Enhancing Security in the Banking Sector using Biometric and Cryptography. A proposed framework for BACCSOD in Ghana.

Gerald Tietaa Maale[1], James Ben Hayfron-Acquah [2], Joseph Kobina Panford[3]

Computer Science Department, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

---

Abstract - *The era of Information Technology has evolved to the extent of simplifying almost all herculean tasks that are known to mankind. There is no exception for the financial sector in Ghana. Banks in the developed countries have seen different measures put in place to make daily banking routines comfortable and secure. The aim of this study was to explore ways of enhancing security using biometric and cryptography for the banking sector. For the purpose of this study, the biometric fingerprint and the OTP technologies were used for enhancing security of the banking system. It was found that the biometric fingerprint system could solve challenges posed by the use of signatures and thumbprints in verifying customers' account when withdrawing monies. It was also found that the use of a two level authentication model for authorising employees to login to the banking system would increase the performance and enhance security of the system. Based on responses from the respondents (employees and customers), a security framework was developed using biometric fingerprint, the Rijndael AES algorithm and OTP technologies in a form of cryptography were used. The proposed security framework was modelled by using system decomposition and taking into consideration the various sub systems that would communicate with each other. A prototype was developed in C# and tested. After the testing it was found out that the model or framework is feasible to secure and enhance the security of the banking system.*

Key Words: **Encryption, Security, Fingerprint, OTP, Bank, Authentication, Authorisation**

1.INTRODUCTION

1.1. Background

There exist various modes in which one can always transact business either with or without the help of employees of any financial institution. Most financial institutions delay customers unnecessarily over authentication and verification of accounts via the traditional methods of authentication. Signatures are now obsolete in using to authenticate a customer at a banking hall and then cross matching it with an old scanned low quality picture. A signature can always be forged and an identity card can be stolen or duplicated to impersonate a bank customer.

This therefore brings to bare the need for integrating a service with biometric and cryptographic authentication and authorization. The benefits of using biometric and cryptographic authentication systems in banking will secure the verification of a customer to the system and remove signature vulnerabilities. Many systems utilize a combination of these methods in order to increase the level of security. Thus, a possible option is to introduce biometric and or cryptographic authentication to secure the day to day transaction in the banking sector.

1.2. Research problem

CrossMatch [1] noted that most people in Africa, the Middle East and Asia are not banked because they cannot just conform to the requirements associated with identification in most financial institutions. Modern businesses use automated systems in a form of a computerised security system to verify users to ascertain their identities. There are about three approaches in which an individual is required to proof identity:

The first approach which asks for a user's username and password as noted by DigitalPersona [2] is the weakest connection in a network and system security, although that is the widely used approach in banking. This has been used for some time now in computing systems, but unfortunately has a problem that can be related to the decay of information or forgetfulness associated with the human memory and the unreliable mechanisms like the use of mnemonics or clues to retrieve stored information like password. Representations of identity from Surrogate as cited in Jain, Pankanti [3] stated that passwords are no longer

adequate for use in banking and government applications.

The second approach uses personal possessions of an individual to form identity. This approach is however inadequate because possessions like ID card and debit or credit card can be stolen. A password can be merged with the use of a credit card as used in ATMs to get around this problem as suggested by [4]. This however does not solve the problem because of the problem of the password in the first approach.

The third approach requests a user to authenticate an identity by using a unique trait such as the signature, which is also regularly used in banks. The challenge with this approach of using signatures is the replication of the signature by a counterfeiter. It becomes worst when a customer is an illiterate and prefers to use a thumb print instead of a signature in the banking sector.

All the above mentioned three approaches of identification have serious challenges when it comes to secure banking. Ghanaian banking environments and BACCSOD for that matter have similar mechanisms to check the identity of bank customers and are not an exception of these security challenges identified within the three approaches.

A new approach is therefore to propose a unique trait for a customer such as the use of biometric to get around the challenges that already exist. According to Jain, Bolle [5], no biometrics is effectively adequate to meet the needs of all authentication systems and this will request the use of some cryptographic protocols to further provide enhancements to security for the banking sector.

