Nigerian Research Journal of Engineering and Environmental Sciences 8(2) 2023 pp. 533-541
p ISSN: 2635-3342; e ISSN: 2635-3350

Nigerian Research Journal of Engineering and Environmental Sciences
Journal homepage: www.rjees.com

Original Research Article

A Cardless Automated Teller Machine (ATM) Transaction Using Hybrid Security Approach

[1]Okolie, C.C., *[2]Ahiara, W.C., [3]Nwogu, E.R.

[1]Department of Computer Science, National Open University of Nigeria.
[2]Department of Computer Engineering, Michael Okpara University of Agriculture Umudike, Nigeria.
[3]Directorate of ICT, Michael Okpara University of Agriculture Umudike, Abia State, Nigeria.
*ahiara.wilson@mouau.edu.ng

http://doi.org/10.5281/zenodo.10442781

ARTICLE INFORMATION

Article history:
Received 04 Nov. 2023
Revised 10 Dec. 2023
Accepted 11 Dec. 2023
Available online 30 Dec. 2023

Keywords:
Authentication
Cardless ATM transaction
Hybrid security
Python flask
OTP

ABSTRACT

Due to the tremendous increase in the number of criminals and their activities, the Automated Teller Machine (ATM) has become insecure. This necessitated an urgent need to improve security in ATM transactions. However, the ATM systems in use today utilize no more than an access card along with either a Personal Verification Number (PIN) or fingerprint for identity verification, and so not sufficient or sophisticated enough to combat the rising security threats. For that, other attendant security techniques such as users' mobile number, facial recognition, and One Time Password (OTP) have been integrated in this work to form a hybrid security interface to ameliorate potential security breach. To perform a transaction, a user's face is captured and checked against a database of face images. Once there is a match, a One-Time-Password (OTP) is automatically generated and sent to the phone number associated with the bank account. This OTP is expected to be entered to complete the transaction initiated earlier. The proposed system which is made up of server and client side(frontend) application have been developed using Python Flask and React frameworks respectively. The user friendly web application designed grants access to user with authentic signature making it possible for cardless ATM transaction. Having tested the new system, it showed a promising result with high efficiency and capability while mitigating ATM security threats.

1. INTRODUCTION

Before now, it was easy to carry out banking operations and transactions due to low demand for monetary transactions. However, in the recent years, as human demands and business transactions become more complex, the influx of customers in and out of banking halls increased rapidly. Therefore, this necessitated the urgent need for electronic banking: the use of Automated Teller Machine (ATM) and the internet

banking. This electronic banking has undoubtedly helped to decongest banking halls, reduce the volume of cash carried about in bags and subsequent predisposition to incessant out-of-bank-robbery. In Mieseigha and Ogbodo (2013), it is observed that the use of electronic transaction helps to achieve transparency and accountability as well as a decrease in cash-related fraud. The long term shift to debit and credit cards was studied by Zandi *et al.* (2013) for 56 countries to know whether ATM card can stimulate economic growth and it was discovered that the electronic card payments could indeed increase efficiency and boost the consumption of the economy. The importance of this electronic card was also drawn to its use as a cashless policy device for fund transfer between one account and another (Manish *et. al.,* 2020).

Despite the positive impact of ATM usage on financial institutions and customers, inherent risks and challenges such as card skimming, cloning, maintenance costs, and password guessing are acknowledged. Researchers in the light of Shubhra (2017), have made pragmatic efforts to raise awareness and educate ATM users on safeguarding their cards and accounts. Similar challenges were observed in the work of Adeoti (2011). His investigation into ATM-related frauds in Nigeria reveals alarming statistics, emphasizing the global reach of these issues and their potential to hinder economic growth. The negative impact of this fraud in the banking sector is so devastating that it has also been observed in more than 70 countries in the world, according to Park (2012), and is capable of reducing the growth of economy because the allocation of funds for private investments will be biased

Concerns about the reliability of Personal Identification Numbers (PIN) and passwords are raised by Jafri and Arabnia (2013), leading to the exploration of biometric systems with biological characteristics for enhanced security. The high incidence of global ATM frauds, particularly affecting non-Information Technology (IT) savvy users, further justifies the need for enhanced security measures (Oyewole *et. al.,* 2013).

