International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.17, June 2025

PINAF: A Multi-Level Security Model for Mobile Payment Systems in Nigeria

Mobolaji F. Oladapo
Federal University of Technology, Akure
Ondo State
Nigeria

Olutayo K. Boyinbode
Federal University of Technology, Akure
Ondo State
Nigeria

Kolawole G. Akintola*
Federal University of Technology, Akure
Ondo State
Nigeria

ABSTRACT

Mobile payment systems face significant trust challenges within the Nigerian population, stemming from perceived risks, system complexity, and concerns about reliability. In response, the 2011 Cashless Policy enacted by the Central Bank of Nigeria (CBN) has continued to drive the development of safer and more user-friendly mobile payment platforms. Common security mechanisms include personal identification numbers (PINs), biometric verification, and facial recognition. Integrating these modes provides enhanced security and addresses key gaps in Nigeria's cybersecurity landscape. This research presents the development of a multi-level security model for mobile payment systems, named **PINAF**, designed to address these challenges. The PINAF application encompasses user enrollment, authentication, and payment processing. Face detection was implemented using the Viola-Jones algorithm, facial recognition was performed using a Support Vector Machine (SVM), and user data was encrypted using the Rivest-Shamir-Adleman (RSA) algorithm. Evaluation results showed that the Viola-Jones + SVM approach achieved 90% accuracy, 92.3% recall, and an F1-score of 0.90, outperforming existing facial recognition models. The proposed model demonstrates a significant improvement in the security and reliability of mobile payment systems in Nigeria.

General Terms

Security, Mobile Applications, Payment Systems

Keywords

Multi-level Authentication, Mobile Payment, Face Recognition, Biometric Security, Cashless Policy

1. INTRODUCTION

Payment by cash is still dominantly used in developing countries and this attributes to about 90% of payment method in daily transactions[3]. Nigeria has been one of the countries to have evolved gradually from cash transactions to electronic transactions in an era popularly called 'cashless policy era' an initiative of the Central bank of Nigeria (CBN) in April, 2011[6, 2]. A study by Nwaolisa and Kasie (2012) [7] evaluated participants' preferences for payment methods in Nigeria, specifically comparing cash, internet banking, and credit cards, following the implementation of a cashless policy. The findings revealed that 82.6% of respondents still preferred cash payments, a statistically significant majority that highlights the limited adoption of electronic alternatives. The predominant reasons cited for this preference included a lack of adequate education on digital payment platforms, which might be attributed to concerns related to trust and awareness regarding their usage [6, 1]. Even beyond Nigeria and the African continent, many countries continue to favor traditional payment methods over digital alternatives. This persistent preference is often attributed to factors such as the perceived complexity of digital systems, lack of trust in their reliability, and concerns about privacy[9]. There is a growing need to develop a user-friendly and secure mobile payment system that is perceived as both intuitive and robust by Nigerian consumers. Such a system would promote greater adaptability to digital payment platforms and foster sustained acceptance of the cashless policy introduced by the CBN. In response to this need, this research aims to design and implement a multi-level security model for mobile payment systems that strengthens user authentication, addresses privacy and data-sharing concerns, and ultimately enhances consumer trust and adoption of digital payment solutions in Nigeria. The specific objectives of this research are as follows:(i) to design a multi-level security model incorporating PIN verification, biometric authentication, and secure transaction protocols. (ii) to implement the proposed model in a prototype mobile payment application. (iii) to evaluate the usability, performance, and effectiveness of the model in enhancing user trust and system security.

2. METHODOLOGY

2.1 PINAF Architecture

The conceptual diagram presented in Figure1 is composed of three major stages also known as modules. The first module is the Enroll-

ment module which collects the user data and biometric characteristics represented in digital form stored in the database. It makes use of Viola and Jones algorithm[10] to enroll a face and RSA algorithm[8] to encrypt user's data respectively The second module is the Authentication module whereby the user information and features in the enrollment module is verified using Support Vector Machine[5] to test if it matches with those stored in the database. The third module is the Payment Authentication module carried out by the Online Banking software (OBS) to enable transactions to be carried out from a user's account.