1.3. Research questions

i. What mechanisms can be put in place to enhance security by using cryptography in banking?
ii. How can security be enhanced by using biometric features in banking?
iii. What approach can be used to develop a security framework for the banking industry?

1.4. Objectives

The general objective of the study is to explore other ways of authenticating and verifying employees and customers using biometric and cryptography. The specific objectives of the study are to:

i. Determine mechanisms that can be put in place to enhance security by using cryptography in banking.
ii. Explore ways of enhancing security by using biometric features in banking.
iii. Develop a security framework for the banking industry.

1.5. Significance

Executive leaders in banks, government agencies and other enterprises have noted that employing biometrics is a more reasonable and secured way to deliver efficient financial services [1]. It has reached a point in Ghana where authentication technologies can be adapted to ease customer forgetfulness in entering passwords and signing signatures. BACCSOD, the financial institution used for this study has a vast majority of its customer base in the informal sector and most of its clients not formally educated. It is evident that clients already have a conception of the fingerprint technology but in a legacy and unsecured way. Therefore, this study is aimed at eliminating forgeries, insecurity and inconveniences associated with the existing technological methods in the financial sector by using the combination of biometric and cryptography to enhance the security in banking in BACCSOD.

2. LITERATURE REVIEW

2.1. Understanding Biometrics

Biometric refers to the spontaneous proof of identity based on an automatic recognition of a person's physiological or behavioural characteristics [6]. Biometrics establish an individual's identity based on who he is rather than by what he possesses for instance ID Card or what he remembers like a password [7]. Recognition of a person by a unique part of their body and then linking that part to a well-known identity forms a reliable and powerful method of identifying oneself [3]. Biometrics are therefore captured and compared with another instance at the time of verification or identification [8]. Physiological biometrics include those based on the verification of fingerprint, hand geometry, eye iris and face. Behavioural biometrics include those based on voice,

signature, typing behaviour, and pointing. Biometrics methodologies follow a similar operation: a digital template is created during an enrolment process, then the template is stored in a database [9].

A. Fingerprint Recognition

Fingerprint identification uses the process of comparing two samples of finger ridge skin imprint from human [10]. Fingerprints are popular in identifying and verifying individual's identity using the ridges and valleys (minutiae) on the surface tips of a human finger helps to identify a person [11].

B. Face Recognition

Facial recognition is the use of facial features for the recognition an individual's identity. A facial recognition system is designed to authenticate a person with the use of a computer application which captures images or video from a camera source analysing the facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These dimensions are then designed into modules and stored in a database. According to Babich [10], the face of a person has 80 nodal points which can be measured by using a software.

C. Iris Recognition:

Iris recognition is a computerised method of using an individual's eye as a unique feature of the human body to provide identity using mathematical patterns on images. Iris recognition uses a pattern recognition and capturing process via the use video images [12]. Algorithm of the iris recognition examines the patterns in the iris and converts the pattern to a 512-byte digital template and store in a database.

D. Hand Geometry

Hand geometry involves the measurement and analysis of the human hand [13]. According to Bača, Grd [14], "Every human hand is unique" (p. 80). The hand geometry method of authentication involves capturing the top and side views of the hand using a camera to enrol an individual template in a database. Two snapshots of the hand are taken and the average of resulting feature vectors is computed and stored.

E. Voice

Voice in biometrics is obtained as a numerical model of the sound of a person's voice. The identity of a voice is identified when the two processes match the sample taken from the individual. According to Babich [10], the human voice has about 100 distinctive features that make voice biometrics to be one of the most dependable.

F. Signature Recognition

Signature recognition is an illustration of an individual's writing that has been accepted as unquestionable proof in documents [13]. The manner in which an individual signs his or her name is recognized to be a distinguishing feature of that individual. Professional counterfeiters can reproduce signatures to impersonate the recognition of an individual.

2.2. How Biometrics Work

The biometric process involves three processes that is capture, process and enrol. This is then followed by an identification or a verification process. Raw biometric data is captured during the capture process by using a fingerprint reader or a live camera. The capture device is used to extract the unique features of the individual as raw biometric data and then converted into a processed biometric identifier record known as a biometric template. This process is usually known as the enrolment process; the template is then stored in a database for future use. A biometric system is sometimes used for identification or verification. The identification module uses the one-to-many approach. This is when a specific biometric template is searched among several biometric templates. The verification module also uses one-to-one approach of authentication. This is when the identifier is present before the biometric device to authenticate.

