JEMT 6 (2018) 21-29 ISSN 2053-3535

Journal of Engineering and Manufacturing Technology
www.bluepenjournals.org/jemt

Development of hybrid pin-biometrics database identification and verification system: Demonstrated in automated teller machine

Lasisi, H[1], Oyeniran R. O.[2], Saka-Balogun, A. R.[1] and Oladepo O.[1]*

[1]Electrical and Electronics Engineering Department, Osun State University, Osogbo, Nigeria.
[2]Electrical and Electronics Engineering Department, Osun State College of Technology, Esa-Oke, Nigeria.

Article History
Received 02 February, 2018
Received in revised form 15 March, 2018
Accepted 20 March, 2018

Keywords:
Automated teller machine,
Biometric,
Database,
Hand geometry,
Verification,
Signature.

Article Type :
Full Length Research Article

ABSTRACT

The current rate of crime, fraud, terrorism and vandalism across the globe pose great threat to economic development and sustainability. Much as security and confidentiality of persons have been areas of worry, authentication and verification of individuals have become more of concern nowadays. A robust authentication and verification system requires every citizen to have a biometric identity card linked to a national database server; suggested to be a harvest of various databases of government departments, agencies, financial institutions and law enforcement bodies. The integrity of the system depends more on the database and the employed biometrics technology. Biometrics robustness could be improved through hybridization of verification techniques. This paper proposed a framework for user's identification and authentication using hybridization of personal identification number (PIN), fingerprint, iris and magnetic stripe card. The robustness of the hybrid system is demonstrated in automated teller machine (ATM) in comparison with the conventional PIN authentication method. Although, denial of proxy withdrawal could be stated as demerit of this hybrid biometrics system, the security level is worthwhile. A single integrated multi-application card could be achieved by using chip-based general multipurpose card (GMPC) technology, which allows for input of several applications on one card. The system could be used by governments to boost security system, financial budgeting, as well as health care services planning and management.

INTRODUCTION

The current rate of crime, fraud, terrorism and vandalism across the world call for a robust identification, authentication and verification system for individuals in order to achieve adequate national security, economic development and sustainability. Automated teller machines (ATMs) innovation paralleled the growth of the personal computers (PC) and telecommunications industries (Mario and Annuar, 1995). However, every single authentication and verification system used in isolation is vulnerable to fraud. For example, fraudsters have devised different skills to beat the personal identification number (PIN) security system used in ATM (Jayasinghe et al., 2015). Various forms of fraud are perpetuated, ranging from: ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, force withdrawals and lot more.

Consequently, a system that combines more than one authentication and verification systems could guaranteed some level of improved security and provide the necessary succor. This paper provides a framework for

*Corresponding author. E-mail: ooladepo@yahoo.com.

user's identification and authentication using hybridization of personal identification number (PIN), fingerprint, iris and magnetic stripe card. This is a combination of the conventional PIN and Biometrics systems. Fingerprint and iris are chosen over other biometric identifiers because they are cost efficient, ease to use, of high matching accuracy, require less hardware, popular and highly accepted by the society as identification and authentication technologies.

Biometrics is measurement and analysis of unique physical or behavioural characteristics such as finger-print, face, gait, iris, hand geometry, signature as a means of verifying personal identity (Mahesh and Govindarajulu, 2016). Personal identification based on biometric has been receiving extensive attention in public security and information security domains (Yakub et al., 2017). The critical attributes of these characteristics for reliable recognition are the variation of selected charac-teristics across the human population and uniqueness of these characteristics (Omar, 2002).

The security level of the hybrid system is on the high scale. A single integrated multi-application card could be achieved by the use of chip-based general multipurpose card (GMPC) technology, which allows for input of several applications on one card. Thus, it could be modified by governments and used to boost national security system, financial budgeting, as well as health care services planning and management. The paper is segmented into five parts; the topic under discussion was introduced in part one while part two dealt with methodology. Results and discussion occupied the third part while conclusion is in the fourth part. Recommen-dation on the topic was made in the fifth part of the paper.

Personal identification number (PIN)

A personal identification number (PIN, pronounced "pin"; often called PIN number) is a numeric password shared between a user and a system. The PIN is used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user identifier or token (the user ID) and a confidential PIN to gain access to the system. Upon receiving the user ID and PIN, the system checks up the PIN based upon the user ID and compares the looked-up PIN with the received PIN. The user is granted access only when the PIN entered matches with the PIN pre-stored in the system. The PIN can be hacked by the hacker since there is a lot of numbers to choose from (Jayasinghe et al., 2015; Omar et al, 2000). Besides, people preferred to use PIN that are easy to be remembered and guessed, for example date of birth, than well-chosen password.