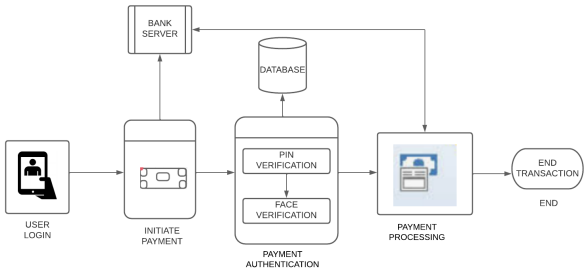

Fig. 1: System Architecture of the PINAF Multi-Level Secure Mobile Payment Model. This diagram illustrates the sequential workflow of the PINAF system, beginning from user login to payment initiation, followed by dual-level authentication (PIN and face verification), and culminating in payment processing via a banking server and database, with transaction completion.

2.2 Steps involved in developing PINAF

PINAF is designed to carry out out secured payment transactions on mobile devices using the PIN and face recognition respectively. The steps involved in this process are described as follows:

—**Enrollment phase:** The enrollment mode is a one-time setup process where the system captures and securely stores the user's PIN and biometric data (e.g., face image), which will later be used for authentication during login or payment.

—**Recognition Phase**: This is the second phase of the multi-level secured mobile payment system. Following a successful enrollment, this phase is responsible for validating the identity of the user by comparing the newly provided biometric data with the data previously stored during enrollment. The verification process involves the use of both a personal identification number (PIN) and facial recognition, ensuring dual-level authentication.

—**Payment Authentication Phase**: This is the final phase of the multi-level secured mobile payment system. It is based on a Secure Online Banking Server (SBS) and Online Banking Software (OBS). The SBS is responsible for handling customer data, establishing secure communication with the OBS, and verifying trusted biometric devices. The OBS, installed on the user's mobile device, interacts with the SBS to process transactions securely after successful identity verification.

2.3 PINAF Face Biometric Architecture

PINAF Biometric architecture has the following main components explained below with Figure2 displaying the architecture.

—**Sensor**: The sensor which is the first block is responsible for capturing the user's biometric information. In this case, it refers to the mobile phone camera, which serves as the interface between the user and the system by acquiring facial data for authentication purposes.

—**Pre-processor**: This is the second component of the system, responsible for preparing the captured biometric data for further processing. It eliminates background noise, enhances image quality, and performs normalization to ensure consistency across different input conditions.

—**Feature Extractor**: This is the third and the most critical components of the biometric system. It is responsible for extracting unique and distinguishable features from the pre-processed biometric data. These features characterize the user based on measurable properties, enabling accurate identification or verification during future recognition attempts.

—**Template Generator**: This component generates a biometric template from the extracted features. The template serves as a digital reference used during the authentication process to compare with newly captured biometric data.

—**Matcher**: The matching phase is carried out by the matcher, which compares the newly generated biometric template with the previously stored template. It uses algorithms such as Hamming distance to measure the similarity between templates and determine whether there is a match.

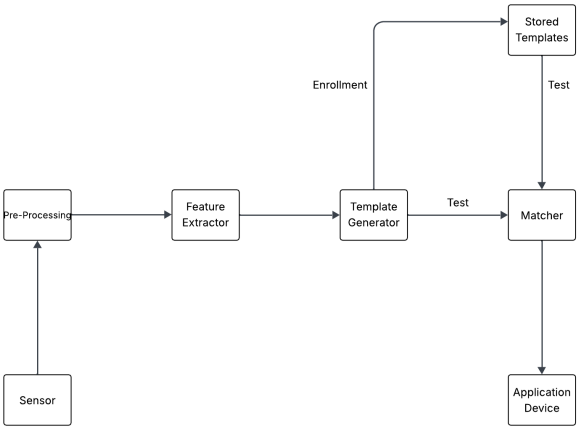

Fig. 2: Architecture of a Biometric Face Recognition System Used in PINAF. This diagram illustrates the functional blocks of the biometric recognition component in the PINAF system. The process begins with the sensor capturing the user's face, followed by pre-processing to reduce noise. Feature extraction and template generation then occur, producing reference templates stored during enrollment. During authentication, newly captured templates are matched against stored templates using a matcher before granting access through the application device.

2.4 PIN as a first level of security in PINAF

A personal identification number (PIN) is a secure alphanumeric or numeric code used for authenticated access to a system. Users will be required to choose a random four digits of their choice as their personal identification number. There are 10,000 possible variations starting with 0000, 0001, 0002, etc. Because the PIN authorizes the user to access sensitive information, it's fundamental to keep the number secret. Users have the option to change their PIN and might be required to do so in case of suspected fraudulent activities. If a PIN is lost or forgotten, it needs to be reset. User PIN

details was encrypted using the Rivest-Shamir-Adleman algorithm (RSA)[8].