2.3. Understanding Cryptography

Cryptography according to Delfs and Knebl [15] is also the art of keeping secrets secret. Cryptography generally is about creating and analysing procedures that prevent adversaries from intercepting communications. Cryptography can therefore be used for user authentication but not only

protecting data from alterations. According to Menezes, Van Oorschot [16], modern cryptography is essential in information security including data authentication, confidentiality, integrity and non-repudiation.

i. Authentication/ Identification: This service applies to the sender and recipient of the message. The two individuals communicating should identify each other by using established keys.
ii. Confidentiality: Any adversary intercepting an encrypted message should not have access to the original message, unless having access to the key. The encryption and decryption schemes are the features of confidentiality.
iii. Data Integrity: the recipient of a message is assured that the original data has not been tempered by any adversary.
iv. Non-repudiation is a service which prevents a person from disagreeing to earlier actions in a communication which sometimes involves a trusted third party to resolve the disagreements that occur.

1) 2.3.1. Types of Cryptographies

There are basically two types of cryptographic systems used to secure communication between entities: secret key (or symmetric) cryptography and public key (or asymmetric) cryptography. The initial unencrypted data is known as plaintext and it is then encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext [17].

A. Symmetric or Private Key or Secret Key Cryptography (SKC)

Symmetric-key or private key encryption are set of rules that protect messages using same secret keys to encrypting plain texts and decrypting ciphers. Symmetric key requires the possession of the same key to encrypt the data by the sender and also to decrypt the same data by the recipient. The sender uses a secret key to encrypt the plain data and sends it to the receiver. The recipient then uses the same secret key to decrypt the data to decipher the data. This thus is called symmetric encryption because a single same key is used for functions [15].

There are two types of symmetric keys that is stream cipher and block cipher. A **stream cipher** is a symmetric key where plaintext text and a keystream are combined together to form encryption. Stream ciphers encrypts plain text one a time using a text corresponding to the keystream [16]. Stream ciphers runs at a higher speed and have lower hardware complication. **Block cipher** is a symmetric block cipher that encrypts data in fixed-size often 64 bit blocks. Messages that exceed n bits usually requires partitioning the message into n-bit blocks and encrypt each separately; where n is the number of bits. A block cipher encrypts one block of data at a time using the same key on each block [17]. A block cipher can be completely altered if the private key can be found from a cipher text.

DES (Digital Encryption Standard): The DES is a block cipher with symmetric private key which uses a 64-bit key as block length of which 8 bits for error-checks. DES has a key length of 56 bits and encrypts blocks of 64 bits of plaintext at a time. According to Garrett [18], ANSI included DES as an encryption algorithm for the private sector but was considered insecure due to its short key length which can be vulnerable to brute force attack.

AES (Advanced Encryption Standard): AES replaced DES from an organised contest by NIST. NIST [19] requested that the new AES algorithm must use a symmetric key block cipher that should support a minimum block sizes of 128-bits and key sizes of 128, 192, and 256-bits. Rijndael was announced by NIST as the winner of the contest. The Rijndael algorithm can extend the block length and key length by multiples of 32 bits. The Rijndael is suited for the efficient application in hardware or software on an array of processors.

Asymmetric or Public-Key Cryptography (PKC)

Asymmetric cryptography is key system that uses both public and private keys known to the owner only. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher text. Both keys are required for the process to work [15, 17].

RSA public-key encryption: RSA is public key encryption that uses a both public key and a corresponding private key in each entity. The RSA system is created by finding the product of two very large prime numbers and making their product *n*

public, whereas the factors of *n* are kept secret and used as the secret key. The basic idea is that the factors of *n* cannot be recovered from *n*. The security of RSA depends on the tremendous difficulty of factoring [15].

Diffie–Hellman Key Agreement: Diffie–Hellman key also known as the exponential key exchange enables two parties that have never communicated before to agree on a large prime number over a public channel. D-H requires the parties to pick another number such that the number is greater than the prime number. The public keys are public whilst keeping the private key secret to cipher and decipher message from both parties [17].

