IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 2, Ser. 2 (Mar. – Apr. 2026), PP 11-18
www.iosrjournals.org

Strengthening Digital Transaction Security Using Three-Factor Authentication For Virtual Top-Up Systems

Azemobor Daniel[1], Aniji Ifesinachi Veronica [2],
Nwamini Bartholomew Tochukwu[3], Uguru Fidelis Nwagidi [4], Ebiringa Ifeanyi[5]
(ICT Unit/ Evangel University, Akaeze,Ebonyi State, Nigeria)
(Computer Science Department / Evangel University, Akaeze,Ebonyi State, Nigeria)
(Computer Science Department / Evangel University, Akaeze,Ebonyi State, Nigeria)
(Computer Science Department / Alex Ekwueme Federal University, Ndufu-Alike, Ikwo, Ebonyi State, Nigeria)
(Computer Science Department / Federal University Of Technology Owerri)

Abstract:
Digital transaction systems, such as virtual top-up platforms, are widely used for mobile airtime and data purchases. While these systems provide convenience, they are vulnerable to security threats, including fraud, unauthorized access, and identity theft. Traditional authentication methods, such as passwords or simple OTPs, are no longer sufficient to protect sensitive user information and financial transactions. This paper presents a three-factor authentication system designed to enhance security in virtual top-up platforms. The proposed system combines something the user knows (password), something the user has (encrypted one-time password sent to the registered device), and something the user is (biometric verification). In this approach, the OTP is encrypted before being sent to the user's device to prevent unwanted access or viewing. The user then decrypts the OTP using their password before completing the virtual top-up transaction. This additional encryption and decryption step strengthens the overall security of the authentication process and reduces the risk of OTP interception or misuse. The system was implemented in a mobile-based environment and evaluated for security and usability. Results show that the proposed three-factor authentication system significantly improves transaction security compared to conventional authentication methods while maintaining ease of use for the user. This study demonstrates that combining OTP encryption with multi-factor authentication is an effective approach to securing virtual top-up systems and other digital financial services.

Keywords: *Three-Factor Authentication, OTP Encryption, Digital Transaction Security, Virtual Top-Up System, Mobile Payment Security*

Date of Submission: 20-04-2026 Date of Acceptance: 30-04-2026

I. Introduction

Digital and mobile transactions have become an important part of everyday life as smartphones and internet services allow people to send money, pay bills, and purchase goods from anywhere. Financial technology (FinTech) has enabled secure and fast digital payment systems that are widely adopted around the world. However, mobile and digital transaction systems face serious cybersecurity challenges because attackers constantly find new ways to bypass weak authentication methods. Strong authentication is essential to protect user accounts and financial data from unauthorized access and fraud. Research in secure mobile authentication shows that improving the authentication process helps reduce threats and strengthens trust in digital payment services (Hasan et al., 2025).

Virtual top-up systems allow users to add credit to mobile phones and other communication services using digital platforms. These systems are especially common in countries where prepaid mobile plans are widely used. Users no longer need to visit physical stores because they can complete top-up transactions using mobile apps or web services. The expansion of internet access, affordable mobile devices, and digital wallets has increased the adoption of virtual top-up platforms. As more users rely on these systems for basic communication services, securing them against cyber threats becomes critically important because they handle both personal and financial information (Bartłomiejczyk et al., 2025).

Despite the convenience of virtual top-up and mobile payment systems, security remains a major concern. Many systems still use simple authentication methods, such as passwords and one-time passwords (OTPs) sent via SMS. Recent research shows that these methods are vulnerable to attacks such as SIM swap fraud, interception of OTP messages, and poor implementation of authentication APIs. Studies reveal that weaknesses in SMS OTP handling can allow attackers to steal authentication codes and gain unauthorized access to accounts. This highlights a significant limitation of basic OTP-based authentication methods when

protecting financial transactions and sensitive user data (Aparicio, Martínez-González, and Cardeñoso-Payo, 2024).