To mitigate these drawbacks, various researchers propose innovative security measures. These includes fingerprint and PIN usage (Afriyie and Arkorful, 2019), facial recognition systems (Aru and Ihekweaba, 2013), robust fingerprint authentication models (Onyesolu *et al.*, 2012), Quick Response (QR) code systems (Abhishek *et al.,* 2016), and secure ATM banking systems employing advanced encryption algorithms (Dondo *et al.*, 2017). Additionally, Marcarthy and Ojekudo (2018) and Madhuri *et al.* (2018) propose multifactor authentication systems combining biometrics, QR codes, and PINs to further enhance ATM security and save withdrawal time. In separate studies, Awajionyi and Ojekudo (2020), Kumar *et al.* (2017) and Jathumithran *et al.* (2018) proposed a biometric fingerprint-based system along with Bank Verification Number (BVN) to enhance ATM transaction security. Similarly, Kwakye *et al.* (2015) and Olaniyi *et al.* (2019) focused on fingerprint biometrics but incorporated a secured bio-cryptographic authentication system for cardless ATMs with encrypted PIN. It is worth noting, however, that the fingerprint biometric method has potential vulnerabilities, including the risk of cloning.

To combat these challenges, a cardless ATM transaction using a hybrid security approach is proposed in this work, incorporating a three-tier approach: One-Time Password (OTP), face recognition, and the user's mobile number. This approach aims to enhance the overall security protocol and identity verification by utilizing unique and irreplaceable characteristics.

2. METHODOLOGY

This section gives the analysis of the proposed system as well as its benefits. It also describes the software model, algorithm and the various design concepts adopted in detail to develop a new functional system.

2.1. Analysis of the Proposed System

User registration is the first activity that must be carried out by a user on the platform. During the registration process, users supply required information such as name and email. Users' face is captured and a machine learning module (OpenCV) is used to generate an Identity (ID) matching the facial image. This facial ID is saved together with the other information entered by the user. The aforementioned process is a model that creates bank account for the user. Once a user's account is created, he can perform transactions such as

withdrawal or transfer. For transaction to be successfully completed, the face of the user is captured, and the machine learning module processes it into a unique facial ID that is checked against the system's database. If the face matches the account, a One-Time-Password (OTP) is generated and forwarded to the phone number associated with the account. The user is expected to enter the OTP before a preset expiration time. If the OTP entered by user is verified, the initiated transaction will be completed. In a situation where there is no match for the facial image or incorrect OTP entered, then the initiated transaction is cancelled and said to be unsuccessful.

Authentication of the financial system on user access is very important in protecting the interest of the bank stakeholders. The single-tier and more authentication system as an existing system are not very efficient and effective, this motivated the proposed work. To improve the existing system, a hybrid security parameter (facial recognition, One-Time Password (OTP), and mobile numbers) will be used. This is a high-level authentication model. Combining the three models will add to the strength of the cardless ATM security to avoid unauthorized users from accessing other people's accounts. Facial recognition is a module designed for human facial recognition, identification, and verification. The dataset of registered users is collected with a specific identity assigned to a folder of the collected picture with a help of a library known as OpenCV. An OTP is generated at a given interval. The platform is managed by Google. The password is randomly generated and active at a given time interval. The user registers with a Gmail account. The mobile number is the number of a GSM subscriber registered in the name of the user(s). The three-tier module is implemented using the python language. The other significant libraries like OpenCV, and flask have their functionality in the complete system.

The benefits of this proposed hybrid security system is so numerous that it takes into consideration not only the main objective of intensifying the protocol to avoid vulnerability, not requiring special skill on how to use the ATM but also requires no ATM hardware implementation or design.