Magnetic stripe card

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card, made of plastic with embedded integrated. A card with a magnetic stripe serves as a data carrier, with the data being read and stored electronically. In the back of the magnetic strip card there is magnetic strip to hold the information of the cardholder. These magnetic strips mainly have two or three tracks with varying storage capacities. Possible types of data stored in magnetic stripe card are mainly: cardholder name, card number / account number, expiration date etc.

Biometric authentication

Biometrics are biological authentications, based on some physical characteristics of the human body (Mahesh and Govindarajulu, 2016; Gaurav and Shilpa, 2017). The list of biometric authentication technologies is still growing. The two categories of biometric identifiers include physiological and behavioral characteristics (Bechelli et al., 2002). Physiological characteristics are related to the shape of the body, and include but not limited to: fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina), and odor /scent. Behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait, digital signature and voice (Navneet and Vijay, 2012). There are devices made to recognize these biometrics nowadays. Biometric authentication mechanism is receiving a lot of public attention. A biometric device is perhaps the ultimate attempt in trying to prove who you are (Polemi, 1997). Biometrics authentications in conjunction with password/PIN system provided a level of improved security in authentication and verification (Lasisi and Ajisafe, 2012).

METHODOLOGY

The methodology herein involves design, development and incorporation of a fingerprint and Iris biometric authentication systems into the generic ATM PIN system using c# programming language. The software development kit (SDK) helped in modeling various stages of the authentication and verification procedures. The robustness and security level of the hybrid system was demonstrated and evaluated over the conventional PIN system.

The process to identifying individual through PIN, fingerprint and iris biometric system was established and detailed. The methodology involves issuance of pin code to the individuals as well as registration of the individuals' PIN, fingerprint and iris using smart card. The "futronic FS25" device was used as fingerprint device and the system webcam for the enrollment of individual iris

Figure 1. Captured screenshot of the administrative component for PIN registration.

respectively. These were done on the ATM sever interface which has administrative privileges of adding and deleting iris templates, signature scans and pin code issuance.

Basically, the hybridization of the technologies required the incorporation of a smart card, fingerprint and iris scanner/reader. The workability of the system was demonstrated by integrating the hybrid system with the conventional ATM authentication system. User screens were created to guide the client through the process, and to give notification of fingerprint and iris acceptance or denial.

The application solicits for the supply of the user's PIN, fingerprint and iris, and then activates the sensors which capture the parameters, encrypts it and sends it to the system de-encrypts sub-system. The supplied PIN and the captured fingerprint and iris are compares to the stored templates in the system database. The application then notifies the user the results of the validation process and hence, provides appropriate transaction authorization or denial.

The hybrid biometrics system basically consists of two components: administrator component and client component.

The administrator component

The administrator component (SERVER) stores user's specific data such as name, user's pin, identify card number, account number, fingerprint and iris template in the database for matching, record and recovery purposes. The user's information, PIN and the required biometrics are collected in the process of enrolling the users.

The client component

The client component consists of four sub-components/units: measurement unit, feature extraction unit, comparison unit and reference database unit. The measurement component is in charge of capturing the user's fingerprint and iris when he or she tries to identify him or herself. Then the captured fingerprint and iris image is passed to the feature extraction unit. Feature extraction unit takes the raw image and extract key features from it. Next, the key features are passed to the comparison unit which compares it with the key features stored in the reference database. The hybrid biometrics client component acts exactly like the normal ATM client interface except that it in addition, asks for the users fingerprint and iris for authentication.

Figures 1 to 4 show the administrative component sequentially registering the PIN, the fingerprint and the iris. However, Figures 5 to 9 are for the client's component of the system.