2.5 Face Recognition as a Second Level of Security in PINAF

Facial recognition served as the second level of security in the multi-level secured mobile payment system. It was employed to identify or verify a user's identity based on their facial features. The process involves capturing, analyzing, and comparing facial patterns to determine authenticity. This implementation consists of two main steps: *face detection* and *face verification*. The **Viola-Jones Algorithm** [10] was used for face detection due to its efficiency in identifying human faces in real-time, while the **Support Vector Machine (SVM)** [5] was employed for face recognition and classification. Together, these techniques enabled accurate and efficient biometric authentication within the PINAF system.

2.6 Payment Authentication

The final phase of the PINAF system is **Payment Authentication**, which is carried out using an Electronic Fund Transfer (EFT) mechanism. Once the user has been successfully authenticated through the dual-layer security system, and a payment request is initiated, the transaction is processed via the Automated Clearing House (ACH) network. The ACH request is submitted by the bank, where it is batched and then transmitted to the relevant financial institutions for settlement and crediting of the respective beneficiary accounts as specified in the original transaction entry.

3. SYSTEM IMPLEMENTATION

3.1 System Requirements

The implementation of PINAF was carried out on a computer system with specified hardware and software requirements which are stated as follows:

3.1.1 Hardware Requirements. PINAF was implemented on system with the following hardware specifications:

—Personal Computer with 2.30 GHz and 4GB of RAM
—2GB of RAM
—Screen resolution 1280 x 800 pixels

However, the PINAF is not limited to this specification as higher level as well as some lower level specifications can be used for the system implementation.

3.1.2 Software Requirements. The following are the software tools used for the implementation of the PINAF:

—Android Studio
—Microsoft Windows 7/8/8.1/10 Operating system as the platform
—Languages: HTML, CSS, JS, XML, Java
—Libraries: OpenCV, Android Material Design

The implementation stages are presented as follows:

—Application installation
—Application Menu

3.2 Application Installation

PINAF payment system is installed on a camera enabled android mobile device and run.

3.3 Application Menu

The installed application is then clicked on to launch the application. The application menu consists of the:

—Sign up page

—Login page

—Dashboard

3.3.1 ***Sign-up page.*** The sign-up page is also known as a registration page. It enables users to independently register and gain access to the system. Figure 3 - 6 shows the sign-up page of PINAF. The sign up page requires a user's information to be enrolled in the system to carry out transactions. User information to be registered on the sign up page includes:

—Full name: This consists of the user's surname and first name.

—E-mail address: This is the user's valid e-mail address.

—Password: This is a string of characters that allows a user access to the system.

—PIN: This is the user's four digit numeric code to authenticate payments.

—Face Registration: This is the registration of the face image of the user into the system.

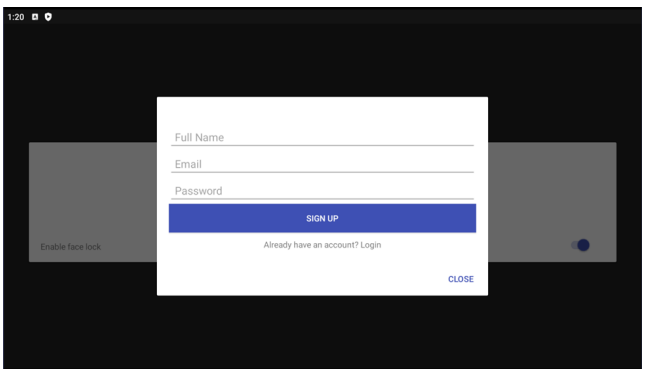

Fig. 3: Sign-up page. This interface shows the registration screen where a user inputs their full name, email address, and password to create a new account in the PINAF mobile payment application. This step forms part of the Enrollment Phase, where user credentials are captured and stored for future authentication and access to secure mobile transactions