2.2. The Proposed System Design

The proposed system consists of frontend and backend. The frontend is built with react framework, Bootstrap, Hypertext Markup Language (HTML) and JavaScript while the back-end which is the server-side containing the database, is built with PostgreSQL database management system and python flask framework, a micro framework in python language that is used for web development.

The proposed work is designed to have its modules (facial recognition, one-time password, mobile numbers, and transaction). The modules have several components and user-friendly interfaces.

2.2.1. System architecture

System architecture is a conceptual model that is designed to define the structure, behavior, and views of a system. The proposed system architecture is shown in Figure 1. The system architecture consists of three components which are the user interaction module, server module and facial recognition engine. The user interaction module provides a means for the user to interact with the system while the server module handles processes like data storage, OTP generation and verification. The facial recognition engine is responsible for mapping faces to unique identities.

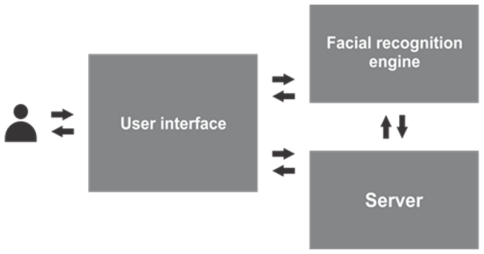

Figure 1: Architecture of the proposed system

2.2.2. Database design

A database is a collection of data or entities with related information. Database design is the organization of the data based on the database model. According to Lightstone (2009), database design involves classification of data and identification of its inter-relationships. The designer of the database determines the type of data to be stored and how the data elements will interrelate. Table 1 represents the user schema and Table 2 represents the OTP schema which only updates whenever user requests for a code without updating the user‘s record.

Table 1: Fields of the user database

S/N	Field name	Data type	Length
1	userId	Int	Auto increment
2	fullName	Varchar	30
3	Email	Varchar	30
4	Password	Varchar	6
5	facialId	Varchar	40
6	phoneNumber	Varchar	11
7	accountNumber	Varchar	30
8	accountBalance	Int	11
9	createdAt	Timestamp	30
10	updatedAt	Timestamp	30

Table 2: Fields of the OTP database

S/N	Field name	Data type	Length
1	codeId	Int	Auto increment
2	Code	Varchar	8
3	expirationTime	Timestamp	-
4	createdAt	Timestamp	-
5	updatedAt	Timestamp	-

2.3. The Algorithm of Proposed System

The following algorithm describes the proposed system.

1. Capturing of user face using camera
2. Generate facial ID using machine learning module
3. Verify facial ID on database
4. If facial ID is authentic, then go to step 5, else go to step 9
5. Generate OTP and send to user’s phone number
6. Accept OTP from user
7. If OTP is valid, then go to step 8 else, go to step 9
8. Complete initiated transaction, and go to step 10
9. Cancel transaction and go to 10
10. Exit

2.4. Modeling of the System

In this work, the design tool used is Unified Modeling Language (UML). The Unified Modeling Language is a standard graphical notation with symbols and connectors that helps in describing software analysis, design, and documentation of every part of an application development process. A use case diagram summarizes the details of the system and it is also known as actors as they perform various interactions with

the system. The main actors in this work are the account holder and the administrator. Figure. 2 shows the use case diagram of the proposed system.