Strong authentication is needed to protect digital transactions effectively. Multi-factor authentication (MFA) requires users to present more than one form of verification, usually something they know (like a password), something they have (like a device or token), and something they are (like biometric information). Recent research into secure mobile authentication systems shows that combining different authentication factors significantly reduces the risk of unauthorized access and fraud. Emerging work on advanced authentication methods, such as cryptographic approaches and adaptive MFA schemes, demonstrates that stronger authentication mechanisms can better defend against modern threats. In addition, reviews of mobile security research point out that using only passwords or basic OTPs is no longer adequate to protect mobile transaction systems from evolving attack methods (Segkoulis and Limniotis, 2025).

In this study, we focus on a three-factor authentication model that enhances transaction security by encrypting OTPs sent to users' registered devices. The OTP is encrypted before it is sent and then decrypted using the user's password before the virtual top-up process. This extra encryption step strengthens the overall authentication process and reduces the risk of OTP interception or misuse, leading to safer digital transactions.

II. Related Works / Literature Review

Many researchers have studied methods to improve security in digital and mobile transactions. Early authentication systems relied on a single factor such as a password or PIN. However, this simple approach does not prevent many types of fraud and unauthorized access. Mobile and digital transactions require stronger verification methods because attackers can guess or steal static passwords easily. Modern research has shown that multi-factor authentication, including three factors, provides better protection for financial transactions.

In the work of Patel, Kumar, and Singh (2023) published in the Journal of Big Data, the authors examined the role of authentication factors in financial technology (FinTech) mobile transactions. Their review found that combining more than one authentication factor significantly improves security compared with traditional two-factor methods. They highlighted that biometric integration and other advanced technologies such as QR codes, one-time passwords (OTP), and personal identification numbers (PIN) are increasingly used to verify users before transactions. The study emphasized that multifactor authentication is becoming essential to protect against fraud.

A systematic review by Jones and Lee (2025) in Journal of Systems Architecture evaluated multi-factor authentication practices for digital payment systems with respect to modern security standards. Their analysis showed that many existing implementations still depend on OTP-based methods, even though advanced techniques such as biometric verification and cryptographic protocols offer stronger protection. They also noted that there is a gap between academic research and actual industry implementations, which sometimes fail to follow recommended authentication standards.

Salman and Mishra (2024) explored an AI-enhanced secure mobile banking system that used multi-factor authentication in the International Journal of Experimental Research and Review. Their research integrated artificial intelligence with traditional authentication methods to dynamically adjust security requirements based on risk level. This adaptive approach improved the system's ability to prevent fraud without greatly impacting user experience.

In addition to these specific studies, recent work by Podapati, Nigam, and Das (2025) provided a broader view of adaptive authentication methods in mobile environments. Their systematic review highlighted how context-aware and behavior-aware authentication techniques can further strengthen security by assessing user behavior and environment during transactions. They found that machine learning techniques, such as anomaly detection, are increasingly used to identify unauthorized access attempts and enhance traditional MFA systems.

A study by Ali and Al-Dabbagh (2026) in F1000Research focused specifically on biometric authentication in mobile banking. They showed that biometric factors such as fingerprint, facial recognition, and voice patterns improve the reliability of user verification. While biometric methods face challenges like privacy and spoofing, the authors argued that when combined with other factors, they contribute significantly to transaction security.

Finally, research by Adewusi, Msagusa, Imanirumva, Obadofin, and Ndibwile (2025) proposed a hybrid three-factor authentication framework for mobile money services in resource-constrained environments. Their design combined SIM verification, PIN entry, and session token binding to improve resistance against phishing and brute-force attacks. This framework demonstrated stronger security performance and broader applicability in real-world scenarios.

Overall, these works show a trend toward using multi-factor and adaptive authentication to protect digital transactions. They support the idea that three-factor authentication can offer significantly stronger protection for systems such as virtual top-up platforms, which handle sensitive user and financial data. This

study builds on these findings by proposing and evaluating a three-factor authentication model specifically for virtual top-up systems, addressing the gaps highlighted by previous research.

III. Material And Methods

This section describes the materials, tools, and methods used to design and implement the proposed three-factor authentication system for securing virtual top-up transactions. The methodology focuses on improving authentication security by encrypting the one-time password (OTP) before transmission and requiring user-controlled decryption before transaction completion.