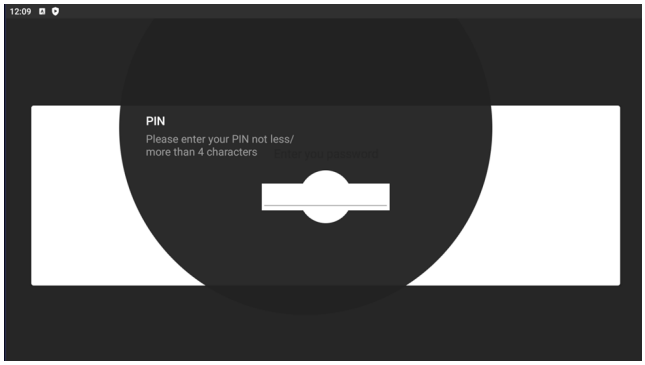

Fig. 4: Pin registration in the Sign up page. Users are required to enter a 4-digit PIN, which is later encrypted using the RSA algorithm. This step precedes biometric (face recognition) authentication and ensures that only users with valid PIN credentials can proceed with mobile payment processing

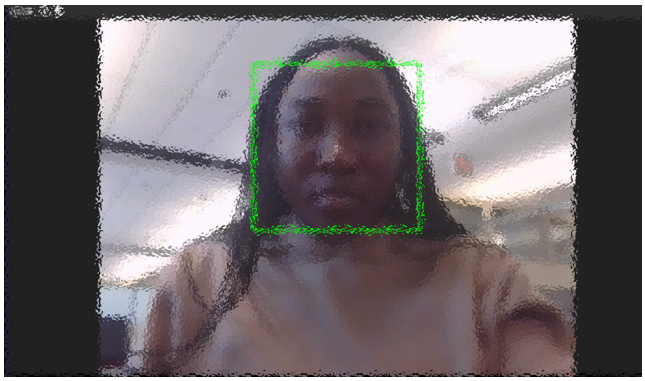

Fig. 5: Face registration on sign up page. At this stage, the user's facial data is captured via the mobile phone's camera (sensor) and processed for feature extraction using the Viola-Jones algorithm. These features are then encoded and stored as templates for future authentication using Support Vector Machines (SVM)

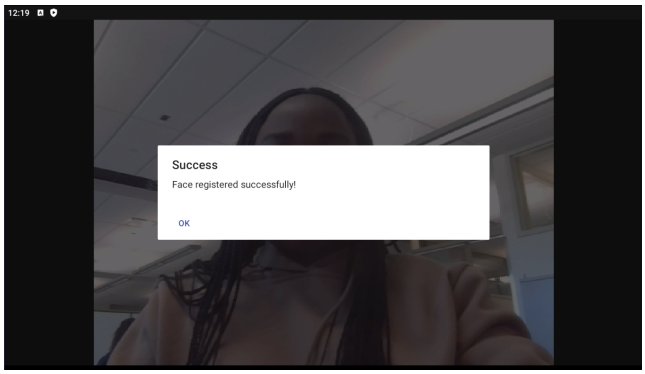

Fig. 6: Face successfully registered. After a successful face registration it notifies the user who can then proceed in using the app for their transactions.

3.3.2 ***Login Page***. The Login page allows a user to gain access to the application by entering their details registered during sign up phase. The step involves the user entering the username and password to gain access into the system. The system checks for the validation of the password, if valid then the user is passed on to the page. A user is automatically logged out due to inactivity. In this event, they will be returned to the login page, which will display an informational message explaining what happened. Five minutes is the duration before a session timeout. Figure 7 below shows the login page of the system.

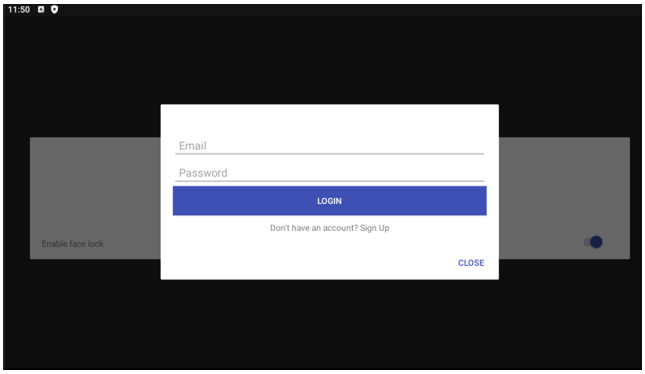

Fig. 7: Login Page. Here, the user provides their registered email and password.