2) 2.3.3. Application of Cryptographic Protocols

A. Challenge-Response

Challenge-Response protocol involves the use of challenges or questions and answers to parties involved in the communication. The sender of the message provides a challenge to the recipient, and the recipient provides the valid answer to the question. The value is encrypted with a secret key and the result is sent back to the challenger, for comparison with his own calculated value.

One-Time Passwords (OTP)

The One-Time Password makes it more impossible to gain unauthorized access to restricted sections of a user account. One-Time Password offers a continued alteration of passwords or PINs to prevent attackers from guessing passwords to authorised systems [20].

2.5. Consideration of Biometric Fingerprint Recognition

Biometric helps an individual to be verified or identified by using traits of part of the human body that is unique. For the purpose of this study, the biometric fingerprint recognition system has been considered. The study of the various biometric technologies by Jain et al. (2006) which was structured under seven modalities: universality, uniqueness, permanency, collectability, performance, acceptability and circumvention were tested. From the test, it was indicated the fingerprint recognition possessed the most modest and affordable ratings for the use as an authentication system. The biometric fingerprint technology uses a unique trait that is the fingerprint which is easy and convenient to setup for the use in banks to perform enrolments and verification of customers and employees considering the various modalities studied by [5, 13, 21].

2.6. Consideration of the AES algorithm and OTP technique

In this study, the Rijndael AES algorithm and the OTP would be used as the main cryptographic protocols for encrypting and decrypting data to prevent adversaries from eavesdropping. The OTP is a unique short password that validates an authentication session and provides continued alteration of random codes to prevent attackers from guessing the right code within a given period of time usually 30 seconds which cannot be reused.

3. METHODOLOGY

3.1. Population and Sampling

A qualitative research methodology was primarily used in this study to gathered data. The biometric and cryptography security framework was modelled using UML diagrams, algorithms for encrypting and decrypting data, and the Futronic SDK for biometric enhancements.

BACCSOD is one of the leading financial institutions in Ghana located in the Brong Ahafo region with wide coverage of its members throughout the region. BACCSOD has two administrative headquarters in Sunyani and Techiman with about twenty-six (26) branches in the whole of Brong Ahafo Region of Ghana. BACCSOD can located at almost all Catholic Parishes in Brong Ahafo region with about 150,000 active clients and about 150 employees for all branches.

The study used the convenience sampling and purposive sampling techniques. Customers were sampled using a convenience sampling technique because they were easily spotted and readily available for the study. Because of the busy nature of employees' work at the bank, they were sampled using a purposive

sampling technique targeting specific employees across both managerial and non-managerial positions to spare a few minutes for the study.

Because of the large population of both customers and employees of BACCSOD, the study used the administrative headquarters of BACCSOD at Sunyani and Techiman for sampling. Out of 25 employees at the Techiman BACCSOD branch, 14 were sampled. Also, out of 19 employees at the Sunyani branch of BACCSOD, 12 were sampled. A total number of 26 employees were sampled to respond to the questionnaires. 20 customers from each branch (a total of 40 customers) were also sampled to respond to the questionnaires.

The data collection methods used in this study were observation, interviews and, secondary sources of data, which were all used to collect and process data to achieve all the objectives of this study with unblemished comprehension of the problem. This method was used as capturing process for the study. It aided in the collection of requirements of the operations of the day-to-day business in the bank.

The management of the organisation, employees and customers were debriefed on the research and made to understand the essence of the study was purely academic-based research.

3.2. Proposing the new security framework

The data that would be collected will aid in proposing the new security framework for BACCSOD. The new security framework seeks to enhance the already existing banking system of BACCSOD using biometric and cryptography. A system analysis and design would be modelled to implement the various mechanisms of the enhancements to the already existing banking system.

4. RESULTS AND DISCUSSION

4.1. Existing Banking System

Employees were observed on how they used the existing banking system that is Tally ERP. The Tally ERP9 application is a fully developed accounting package for the use in most financial institutions in the world including It was however observed that passport photograph, signature or thumbprint of customer, address of customer and identity of customer were not used in the Tally system.