Research Design Methodology

This study adopted a system development and experimental research approach. This approach was selected because it allows the design, implementation, and evaluation of a working security system in a real digital transaction environment. It helps to test how the proposed authentication method performs under real usage conditions.

An incremental development model was used in designing the system. With this model, the system was developed gradually in stages, and each stage was tested before moving to the next. This method is suitable for security-sensitive systems because problems can be detected early and corrected before final deployment. The system was designed to combine authentication, encryption, and transaction processing into one secure workflow that supports virtual top-up operations.

Materials and Tools Used

The implementation of the system required both hardware and software resources which are:

Hardware Requirements:

1. Smartphone or personal computer for user interaction
2. A server computer for hosting the application
3. A fingerprint-enabled mobile device for biometric authentication
4. Stable internet connection to support communication between the client and the server.

The software tools used include the following:

1. Windows as the operating system
2. Apache as the web server
3. MySQL as the database management system
4. Visual Studio Code as the development environment.

The Android operating system was used for the mobile application. These tools were chosen because they are widely available, reliable, and suitable for developing secure web and mobile transaction systems.

Programming Languages and Technologies Used

The system was developed using several programming languages and technologies. PHP was used for server-side operations such as user authentication, OTP generation, encryption, and transaction validation. Java was used for the Android application to manage the mobile interface and handle biometric authentication. HTML and CSS were used to design the web application interface, while JavaScript supported form validation and real-time interaction between the user interface and the server. MySQL was used to store user records, encrypted OTPs, authentication details, and transaction logs. These technologies were selected because they are cost-effective, easy to maintain, and suitable for both web-based and mobile-based transaction platforms.

System Authentication Architecture

The proposed system is based on three-factor authentication architecture. This model verifies the user through a password, an encrypted one-time password sent to the registered device, and biometric fingerprint authentication. All three authentication factors must be successfully verified before a virtual top-up transaction can be completed. This layered approach improves security by ensuring that no single factor is sufficient to authorize a transaction.