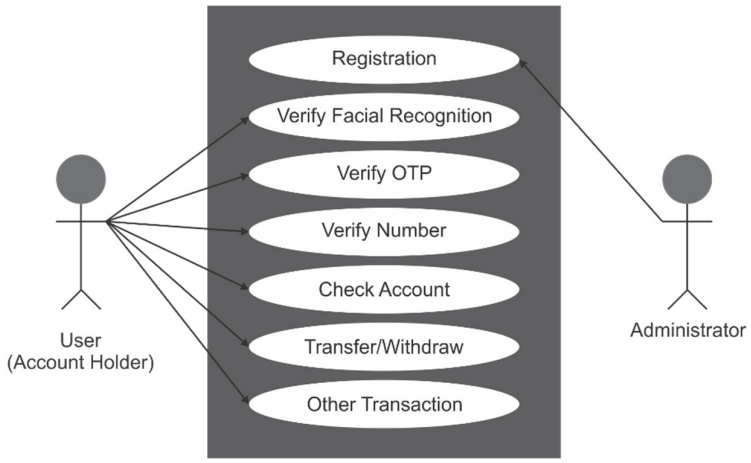

Figure 2: Use case diagram of the system

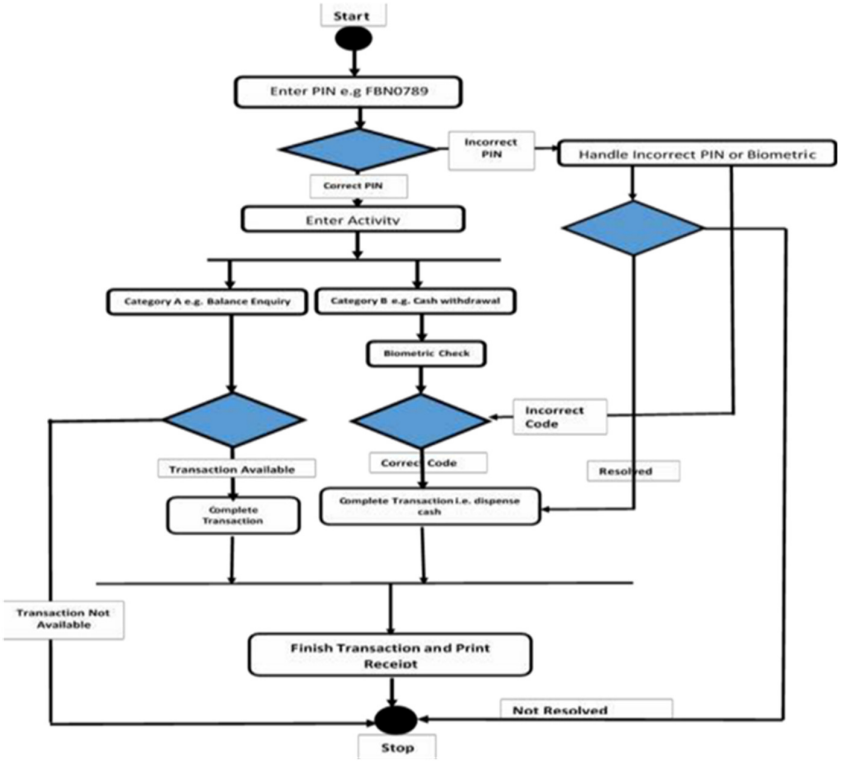

Figure 3: The data flow system design

The administrator creates an account for the account holder using their facial image, One Time Password (OTP) and mobile number. The account holder is then verified using the pre-stored application of face recognition, OTP, and mobile number. The user could view the account, make a deposit and make a withdrawal. This work has the initialization state and the final state. The initialization state describes the verification of the user account holder using a hybrid security approach while the final state describes the monetary transaction(s). Similarly, the work is modeled using a data flow diagram. The diagrams are

contents of specific components that describe several symbols. The symbols represent given object components of a given project implementation. This data flow diagram provides information about the inputs and outputs of each entity, and about the process itself. Figure .3 shows the data flow diagram of the proposed system.

3. RESULTS AND DISCUSSION

3.1. Implementation and Testing

In this section, the designed output describes the various input stages of security from facial recognition to mobile number authentication. It also displays the reports of either success or failed authentication in the course of transaction during the testing phase to ensure the efficient working of the system.

3.1.1. Frontend display

Figure. 4 shows the frontend input page. On this page, a new user could be added to the system by the system administrator. Figure 5 shows the face capturing screen. On this screen, a system user will have their image captured for authentication in the system before they can be granted access to the system. Figure. 6, on the other hand, shows the screenshot of the One Time Password (OTP) input screen. The OTP is sent to the user's phone and used as a second level authentication.

