Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Enhancing Security In The Rural Banking Sector Using Biometric and Cryptography

Henry Kwabena Safori
Ghana Institute of Management & Public Administration
GreenHills Accra, Ghana
E-mail: kwabenahenry@aol.com

ABSTRACT

Since the advent of information technology, nearly every impossible task known to man has been made simpler. Ghana's financial sector is not an exception. Different steps have been implemented in banks in industrialized nations to make daily banking procedures comfortable and secure. The purpose of this study was to investigate how to increase security for the rural banking industry utilizing biometrics and cryptography. For the purposes of this study, the financial system's security was improved using the biometric fingerprint OTP technologies. It was discovered that the problems associated with using signatures and thumbprints to validate a customer's account when withdrawing money may be resolved by the biometric fingerprint technology. Additionally, it was discovered that using a two-level authentication architecture for allowing employees to enter into the banking system would improve the system's performance and security. A security framework was established combining biometric fingerprint and OTP technologies as a kind of cryptography based on responses from the responders (workers and customers). By employing system decomposition and taking into account the many subsystems that will communicate with one another, the suggested security framework was developed. The model or framework can be used to secure and improve the security of the banking system, it was discovered after testing.

Keywords: Rural Banking, Cybersecurity, Biometrics, Cryptography, Security

Proceedings Citation Format
Henry Kwabena Safori (2022): Enhancing Security In The Rural Banking Sector Using Biometric and Cryptography. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022.
Pp 154-160. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P31

1. INTRODUCTION

There are numerous ways to do business, both with and without assistance from staff at any financial institution. Most financial institutions provide their clients unnecessary delays when it comes to account verification and authentication using the conventional methods of

authentication. Signatures are no longer used to authenticate a consumer at a banking facility when a low-quality, outdated scan of the customer's photo is used as a cross-check. An identity card can be stolen or copied, and a signature can always be faked to pass as a bank customer. The necessity of integrating a service with biometric and cryptographic authentication and permission is thus made clear. The advantages of utilizing biometric and cryptographic authentication methods in the banking sector will protect client system verification and eliminate signature weaknesses. In order to raise the level of security, several systems combine these techniques. In order to secure routine banking transactions, it may be possible to introduce biometric and/or cryptographic authentication.

2. RELATED LITERATURE

Verifying customers with only a finger to grant access to their account as proposed by Gerald et al 2016 is one of the best ways to authenticate employees and customers of a bank. In addition to the that is the OTP, the One Time Password which is sent to their phone after verifying their biometrics. After the verification process an OTP will be sent to the customer to ensure authenticity. Employees also goes through the same process to verify them before the user interface of the banking information system is open to them to start their day-t-day activity.

2.1 Fingerprint Recognition

Two samples of human finger ridge skin imprints are compared in the process of fingerprint identification [10]. The ridges and valleys (minutiae) on the surface tips of a human finger are commonly used in fingerprinting to identify and authenticate an individual's identity [11].

2.3 Understanding Cryptography

Delfs and Knebl [15] define cryptography as the art of keeping information secret. Creating and analyzing methods to stop adversaries from intercepting communications is the general focus of cryptography. Because of this, cryptography can be used for user authentication in addition to data protection. Modern cryptography is crucial for information security, including data authentication, secrecy, integrity, and non-repudiation, according to Menezes, Van Oorschot [16].

i. Message sender and recipient are both covered by this service for authentication and identification. The two parties communicating should recognize one another using predetermined keys.
ii. Confidentiality: Unless they have access to the key, any adversary intercepting an encrypted message should be prevented from seeing the original message. The characteristics of confidentiality include encryption and decoding techniques.

2.4 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.

3. FINDINGS

Most rural banks depend mostly on the market women to survive but most of these traders have low level of education. This makes it difficult for then to transact business with the rural banks because the processes involved in getting an account and the withdrawer of funds from one's account seems very cumbersome to them. Getting their signature right for taking money from their account becomes a problem because not all of the traders remember the way they signed when crating the account. Due to this most of them decline the request given them by most banks to create a savings account for them but are interested in their loan facility and since they don't want to be stressed, they decide to ignore.

4.1 Research Gab

The proposed banking verification systems use only a finger to verify their customers in addition to the OTP. When that finger becomes unavailable for use the bankers need to by-pass the system and do manual verification to be able to serve that particular client when the too OTP also fails.

5 RECOMMENDATIONS FOR PRACTICE

Enhancing the banking system with biometric and cryptography makes their system very strong be under estimated by adversaries. Signatures and thumbprints are very easy to be forged by the professionals to use it for the wrong purpose at the right time. This is why its very necessary for every institution to strengthen their security system to avoid losses and again which ever means they use to secure their systems must have a cryptography as an additional method to make it reliable

5.1 Policy and Design

The key cryptographic protocols in this study for encrypting and decrypting data to prevent adversaries from listening in would be the Rijndael AES algorithm and the OTP. The one-time password (OTP) is a one-of-a-kind short password that authenticates a session and offers ongoing random code alterations to prevent attackers from guessing the appropriate code within a certain time limit, often 30 seconds, and which cannot be repeated.

