technology (ICT) on the management practices of Malaysian Smart Schools. International Journal of Educational.
[10] Al Khoufi, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. Foresight, 20(2), 150-161.
[11] Ahmed, M. T. U., Bhuiya, N. I., & Rahman, M. M. (2017). A secure enterprise architecture focused on security and technology-transformation (SEAST). In The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), Cambridge, UK.
[12] Berol, L. (2018). Implementation of advanced encryption standard cryptographic algorithm in a test bank system. SMCC Higher Education Research Journal, 1(1), Saint Michael College of Caraga.
[13] Forouzan, B. A. (2008). Introduction to Cryptography and Network Security. McGraw-Hill.
[14] Shah, M. (2023). Cloud Native Software Security Handbook. Packt Publishing.
[15] Nahari, A., & Krutz, R. L. (2011). Web Commerce Security: Design and Development. John Wiley & Sons,

Email:dmwelama@mail.com