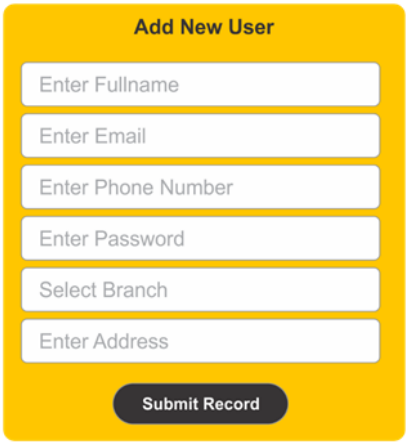

Figure. 4: Frontend input page

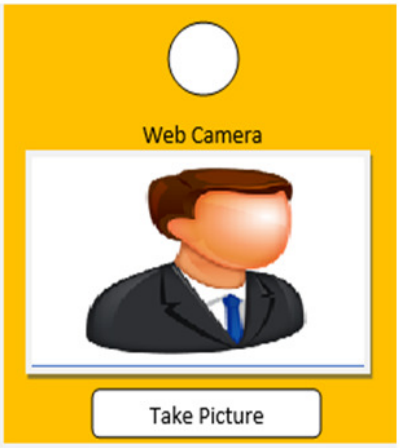

Figure. 5: Screenshot of a facial capture interface

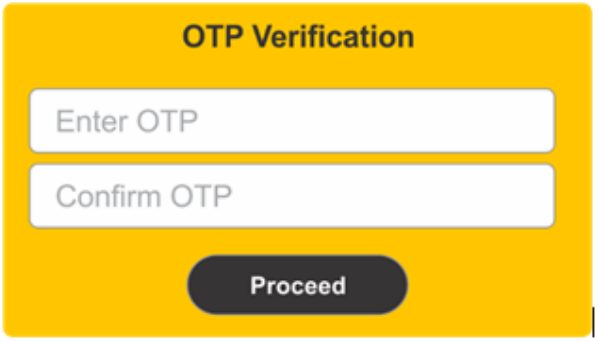

Figure 6: A screenshot of the One-Time-Password input screen

3.1.2. Testing the accuracy of the system

To test the accuracy of this system, a system modal application developed displays at different points, as depicted in Figures 7, 8 and 9, the status of the right and wrong system authentication cum access requests made by supposed user(s) during transaction process.