3.4 Dashboard

The dashboard is also known as the main menu page. It lists options or commands for the user to select in order to execute a particular payment function. The menu page allows a user to navigate to a specific sub-menu to view its detailed information and function. The dashboard contains the user's account number and sub-menus such as transfer, airtime, cable payment and settings sub-menu. Figure 8 below shows the dashboard of the multi-level secured payment system.

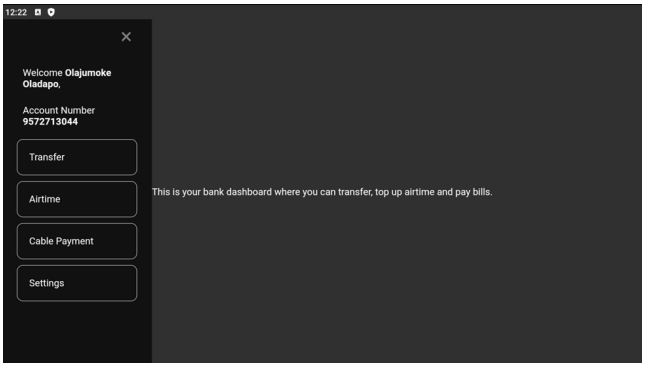

Fig. 8: The Dashboard. After successful login and authentication, users are redirected to the dashboard, which allows them to perform financial operations.

(1) Transfer Menu The transfer menu allows a user to send money to another user with a valid bank account number. The transfer menu consists of the following fields to be filled to perform a

successful transfer: Bank name, account number and amount. Figure 9 shows the transfer menu.

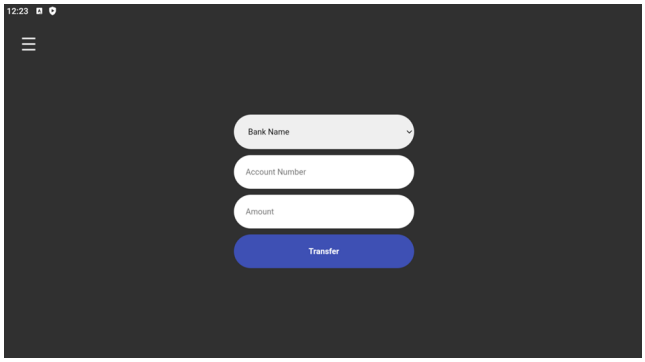

Fig. 9: Transfer Menu. This interface allows the user to securely initiate a bank transfer by inputting: (i)Bank Name: A dropdown list for selecting the recipient's bank. (ii) Account Number: The destination account number for the transfer. (iii) Amount: The value to be transferred. (iv) Transfer Button: To execute the transaction.

(2) Airtime Menu This allows users to buy airtime from their account. Airtime can also be purchased for a third party. Required information to purchase airtime includes Network; the service provider to supply the airtime, Phone number; in which airtime is to be loaded onto, Amount; which is the amount of airtime to be purchased. The airtime menu is initiated by clicking on the "Top Up tab. Figure 10 shows the airtime menu on the multi-level secured mobile payment system.

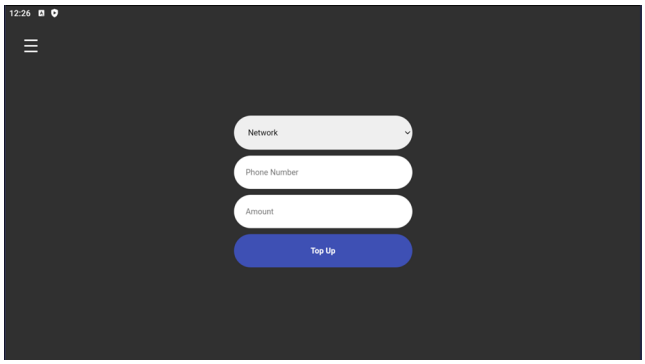

Fig. 10: Airtime Menu. This user-friendly interface allows users to: (i) Select a Mobile Network from a dropdown menu. (ii) Input a Phone Number to receive the top-up. (ii) Specify the Amount of airtime to purchase. (iv) Execute the Purchase using the "Top Up" button.

(3) Cable Payment Menu The cable payment menu allows a user to pay for Television subscriptions based on their service providers. The cable network menu contains the following fields to be filled: Cable network showing a preloaded list of television service providers such as DSTV, Amount; which is the value of the package to be purchased, Smart Card number; which is a unique chipped card code that is assigned to each decoder. Cable payment is authenticated by clicking on the "Pay"tab. Figure 11 shows the cable payment menu of the multi-level secured payment system.