RESULTS AND DISCUSSION

Modified software of a conventional ATM machines was

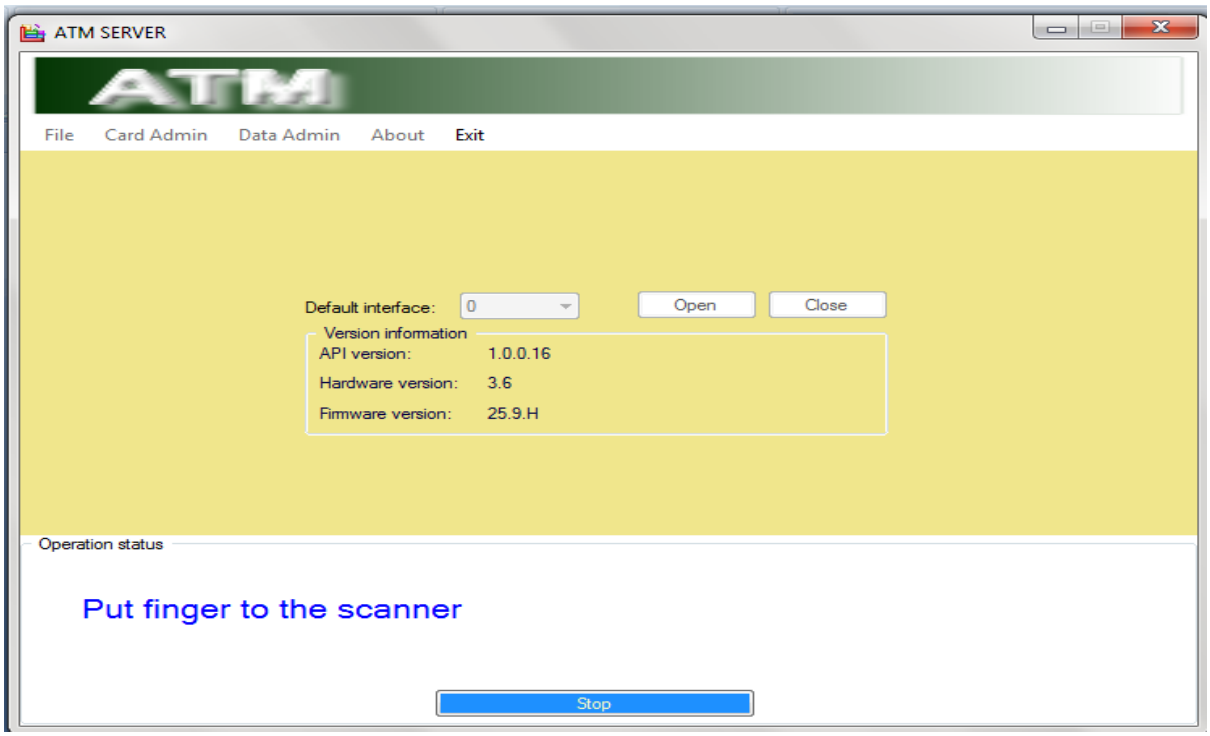

Figure 2. Captured screenshot of the administrative component for fingerprint registration.

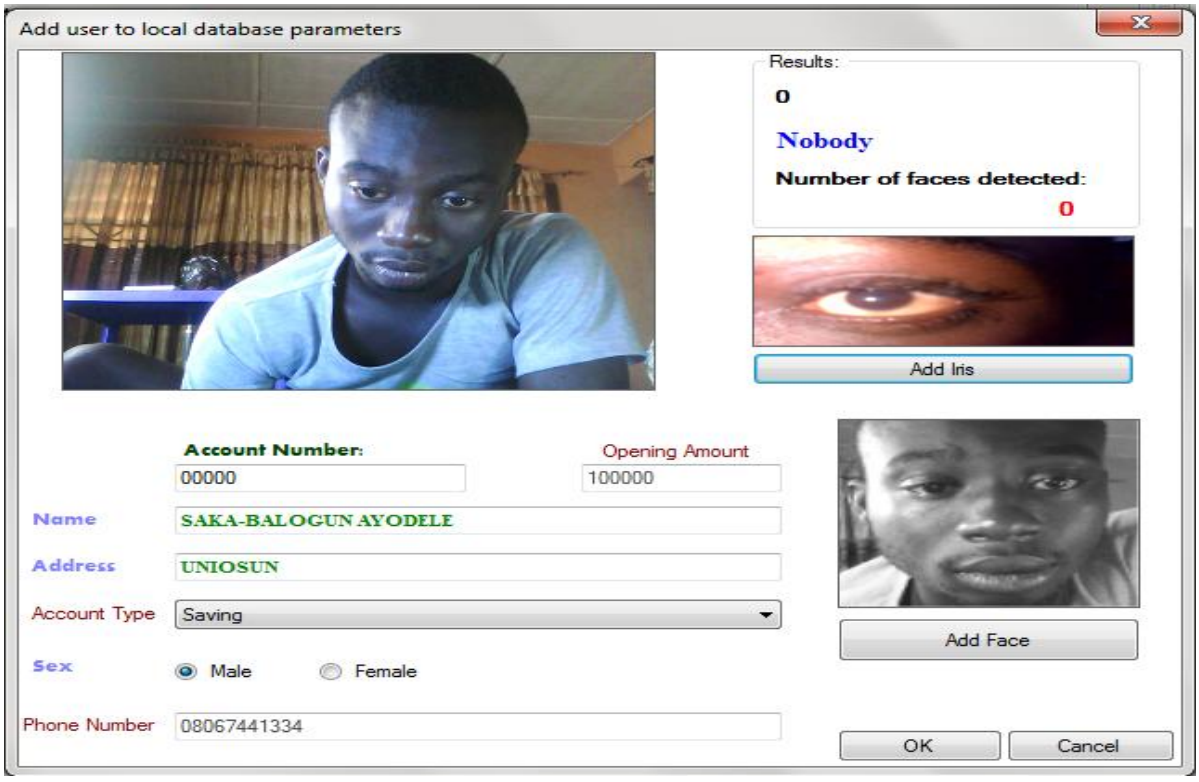

Figure 3. Captured screenshot of the administrative component for iris registration.