4.2. Discussion

Twenty-six (26) employees from both Techiman and Sunyani diocese of BACCSOD were interviewed; 11 females and 15 males. 6 were managerial level members and 20 were non-managerial level members. Respondents responded affirmatively to questions on authentication problems with the Tally ERP, frequency in password resets with the Tally ERP, biometric fingerprint technology and OTP verification system. It was concluded that the new security framework could enhance the existing system if the fingerprint system or the use of OTP is used to authenticate customers during withdrawal process. The OTP was also recommended for the second level authentication for employee's authorisation to the system via login.

4.3. Proposed security framework

The new security framework would use the fingerprint recognition system, the Rijndael AES and OTP algorithms. The new framework will be known as the Biometric-Cryptography Banking Management System, **BCB-MS**.

The process of using a fingerprint system is designed to be simple and hustle free. Customers will place a finger on a fingerprint scanner during an enrollment stage. A quality fingerprint scanner will capture a complete image that can be used as an entirely unique identifier. These biometrics are combined with other data to create a complete identity file for each customer which is encrypted and saved in a central database server. When customers want to access their accounts, they simply scan a finger and an authentication system compares the scanned image to the stored image in the database.

Access to customer's bank is only granted if a scanned fingerprint matches the information stored in the individual's secure identity file in the server. An OTP will be essential in authorising the customers if there are difficulties in using the fingerprint reader to

authenticate at banking terminals in the form of SMS (Short Message Service). The employee would also use the OTP to authenticate a session login coupled with a username and a PIN. The OTP sent on the phone for verification from the OTP Server would be authenticated via SMS. The AES algorithm from Rijndael would be used as added security enhancements to data stored on the system by encrypting PIN codes and OTP codes stored.

System Strengths

The BCB-MS is a security framework developed to integrate a banking system. These are main benefits of this system:

It avoids the use of signatures in banking. The signatures are replaced with the fingerprint recognition system and OTP in verifying a customer.

The system is also capable of taking live photographs and storing them in the database. Customers go through a lot to get a passport photograph to open an account at the bank. This will boost the confidence level of the customer.

The system also reduces the rate of impersonation. This often happens when someone knows your identity (username and password or pin). With the system, a second level authentication is introduced to verify and authorise an employee who uses the system by using OTP.

System Limitations

There are few limitations of the BCB-MS system:

a) It does not address general problems in banking using the various accounting practices.

b) The system only uses a single fingerprint template for verifying a customer. In the event where an individual has a problem with the single finger, there can't be any verification with the fingerprint system unless the OTP verification.

c) The system can only allow an employee to login the system after successfully verifying an OTP code. This however can cause a level of delay when there are problems with telecommunication networks and SMS gateways.

4.4. System Analysis and Design

This section outlines the stages in which the proposed system is modelled. The existing system, Tally ERP is analysed and used to create models using UML diagrams. The Requirements specification document is created to capture user requirements, hardware requirements, software requirements, functional requirements and non-functional requirements of BACCSOD.

Activity diagrams are used as flowcharts to represent the order in which operations happen. An activity implements the description of a use case. In this section, the activity diagram is used to describe how the customer and employee interact with the banking system as illustrated in the use case diagram.

Fig-1. shows the authorisation activity of the proposed security system that deals with the fingerprint and OTP verifications. If the fingerprint verification fails three (3x) times, the next option being the OTP is invoked. If the fingerprint or OTP verification is successful, the next activity is executed. In this process, one of the methods (Fingerprint or OTP) should be able to identify the customer with the appropriate image confirming the owner of the account. If the authorisation is successful, then the employee approves the withdrawal else the customer is obliged to re-verify using any of the two methods.