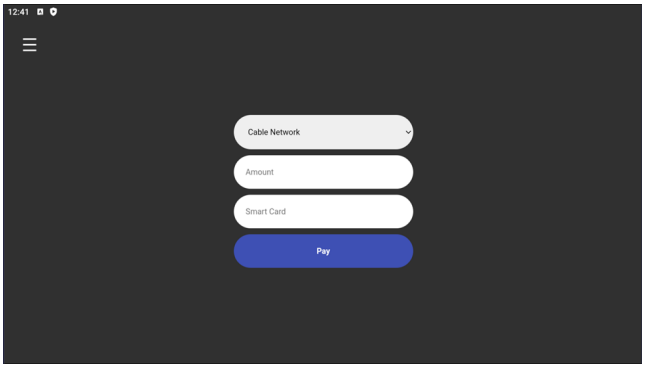

Fig. 11: Cable Payment Menu. This menu enables seamless payment for cable services by allowing users to: (i)Select the Cable Network (e.g., DSTV, GOTV, etc.). (ii) Enter the Amount to be paid. (iii) Input the Smart Card Number linked to their cable account. (iv) Process Payment securely with a single click on the "Pay" button.

(4) Settings Menu The settings menu allows a user to change their PIN or face image at any time. Current PIN and face image must be entered to allow users make changes. Figure 11 shows the settings menu of the system.

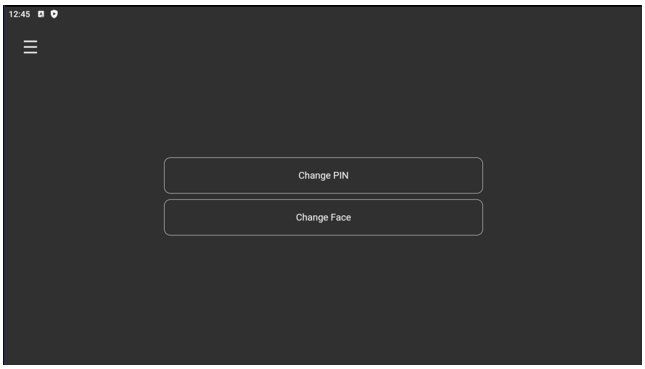

Fig. 12: Settings Menu. This section of the app provides users with easy access to update their authentication credentials.

4. SYSTEM EVALUATION

PINAF is evaluated with performance metrics on 50 face images, and the result is shown below in Table1 and Figure 13:

Table 1. : Performance Evaluation of the Proposed Model (PINAF)

Metric	**Result**
Enrollment Time	$<$ 10 seconds
Prediction Accuracy	$>$ 90%
False Alarm Rate (Face)	1%
Precision	92.3%
Recall	92.3%
Authentication Time	$<$ 2 seconds
Pin Failure Rate	$<$ 1%
User Satisfaction	$>$ 95%
System Uptime	$>$ 99.5%

Table 2. : Comparison of PINAF with existing methods

Authors and Years	**Technique Used**	**Prediction Accuracy (%)**	**Precision** (%)	**Recall** (%)
Angelo *et al*. (2016) [4]	Bridge Approach	80.00	not reported	not reported
PINAF	Viola Jones + SVM	90.00	92.3	92.3

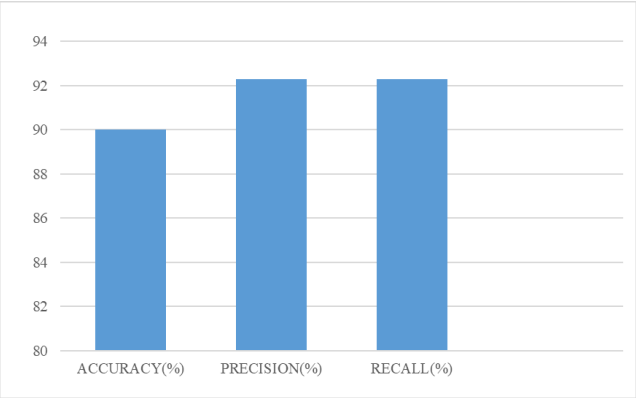

Fig. 13: Precision, Accuracy and Recall of the Model

4.1 Comparison with some other algorithms

The comparative analysis of the system with other existing system is done using some performance metrics. This performance metrics includes: prediction accuracy, precision, recall, false alarm rate, authentication time, pin failure rate, user satisfaction and system update.
Table 2 shows the comparison of the proposed model with some existing works when validated with 50 face image samples. From the Table, the proposed model performed better than the existing models in terms of prediction accuracy of 90%, detection rate/Precision of 92.3% and Recall 92.3%.