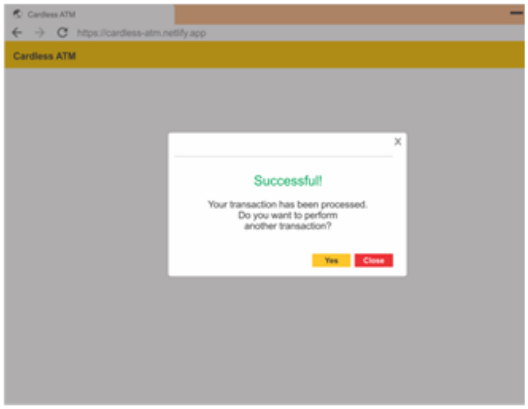

Figure 7: Correct signature supply

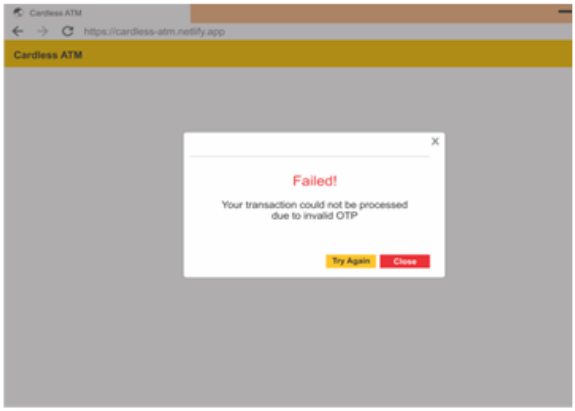

Figure 8: Incorrect OTP capture

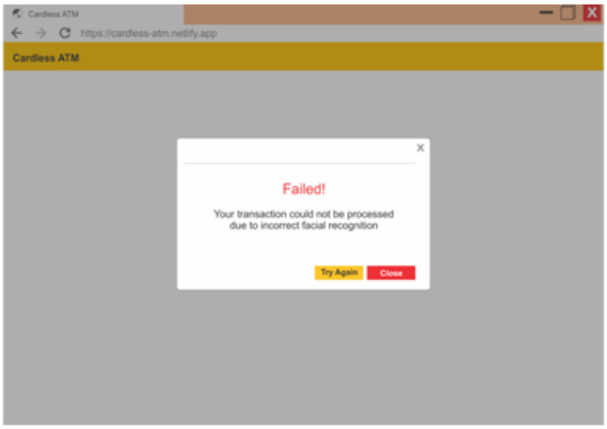

Figure 9: Invalid facial capture

3.2. System Evaluation

Having reviewed the works of some researchers on ATM card transactions and its rising security threats and vulnerabilities in the existing system, it has become imperative to adapt to the urgent need for enhanced ATM security in response to increasing criminal activities. The existing system relies solely on access cards, Personal Identification Numbers (PINs), and fingerprints. The review by Adeoti shows that ATM fraud in Nigeria occurs through card jamming, stolen ATM cards, and shoulder surfing, causing a negative impact on the banking sector and the economy. Additionally, for secure transactionary purposes, ATM cards are issued to users alongside a unique PIN, but the drudgery associated with password guessing can hinder access to users' accounts. The cards are never issued to users without associated charges for maintenance or cost in case of misplacement.

Moreover, the use of fingerprints as a biometric characteristic, in lieu of the proposed face recognition system, makes the former susceptible to cloning. To address these problems, a three-tier security authentication comprising OTP, face recognition, and the user's mobile number is adopted for efficient and robust authentication. The face recognition biometrics, user's mobile number, and the OTP, a numeric or

alphanumeric string of characters randomly generated automatically within a specified time interval, are unique to each user and cannot be replicated. The implication of the test carried out shows promising results, indicating high efficiency and capability of the developed cardless ATM transaction system. The correct signature supply is sacrosanct; otherwise, complete access is denied as it ensures the avoidance of unauthorized access.

4. CONCLUSION

The adoption of the ATM as an electronic means of carrying out some banking transactions has proved to be effective on the banking industry. However, since the advent of ATMs, fraud has been a menace to banks and their customers all over the world, and efforts are being made to reduce or completely eradicate frauds associated with the use of ATM. A workable solution that addresses the requirements of the regulatory authority of banks has been provided by the proposed system. A biometric authentication technique (facial recognition), mobile number, and OTP have been adopted in this work. This proposed hybrid security technique has unique identification and authentication features that makes it less susceptible to replication by hoodlums. Thus, the system will increase customers' satisfaction, and give them a high level of trust against financial crimes. We therefore recommend this system to financial institutions and the society at large as it hopes to reduce the high level of crime that is associated with ATM transactions.

5. CONFLICT OF INTEREST

There is no conflict of interest associated with this work.

REFERENCES

Abhishek, G. M., Mohanan, A.V. and Jaison, G.V. (2016). ATM custodian: A new type of authentication for ATMs. *International Journal of Computer Application.* 6(2), pp. 100-106

Adeoti, J. O. (2011). Automated Teller Machine (ATM) frauds in Nigeria: The way out. *Journal of Social Sciences.* 27(1), pp. 53-58.

Afriyie, O. and Valentina, A. (2019). Enhancing security of Automated Teller Machines using biometric authentication: A case of a Sub-Saharan University. Information and Knowledge Management, Ghana. 9(7), pp. 7-22.

Aru, O. E. and Ihekweaba, G. (2013). Facial verification technology for use in ATM transactions. *America Journal of Engineering Research (AJER).* 2(5), pp. 188-193.