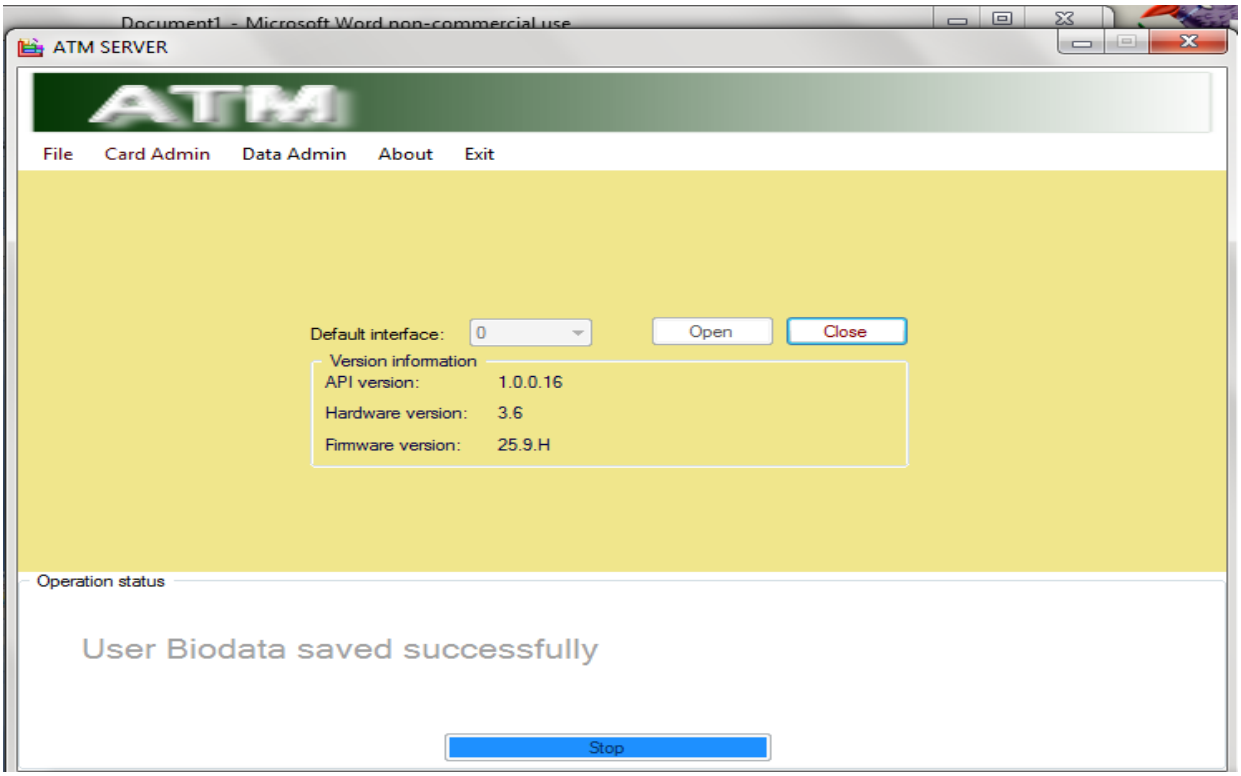

Figure 4. Captured screenshot of registration completion on the administrative component.

Figure 5. Captured screenshot of the user component for card supply.