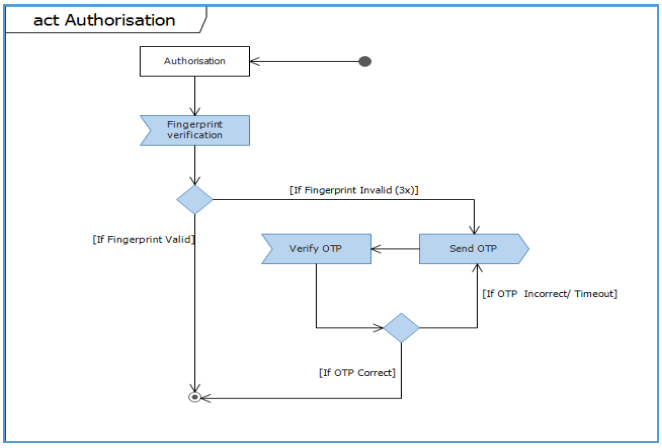

Fig- 1: Authorisation Activity Diagram of the BCB-MS

4.5. System Architecture

The repository architectural style is used for the BCB-MS. According to Bruegge and Dutoit [22], repositories are classically used for database management systems such as a bank system. The location of the data at the central makes it easier to deal with concurrency and integrity issues between subsystems. The layered architecture pattern is used to illustrate the repository architectural style for the BCB-MS. The architecture representation in layers is represented in Fig-2.

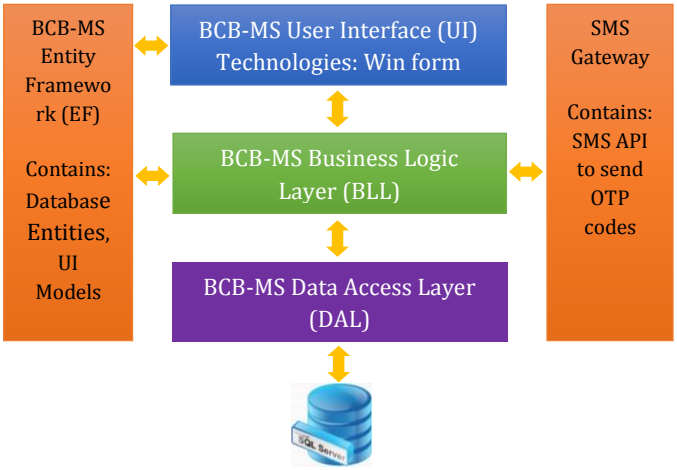

Fig- 2: BCB-MS Application Architecture

From figure 2, the first layer which is the Presentation layer implements the user interface (UI). In the case of the BCB-MS, the user interface has been implemented with Windows Forms (Winform).

The second layer is the Business Logic Layer (BLL). The BLL of BCB-MS contains all the rudiment algorithms that are used for calculations and business rule validations. It further includes the functionality of the system and other components that implement system security, bank information creation and updating the database.

The third layer is the Entity Framework Layer (EF). This layer implements the entity model of the database. This is the only layer that communicates with the Data Access Layer (DAL) of the architecture.

The last layer is the Data Access Layer (DAL). It contains functionality for Creating, Reading, Updating, Deleting (CRUD) items to the database. In this layer, technologies like ADO.NET and Entity Framework were used. The DAL is connected via a database server as back end. The back end of the application is Microsoft SQL Server

4.6. System development

The system was developed using C# and Microsoft Visual Studio IDE. MSSQL Server is a Relational Database Management System (RDBMS) that was used to store the objects of the system and its associated attributes mapping them to their respective entities.

The employee login interface of the BCB-MS was developed to implement a two level authentication system. The use of PINs helps employees to remember a simple a four-digit code which will be authenticated with the combination of an OTP code generated by the system.

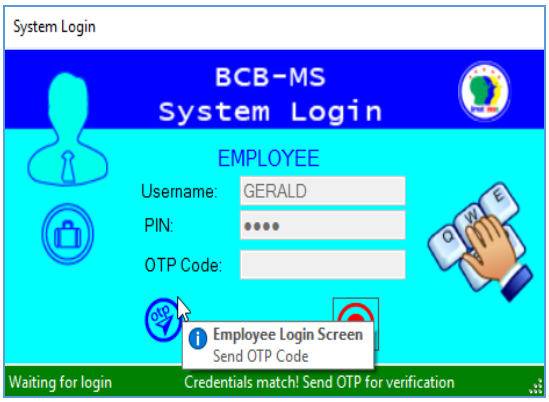

Fig- 3: Employee login interface

Fig-3 shows how the enhancement to the login interface for employees using username, PIN and a valid OTP code. After a successful entry of the first level of authentication, employee clicks to send OTP code via SMS for verification as the second level authentication. If for any reason the OTP code is failed to be entered before 30 seconds, the code is reset for re-verification.