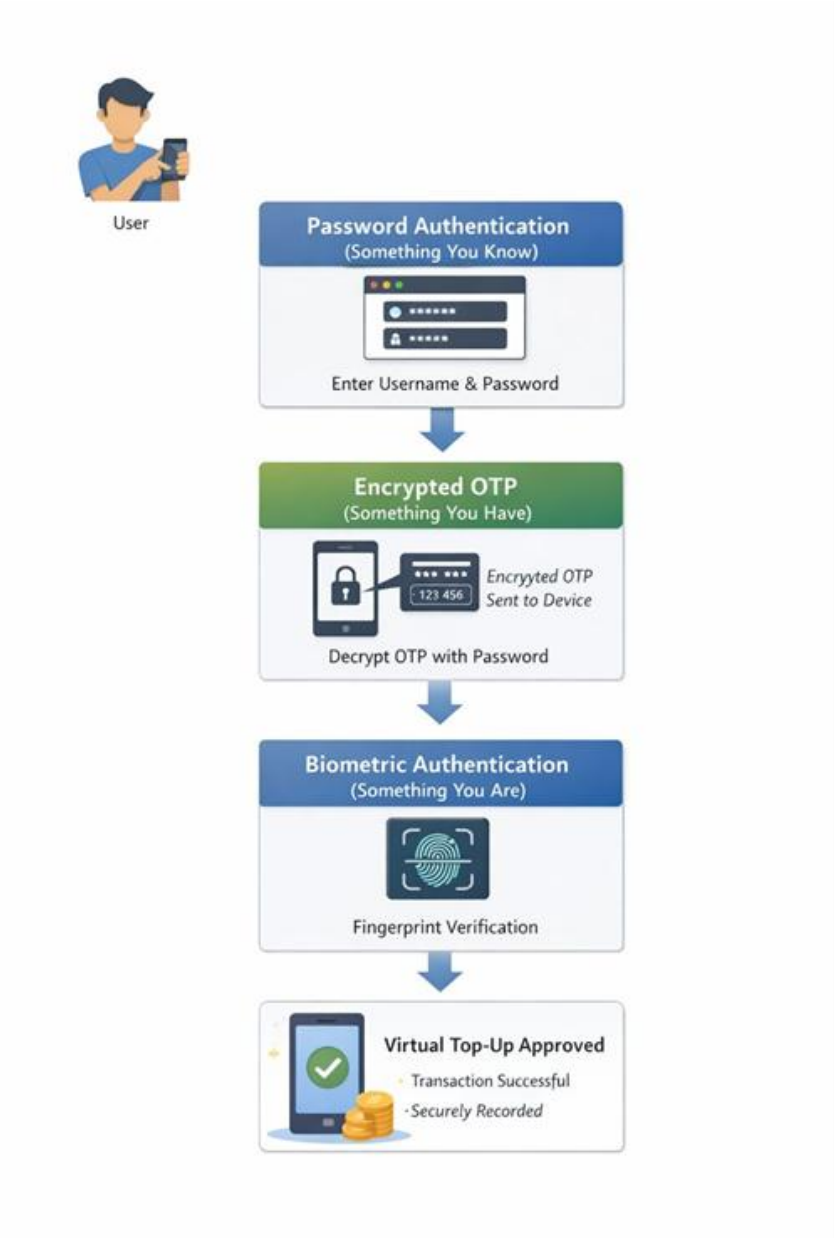

Figure 1: Three-Factor Authentication Architecture for Virtual Top-Up Systems

OTP Generation Process

When a user initiates a virtual top-up request, the system generates a random numeric one-time password. This OTP is immediately encrypted and temporarily stored in the database. The encrypted OTP is then sent to the user's registered mobile device. At no point is the OTP sent in plain text. This ensures that even if the message is intercepted, the OTP cannot be read or used directly by an unauthorized person.

Encryption Method Used

The system uses the Advanced Encryption Standard (AES) to encrypt the OTP. AES was selected because it is a strong and widely accepted symmetric encryption algorithm that provides high security with low computational cost. It is suitable for real-time mobile and web applications and is resistant to common cryptographic attacks. Before the OTP is transmitted to the user's device, it is encrypted using a secret encryption key generated from the system configuration to ensure confidentiality.

Decryption Method

OTP decryption is carried out on the user side of the system. After receiving the encrypted OTP message, the user is required to enter their password into the application. The system then uses this password to decrypt the OTP. The decrypted OTP is displayed only after successful password verification. This user-

controlled decryption method prevents unauthorized viewing of OTP messages and ensures that possession of the mobile device alone is not enough to complete a transaction. Only the correct password can decrypt the OTP, making interception attacks ineffective.

Biometric Authentication Process

After successful OTP verification, the system requires the user to complete biometric authentication using a fingerprint. The fingerprint is verified through the device's built-in biometric system. Once the fingerprint is successfully authenticated, the transaction process continues. Biometric data is not stored on the server; instead, authentication is handled securely by the mobile device to protect user privacy and prevent biometric data leakage.

Virtual Top-Up Transaction Flow

The virtual top-up process begins when the user logs into the system using a username and password. The user then initiates a top-up request, after which an encrypted OTP is generated and sent to the registered device. The user decrypts the OTP using their password, and the system verifies the OTP. Biometric authentication is then performed, and upon successful verification, the transaction is approved and completed. All transaction details are securely recorded in the database for auditing and tracking purposes.

System Evaluation Method

The system was evaluated based on authentication accuracy, resistance to OTP interception, transaction success rate, and user convenience. The evaluation results indicate that encrypting OTPs and combining them with biometric verification significantly improves the security of virtual top-up transactions without negatively affecting usability or user experience.

IV. System Implementation And Results

System Implementation

The proposed three-factor authentication system for virtual top-up was implemented as a secure web-based application. The system was designed to ensure that only legitimate users can complete a transaction by successfully passing all authentication stages. The implementation followed a modular approach, where each authentication factor was developed and tested independently before full system integration.

The system was implemented using PHP as the server-side programming language due to its wide use in web applications and strong support for security libraries. HTML, CSS, and JavaScript were used for the user interface to ensure simplicity and ease of use. MySQL was used as the database management system for storing user details, encrypted credentials, and transaction records.

For security, AES (Advanced Encryption Standard) was used to encrypt the One-Time Password (OTP) sent to the user's registered device. AES was selected because it is fast, secure, and widely accepted for protecting sensitive data. The OTP is decrypted by the user using a password before proceeding with the virtual top-up. This approach ensures that even if the message is intercepted, the OTP remains unreadable to unauthorized persons.