5. CONCLUSION

In this research, a multi-level secured mobile payment system named **PINAF** was developed to enhance the security and user trust in digital financial transactions. The system integrates two layers of authentication: a PIN-based verification using the RSA encryption algorithm and a facial recognition module leveraging the Viola-Jones algorithm in conjunction with a Support Vector Machine (SVM) classifier. User enrollment involves submitting an email address, password, four-digit PIN, and facial image. During authentication, a transaction is approved only if both the entered PIN and captured facial image match the pre-registered credentials. This dual-verification approach significantly reduces the risk of unauthorized access and addresses key concerns around mobile payment security in the Nigerian financial context. The proposed system offers a user-friendly interface while aligning with the objectives of the Central Bank of Nigeria's cashless policy. Evaluation of the model demonstrated improved accuracy, precision, and recall compared to baseline facial recognition methods, validating the effectiveness of the multi-level security model in securing mobile financial transactions. This work will be useful to financial institutions, Insurance companies and several other organizations in Nigeria to make payment on the go. One limitation of this study is that only two algorithms-Viola-Jones for face detection and Support Vector Machine (SVM) for face recognition were combined in developing the biometric verification system. While effective, more advanced feature extraction techniques exist that could potentially improve accuracy and robustness. Future directions for this research could include exploring the use of Principal Component Analysis (PCA) as a feature extraction technique. PCA is known for its dimensionality reduction capability and has been widely recognized for enhancing performance in facial recognition systems. Integrating PCA or other deep learning-based approaches may further strengthen the system's recognition accuracy and computational efficiency.

Acknowledgments

Not Applicable

Funding

Not applicable.

Conflicts of Interest

No conflict of interest.

Data Availability

All codes used for this analysis are provided in the supplementary materials.

6. REFERENCES

[1] Olayinka Abolade. *Consumers' perception towards Fintech and Traditional Financial Institutions (A case study of Nigeria)*. PhD thesis, Dublin, National College of Ireland, 2023.

[2] Ikechukwu A Acha, Clementina Kanu, and Godswill A Agu. Cashless policy in nigeria: The mechanics, benefits and problems. *Innovative Journal of Economics and Financial Studies*, 1(1):28–38, 2017.

[3] Waqas Ahmed, Aamir Rasool, Abdul Rehman Javed, Neeraj Kumar, Thippa Reddy Gadekallu, Zunera Jalil, and Natalia Kryvinska. Security in next generation mobile payment systems: A comprehensive survey. *IEEE Access*, 9:115932–115950, 2021.

[4] Angelo Galiano, Alessandro Massaro, Donato Barbuzzi, Mattia Legrottaglie, Valeria Vitti, Leonardo Pellicani, and Vitangelo Birardi. Face recognition system on mobile device based on web service approach. *Int. J. Comput. Sci. Inf. Technol.(IJCSIT)*, 7(4):2130–2135, 2016.

[5] Marti A. Hearst, Susan T Dumais, Edgar Osuna, John Platt, and Bernhard Scholkopf. Support vector machines. *IEEE Intelligent Systems and their applications*, 13(4):18–28, 1998.

[6] Odi Nwankwo and Onyekachi Richard Eze. Electronic payment in cashless economy of nigeria: Problems and prospect. *Journal of Management Research*, 5(1), 2013.

[7] Echekoba Felix Nwaolisa and Ezu Gideon Kasie. Electronic retail payment systems: User acceptability and payment problems in nigeria. *Arabian Journal of Business and Management Review*, 34(953):1–18, 2012.

[8] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[9] Alaa Mahdi Sahi, Haliyana Khalid, Alhamzah F Abbas, Khaled Zedan, Saleh FA Khatib, and Hamzeh Al Amosh. The research trend of security and privacy in digital payment. In *Informatics*, volume 9, page 32. MDPI, 2022.

[10] Paul Viola and Michael Jones. Rapid object detection using a boosted cascade of simple features. In *Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001*, volume 1, pages I–I. Ieee, 2001.