Awajionyi Urang S. and Ojekudo Nathaniel A. (2020). Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint. *American Journal of Engineering Research (AJER).* 9(9), pp. 36-43.

Dondo, J., Akinyi, M., Okeyo, G. and Kimwele, M. (2017). A Fingerprint & Pin Authentication to Enhance Security at the Automatic Teller Machines. *International Journal of Scientific & Engineering Research.* 8(4), pp. 380-387

Jafri, R., Ali, S. A. and Arabnia, H. R. (2013). Face recognition for the visually impaired. International Conference on Information and Knowledge Engineering (IKE '13) At: Las Vegas, Nevada, USA

Jathumithran, S., Thamilarasan, V., Piratheepan, A., Rushanthini, P., Mercy, J. V., Nirupa, P. and Thiruthanigesan, K. (2018). Enhancing ATM Security using Fingerprint. *ICTACT Journal on Microelectronics*. 4(2), pp. 570 – 575.

Kumar, D.D., Vijay S. B., Bhavani, B., Malathy, E. and Mahadevan, R. (2017). A Study on Different Types of Authentication Techniques in Data Security. *International Journal of Civil Engineering and Technology (IJCIET).* 8(12), pp. 194-201.

Kwakye, M. M., Hanan, Y. B., and Eugene, L. B. (2015). Adoption of biometric fingerprint identification as an accessible, secured form of ATM transaction authentication. *International Journal of Advanced Computer Science and Applications, (IJACSA)*. 6(10), pp.253-264

Lightstone, .S. (2009). Physical Database Design for Relational Databases. In: Liu, L. Ozsu, M. T. (eds) Encyclopedia of Database Systems. Springer, New York.

Macarthy, O. and Ojekudo, N. (2018). A comparative study of PIN based and three-factor based authentication technique for improved ATM security. *International Research Journal of Engineering and Technology (IRJET).* 5(5), pp. 49-54

Madhuri, M., Sudarshan, K., Akshaykumar, K. and Rupali, A. (2018). Cardless Automatic Teller Machine (ATM) Biometric Security System Design using Human Fingerprints. *International Journal of Advance Engineering and Research Development (IJAERD*), 5(5), pp. 392–399.

Manish, C. M., Chirag, N., Praveen, H.R., Darshan, M.J., Khasim, D.V. (2020). Card-less ATM transaction using biometric and face recognition- a survey. *International Journal of Scientific & Engineering Research.* 11(1), pp. 1393-1400.

Mieseigha, E. G., and Ogbodo, U. K. (2013). An empirical analysis of the benefits of cashless economy on Nigeria's economic development. *Journal of Finance and Accounting*, 4(2), pp. 11-16.

Onyesolu, M.O., Odoh, M., Akanwa, A.O., and Nwasor, V.C. (2012). Robust authentication model for ATM: A biometric strategy measure for enhancing e-banking security in Nigeria. *International Journal of Advanced Research in Computer Science*. 3(5), pp. 164-169.

Olaniyi, O. M., Ameh, I. A., Ajao, L.A., Lawai, O. R. (2019). Secure Bio-Cryptographic Authentication System for Cardless Teller Machines. *Journal of Advanced Computer Engineering Technology*. 5(2), pp. 117-128.

Oyewole, O.S., El-Maude, J.G., Abba, M., and Onuh, M. E. (2013). Electronic payment system and economic growth: a review of transition to cashless economy in Nigeria. *International Journal of Engineering, Science and Technology*. 2(9), pp. 913-918.

Park, J. (2012). Corruption, soundness of the banking sector, and economic growth: a cross-country study. *Journal of International Money and Finance*. 31 (5), pp. 907-929.

Shubhra, J. (2017). ATM frauds-detection & prevention. *International Journal of Advances in Electronics and Computer Science (IJAECS).* 4(10) pp. 82-89.

Zandi, M., Singh, V., and Irving, J. (2013). The impact of inequality on economic growth on economic growth, Moody's Analytics, pp. 1-16.