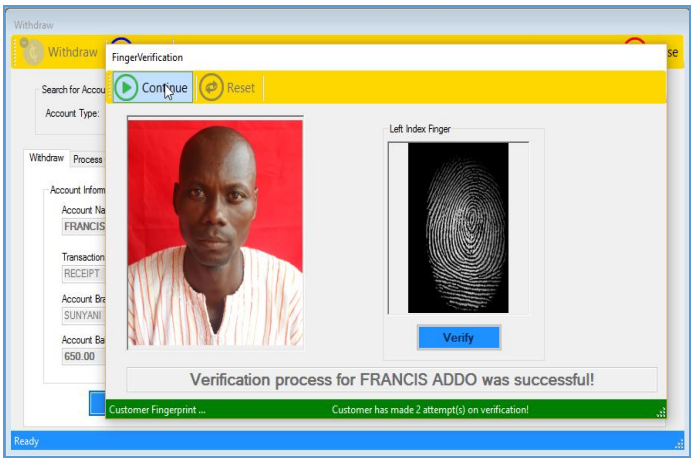

Fig- 4: Verification of customer by fingerprint

Fig-4 shows the authentication of a customer using a fingerprint. The customer is directed to place a recognised finger on the fingerprint scanner to verify the account. The fingerprint is extracted and matched with the enrolled template of the person to verify the authenticity of the account. It is however noted that if the verification using the fingerprint fails for three consecutive times, the OTP option is activated automatically to address the challenge of using the fingerprint scanner.

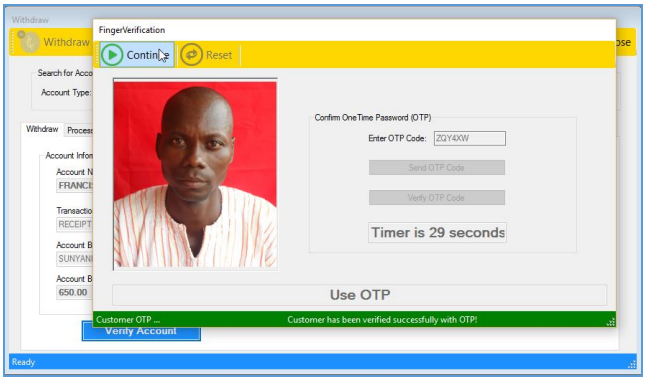

Fig- 5: Verification of customer by OTP

Fig-5 shows the interface for the authentication by use of OTP in verifying a customer's account in place of the fingerprint recognition. After sending the OTP code as a message to the customer via SMS, the customer has within 30 seconds to confirm the code to the employee for verification on the system. The OTP code is always encrypted and stored on the server. During verification, the code is retrieved, decrypted and then matched with the code entered in the textbox of the verification interface.

The BCB-MS is deployed on the banking terminals with the database located on a central server for effective access. Fingerprint readers would be connected to the banking terminals to provide account authorisations by customers. The system was tested using Unit Testing and User Acceptance Testing. Unit testing is the practice of testing certain functions and units of an application code. The unit testing of the BCB-MS was done using Microsoft Visual Studio Unit Testing framework. Tests are usually saved and run again if any part of the code changes. This helps with regressions and increases confidence in fixing errors, refactoring, and late additions. The user acceptance testing was the last testing of the system. The stakeholders evaluated the system to expose the errors and omissions of the requirements that were defined in the analysis phase of the system development. The UAT was conducted at Sunyani in the banking hall of BACCSOD. The testing of the BCB-MS by both employees and customer proved that the developed system had enhanced security using the fingerprint and OTP as a way of authentication and authorisation.