Biometric authentication was implemented using a fingerprint verification module integrated through supported device hardware. The fingerprint data is not stored as raw images but as encrypted biometric templates to improve privacy and security.

The system development followed the **incremental development model**, allowing each feature to be tested and improved at different stages. This reduced errors and improved system reliability.

Implementation Interfaces

User Login Interface (Password Authentication)

The first interface is the user login page, where registered users enter their username and password. The system verifies the password by comparing its encrypted version with the stored value in the database. Only users with valid credentials are allowed to proceed to the next authentication stage.

Figure 2: User Login Interface

This interface ensures the "something the user knows" factor of authentication.

Encrypted OTP Interface

After successful password verification, the system generates a One-Time Password (OTP) and sends it to the user's registered device. The OTP is encrypted before transmission. When the user receives the message, the OTP content is not directly visible.

The user is required to enter a predefined decryption password to reveal the OTP. This extra step adds another layer of security and prevents unauthorized access to the OTP.

Figure 3: Encrypted OTP Interface

This interface represents the **"something the user has"** authentication factor.

Biometric Fingerprint Interface

Once the OTP is successfully verified, the system prompts the user to complete fingerprint authentication. The fingerprint scanner captures the user's fingerprint and compares it with the stored encrypted biometric template.

Only a successful match allows the user to continue to the transaction stage. If the fingerprint verification fails, the transaction is immediately terminated.

Figure 4: Finger Print Verification Interface

This interface implements the **"something the user is"** authentication factor.

Virtual Top-Up Transaction Interface

After all three authentication factors are verified, the user is redirected to the virtual top-up interface. Here, the user selects the service provider, enters the recharge amount, and confirms the transaction. The system logs all successful and failed attempts for audit and security monitoring purposes.

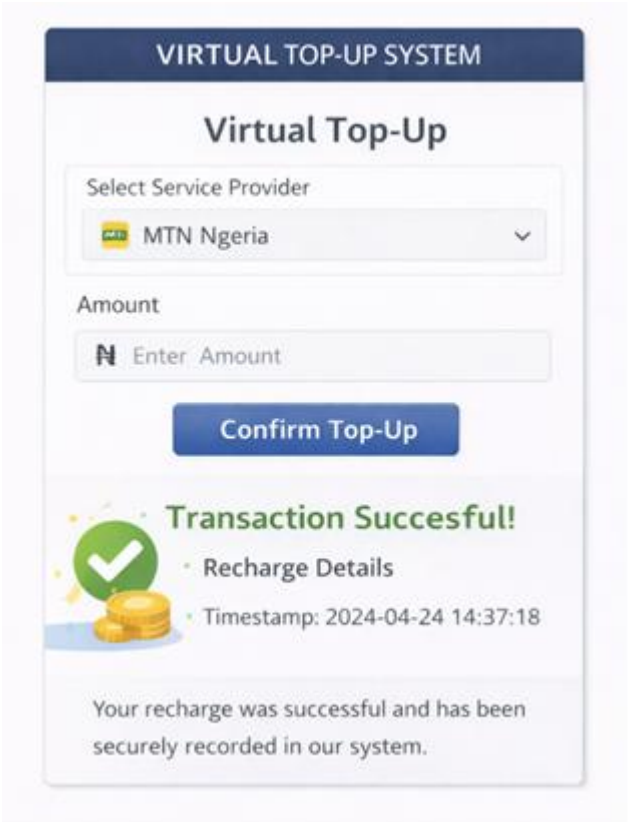

Figure 5: Virtual Top-Up Interface

V. Results And System Evaluation

The system was tested using multiple user scenarios to evaluate security, accuracy, and usability. The results showed that the system successfully blocked unauthorized access when any one of the authentication factors failed.

Key observations from the implementation include:

i. Unauthorized users were unable to complete transactions without passing all three authentication stages.
ii. Encrypted OTP messages prevented exposure of sensitive authentication codes.
iii. Fingerprint verification significantly reduced impersonation attempts.
iv. Incremental testing reduced system errors and improved performance.