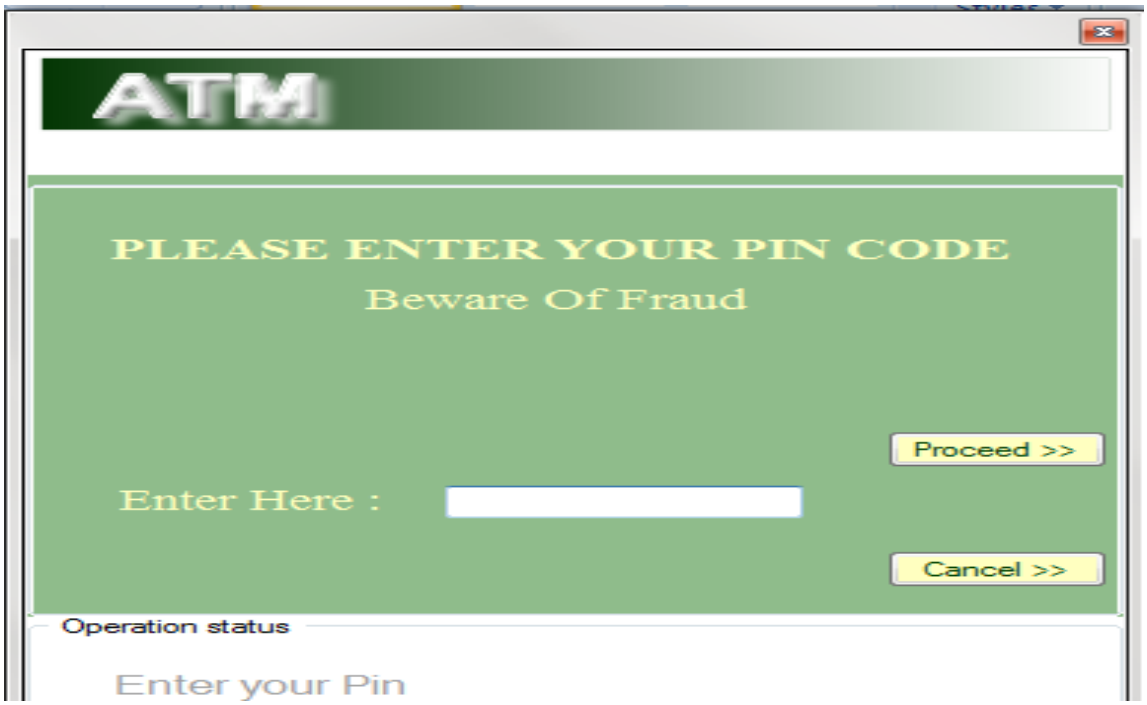

Figure 6. Captured screenshot of the user component for PIN supply.

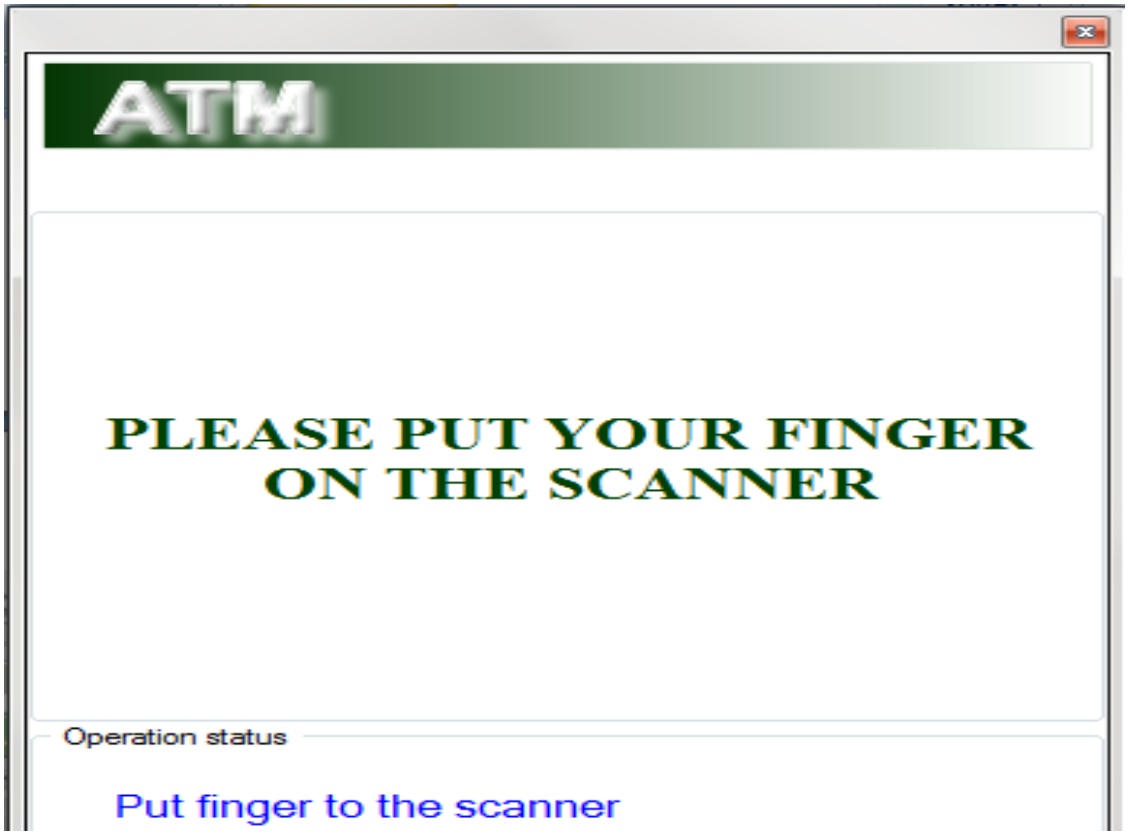

Figure 7. Captured screenshot of the user component for fingerprint supply.