5. CONCLUSION, RECOMMENDATION AND FUTURE WORK

5.1. Conclusion

The use of fingerprint recognition system in banks provides reliable and robust authentications and authorisations. The fingerprint eliminates inaccuracies and vulnerabilities in customers' signatures during cash withdrawal processes. Customers could be assured that transactions would be safely done devoid of all impersonations. Encryptions by using the AES algorithms provide added security enhancements to prevent eavesdropping and attacks. OTP codes generated for employees have added a second level authentication to prevent other employees from stealing keystrokes of senior employees to cause frauds at the banks.

5.5. Recommendations for future work

The following recommendations are made to facilitate and overcome of the limitations stated above in the study:

Future studies should investigate the use of all fingers in verifying an individual of the bank. This will address the problem of the single fingerprint used in this system.

Future enhancement can also be made for an employee to log into the system with a fingerprint instead of the username, PIN and OTP code.

REFERENCES

1. CrossMatch. *BIOMETRICS IN BANKING*. From Unbanked to Lifelong Customer 2014 [cited 2015 October 21]; Available from: http://www.crossmatch.com/biometrics-in-banking/.
2. DigitalPersona. *Enhancing Security with Biometric Authentication*. 2015 [cited 2015 October 20]; Available from: http://www.comptalk.com/documents/white-papers/EnhancingSecurity.pdf.
3. Jain, A.K., et al. *Biometrics: a grand challenge*. in *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*. 2004. IEEE.
4. Das, S. and J. Debbarma, *Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian E-Banking system.* International Journal of Information and Communication, 2011: p. 197-203.
5. Jain, A., R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*. Vol. 479. 2006: Springer Science & Business Media.
6. Mayhew, S. *History of Biometrics*. 2015 [cited 2016 February 14]; Available from: http://www.biometricupdate.com/201501/history-of-biometrics.
7. Jain, A.K., *Biometric recognition: how do I know who you are?*, in *Image Analysis and Processing–ICIAP 2005*. 2005, Springer Berlin Heidelberg. p. 19-26.
8. Onyesolu, M.O. and I.M. Ezeani, *ATM Security Using Fingerprint Biometric Identifer: An Investigative Study.* International Journal of Advanced Computer Science and Applications, 2012. **Volume 3**: p. 68-72.
9. Coventry, L., A. De Angeli, and G. Johnson. *Usability and biometric verification at the ATM interface*. in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003. ACM.
10. Babich, A., *Biometric Authentication. Types of biometric identifiers*. 2012, HAAGA-HELIA University of Applied Sciences. p. 56.
11. Biometric-Solutions.com. *Fingerprint Recognition*. 2015 [cited 2016 4 April]; Available from: http://www.biometric-solutions.com/solutions/index.php?story=fingerprint_recognition.
12. IrisAccess. *Iris Recognition Technology*. 2016 [cited 2016 5 April]; Available from: http://www.irisid.com/productssolutions/technology-2/irisrecognitiontechnology/.
13. Angle, S., R. Bhagtani, and H. Chheda. *Biometrics: A further echelon of security*. in *UAE International Conference on Biological and Medical Physics*. 2005.
14. Bača, M., P. Grd, and T. Fotak, *Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics*. New Trends and Developments in Biometrics. 2012.
15. Delfs, H. and H. Knebl, *Introduction to Cryptography*, in *Principles and Applications*, D. Basin and K. Paterson, Editors. 2015, Springer-Verlag: Berlin Heidelberg. p. 529.
16. Menezes, A.J., P.C. Van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*. 1996: CRC press.
17. Kessler, G.C., *An Overview of Cryptography*. 2015. p. 46.
18. Garrett, P., *Cryptographic Primitives.* 2007.
19. NIST. *Advanced Encryption Standard (AES)* Development Effort 2001 [cited 2016 5 April]; Available from: http://csrc.nist.gov/archive/aes/index2.html.
20. Barral, C., *Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography*, in *À La Faculté Informatique Et Communications*. 2010, École Polytechnique Fédérale De Lausanne. p. 244.
21. El-Abed, M., C. Charrier, and C. Rosenberger, *Evaluation of Biometric Systems*, in *New Trends and Developments in Biometrics*. 2012, INTECH. p. 149-169.
22. Bruegge, B. and A.H. Dutoit, *Object-Oriented Software Engineering Using UML, Patterns, and Java*. 3rd ed. 2010: Prentice Hall. 778.