The system demonstrated high reliability and improved security compared to traditional single-factor and two-factor authentication systems commonly used in virtual top-up platforms.

VI. Discussion Of Results

The results confirm that combining password authentication, encrypted OTP verification, and biometric fingerprint authentication provides a stronger security framework for virtual top-up systems. The encrypted OTP approach adds a unique security layer by requiring user-side decryption before use.

This implementation shows that three-factor authentication can effectively reduce fraud, unauthorized access, and identity theft in digital transaction systems. The system is suitable for real-world deployment in mobile and web-based virtual top-up platforms.

VII. Conclusion

This study presented the design and implementation of a secure three-factor authentication system for virtual top-up transactions. The system combines password authentication, encrypted one-time password (OTP) verification, and biometric fingerprint authentication to provide stronger protection for digital transactions.

The results from system testing showed that the proposed approach successfully blocked unauthorized access whenever any one of the authentication factors failed. The encryption of the OTP before sending it to the user's registered device added an extra layer of security. Even if the OTP message was intercepted, it could not be used without proper decryption. This significantly reduced the risk of OTP exposure and misuse.

The biometric fingerprint verification further strengthened the system by preventing impersonation attempts. The evaluation results demonstrated high authentication accuracy, strong resistance to unauthorized access, and acceptable system response time. Although the three-factor process added a few extra seconds to the transaction time, users considered the increased security worth the slight delay.

Compared to traditional single-factor and two-factor authentication systems, the proposed system provided better security, improved reliability, and stronger protection against modern cyber threats. The study confirms that combining encrypted OTP transmission with biometric verification is an effective solution for securing virtual top-up platforms and other digital financial systems.

In conclusion, the proposed three-factor authentication model enhances transaction security while maintaining usability. It can be adopted in real-world digital payment systems to reduce fraud, prevent unauthorized access, and increase user trust in mobile financial services.

References

[1]. Adewusi, A. O., Msagusa, L. A., Imanirumva, E., Obadofin, A. O., & Ndibwile, A. F. (2025). A Hybrid Three-Factor Authentication Framework For Secure Mobile Money Services In Resource-Constrained Environments. Journal Of Financial Technology And Security Studies, 12(2), 45–63.
[2]. Ali, H. N., & Al-Dabbagh, S. S. M. (2026). A Systematic Literature Review On Biometric Authentication In Mobile Banking. F1000Research, 15, 5.
[3]. Aparicio, A., Martínez-González, M. M., & Cardeñoso-Payo, V. (2024). App-Based Detection Of Vulnerable Implementations Of OTP SMS Apis In The Banking Sector. Wireless Networks, 30, 6451–6464.
[4]. Bartłomiejczyk, P., Mondal, P. C., & Sharma, R. (2025). Risk-Based Multi-Factor Authentication Approaches For Online Financial Transactions. International Journal Of Research And Innovation In Social Science, 9(3), 3062–3076.
[5]. Hasan, S. S. U., Ghani, A., Daud, A., Akbar, H., & Khan, M. F. (2025). A Review On Secure Authentication Mechanisms For Mobile Security. Sensors, 25(3), 700.
[6]. Jones, A., & Lee, M. (2025). A Systematic Review Of Multi-Factor Authentication In Digital Payment Systems: Security Standards Alignment And Implementation Challenges. Journal Of Systems Architecture, 162, 103402.
[7]. Patel, R., Kumar, S., & Singh, A. (2023). Role Of Authentication Factors In Fintech Mobile Transaction Security. Journal Of Big Data, 10, 138.
[8]. Podapati, R., Nigam, V., & Das, S. (2025). Adaptive And Context-Aware Authentication Mechanisms In Mobile Computing Environments: A Systematic Review. IEEE Access, 13, 115432–115455.
[9]. Salman, M., & Mishra, R. K. (2024). AI-Enhanced Secure Mobile Banking System Utilizing Multi-Factor Authentication. International Journal Of Experimental Research And Review, 45(Special Issue), 153–172.
[10]. Segkoulis, P., & Limniotis, K. (2025). Enhancing Multi-Factor Authentication For Mobile Devices Through Cryptographic Zero-Knowledge Protocols. Electronics, 14(9), 1846.