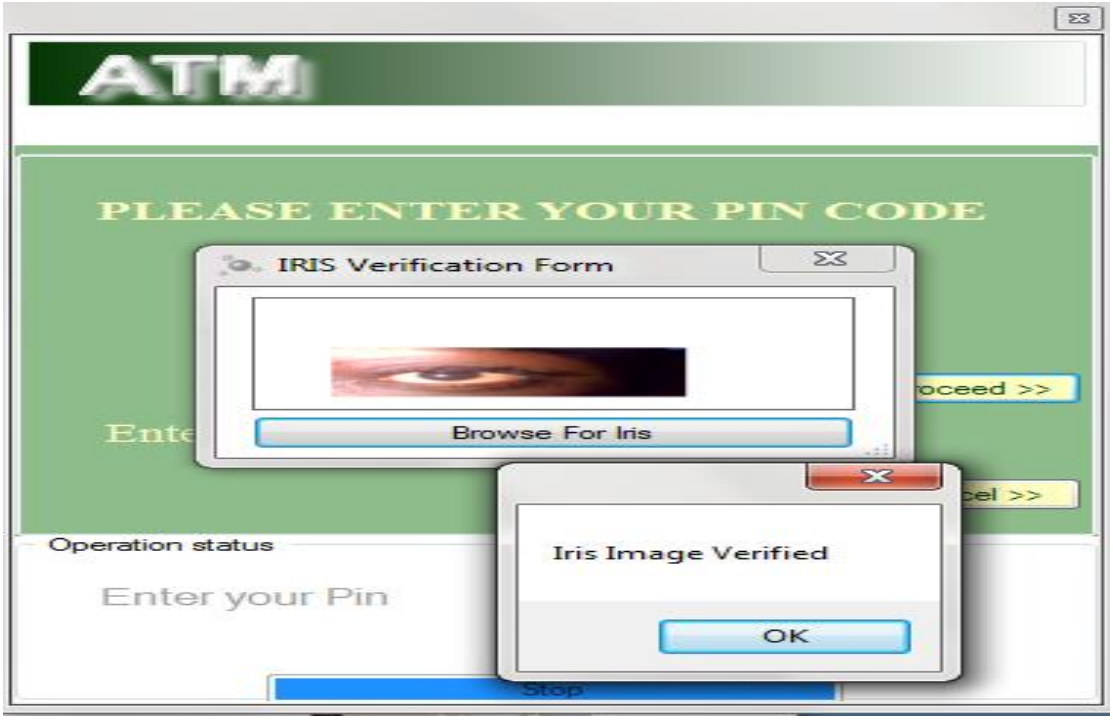

Figure 8. Captured screenshot of the user component for iris supply.

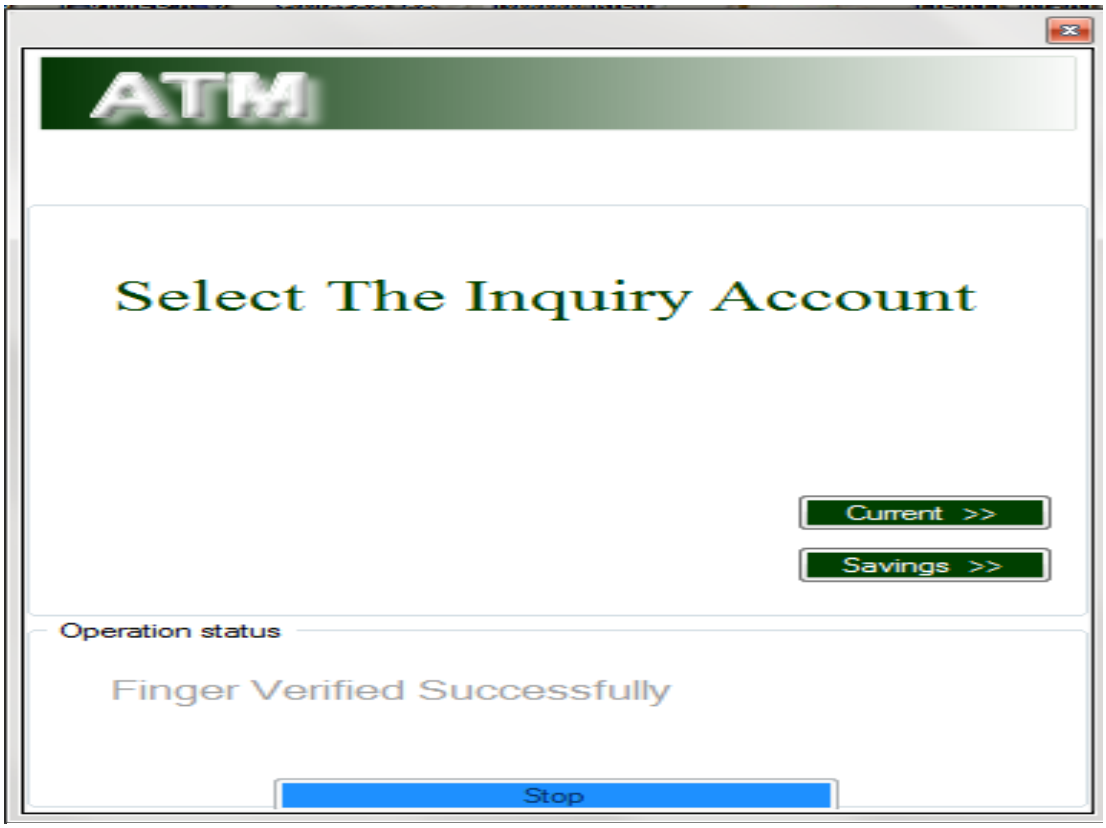

Figure 9. Captured screenshot of the user component for account selection.

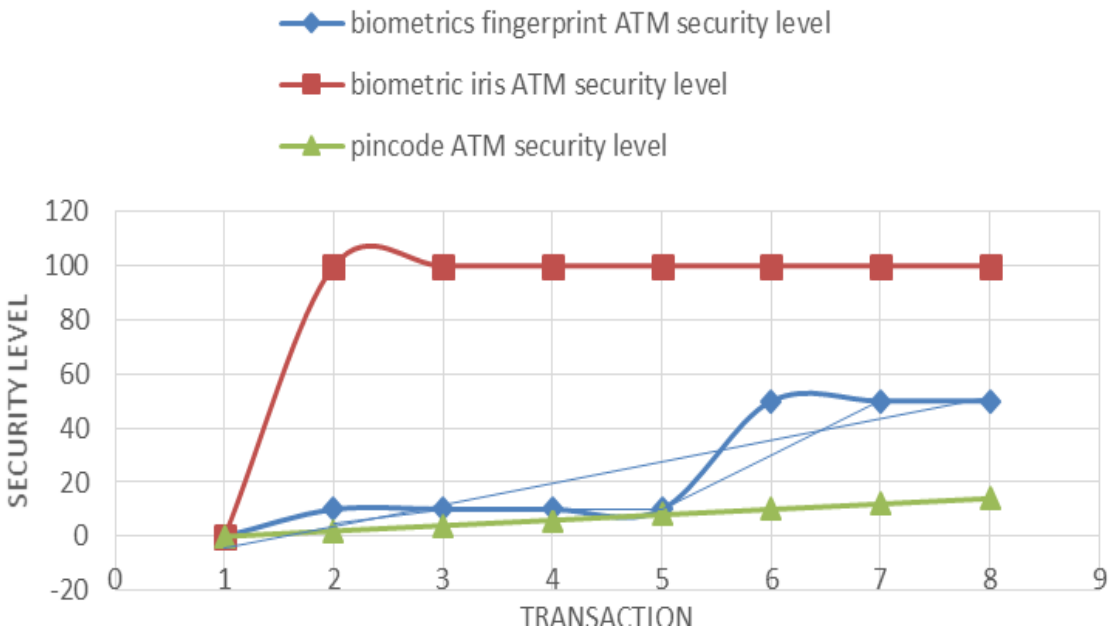

Figure 10. Graph of security levels of identification and authentication systems.

Table 1. Authentication results of the hybrid biometric system.

Cases	PIN	Fingerprint	Iris	Authentication result
1	Valid	Valid	Valid	✓ Approved
2	Valid	Valid	Invalid	Denied
3	Valid	Invalid	Valid	Denied
4	Valid	Invalid	Invalid	Denied
5	Invalid	Valid	Valid	Denied
6	Invalid	Valid	Invalid	Denied
7	Invalid	Invalid	Valid	Denied
8	Invalid	Invalid	Invalid	Denied

used to demonstrate the robustness and efficiency of the hybrid biometrics system in terms of identification, verification and authentication. The system exclusively identifies, verifies and authenticates transactions on correct entering of pin code, matching pre-stored fingerprint and iris in the database as shown in Table 1. From the Table, it is observed that the hybrid system only authenticates and approves transactions if, and only if the PIN, the fingerprint and the iris are valid. The fingerprint and iris reader successfully identified finger and iris from people that were pre-registered and stored in the database. However, in conjunction with the clients' Bank Verification Number (BVN), the system program code could be modified to accommodate registration of two or more next of kins and their respective biometric details, which can make proxy transactions for individuals in case of sickness or accident. This is to ensure flexibility of the system to real life situations. Moreover, multiple fingerprints registration up to six fingers (three fingers from each hand) could be allowed during registration to cater for matching users' identities in case of accident or finger injury.

Figure 10 shows the graphs of security levels of some identification and authentication systems. The Figure further illustrates the robustness of the developed hybrid biometric authentication system. The graphs demonstrated that the hybrid system of "biometric-iris-fingerprint-PIN" has most secured security level, followed by the hybrid system of "biometric-fingerprint-PIN" while the ordinary PIN authentication system has the least security level.

It was observed that fingerprint and iris image for

transaction authentication had to be supplied the exact way it was registered during data capturing. It is therefore recommended for individuals to place the finger and iris on the reader in such a way that the reader captures the middle of the fingerprint and the iris to ensure uniformity and consistency in the enrollment and verification processes.

A problem termed “false rejection”, which happens with any technology and manufacturer (Kumar and Ryu, 2009) may be associated with any biometric based identification system. However, this problem rarely occurs (below 0.1% of the cases. Improper functionality of the authentication system could result from wear and tear, ageing of components on the control circuit, corrupt authentication software and so on. However, for a robust and efficient system, adoption of a periodic preventive maintenance is suggested.

Conclusion

The hybrid biometrics based fingerprint and iris authentication system has been developed and demonstrated. The system demonstrated a high level of security in identification of individuals and authentication of transactions. An identification would be made and transaction approved if and only if all the three components of the hybridization matched the pre-registered respective values. This is unlike conventional ATM PIN system, where authentication is approved so far there is access to the card and the PIN is known.

The developed hybrid system could be deployed in ATMs employed in banks and other point of sales terminals. Although, no proxy withdrawal could be counted as a demerit of the hybrid biometrics system, the security level is worthwhile.

However, in conjunction with the clients’ BVN, the system program code could be modified to accommodate registration of two or more next of kins and their respective biometric details, who can make proxy transactions for individuals in case of sickness or accident. This is to ensure flexibility of the system to real life situations. Moreover, multiple fingerprints registration up to six fingers (three fingers from each hand) could be allowed during registration to cater for matching users’ identities in case of accident or finger injury.

RECOMMENDATION

The developed hybrid biometrics system is recommended for the governments to be used to boost security system to combat the current rate of corruption, fraud, terrorism and vandalism which potent great threat to economic development and sustainability. The system is recommended to be versioned into a single integrated multi-application card so that government programme such as financial budgeting, as well as health care services planning and management could be factored in. A single integrated multi-application card could be achieved by the use of chip-based GMPC technology, which allows for input of several applications on one card. Moreover, adequate selection of memory capacity and healthy maintenance culture are recommended in the hybrid system to ensuring accuracy of the system as the registered population increases as well as coping with high-growth database.

REFERENCES

Bechelli L., Bistarelli S. & Vaccarelli A. (2002). Biometrics authentication with smartcard. Technical report, CNR, istituto di informatics, pisa.

Gaurav P. & Shilpa S. (2017). Sports academy players attendance system using biometric fingerprint identification. Int. J. Sci. Res. Comput. Sci. Eng. Informat. Technol. 2(3):891-893.

Jayasinghe D., Akram R. N., Markantonakis K., Rantos K. & Mayes K. (2015). Enhancing EMV online PIN verification. Trust-com/BigDataSE/ISPA 2015 IEEE. 1:808-817.

Kumar D. & Ryu Y. (2009). A brief introduction of biometrics and fingerprint payment technology. Int. J. Adv. Sci. Technol. 4:25-38.

Lasisi H. & Ajisafe A. A. (2012). Development of stripe biometric based fingerprint authentications systems in automated teller machines. 2nd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA).

Mahesh N. K. & Govindarajulu P. (2016). Biometrics hybrid system based verification. Int. J. Comput. Sci. Informat. Technol. (IJCSIT) 7(5):2341-2346.

Mario Y. & Annuar G. (1995). ATM and biometrics: A socio-technical business mode. University of Miami, School of Business Administration.

Navneet S. & Vijay S. R. (2012). Role of biometric technology over advanced security and protection in auto teller machine transaction. Int. J. Eng. Adv. Technol. (IJEAT). 1(6):249-251.

Omar H., Din R. & Tahir H. M. (2000). Smart cards and the fingerprint: A framework for user identification and authentication. Journal of ICT. 2(1): 67-80.

Polemi D. (1997). Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable. Final report, Institute of Communication and Computer Systems, National Tecchnical University of Athens, April 1997.

Yakub K. S., Moshood A. H., Ismaeel A. A. & Akeem F. K. (2017). Fingerprint based approach for examination clearance in higher institutions. FUOYE J. Eng. Technol. 2(1):47- 50.