The Rijndael AES and OTP algorithms, as well as the fingerprint identification system, would be used by the new security framework. The Enhanced Security Banking Management System will be the name of the new framework proposed. A fingerprint system is made to make utilizing it easy and hassle-free. During the enrollment process, customers will place their fingers on a fingerprint scanner. The full image that is captured by a high-quality fingerprint scanner can be utilized as a completely unique identity. A complete identity file for each customer is created using these biometrics in conjunction with other information. This file is encrypted and saved in a centralized database server. Customers just scan their fingers to gain access to their accounts, and an authentication system matches the scanned image to the image that is already saved in the database.

Only when a scanned fingerprint matches the data in the person's secure identity file on the server is access to the customer's bank permitted. If there are issues utilizing the fingerprint reader to authenticate at banking terminals by SMS, an OTP will be necessary for authorizing the consumers (Short Message Service). Additionally, the employee would utilize the OTP to confirm a session login along with a username and PIN. The OTP that was obtained by phone from the OTP server for verification would be verified by SMS. By encrypting PIN codes and

storing OTP codes, the Rijndael AES technique would be employed as further security upgrades to data saved on the system.

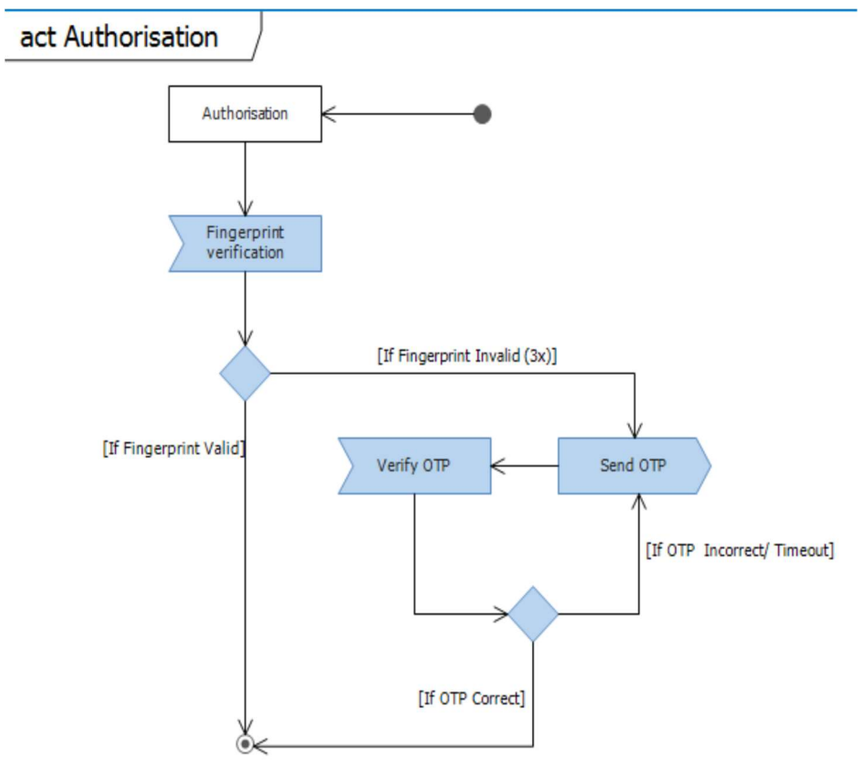

Fig- 1: Authorisation Activity Diagram of the system (source Gerald et al. 2016)

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.

5.2 Conclusion

The application of fingerprint recognition technology in banking institutions offers trustworthy and strong authorizations and authentications. During cash withdrawal procedures, the fingerprint avoids errors and vulnerabilities in customer signatures. Customers might feel secure knowing that no impersonations will be used during any transactions. AES encryptions offer additional security improvements to thwart attacks and eavesdropping. Employees' OTP tokens

now include a second level of authentication to stop other employees from impersonating senior employees to commit bank fraud.

5.3 Directive for future work

Good method of authentication must always be available to use when needed. Using biometric and the OTP for verification at times may not satisfy the need to use such systems. What if the two hands got destroyed in an accident? What if the sim card used in the account registration which OTP will be sent to it is missing and due to some challenges beyond the control of the owner he can't retrieve the number, this means that customer may not be able to access his account and the finances unless the bank bypasses the verification system for that to get the needed funds for the customer. Future works must include the iris recognition as an addition to the biometric and OPT for verifying a customer.

REFERENCE

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
23. Gerald Tietaa Maale, James Ben Hayfron-Acquah, Joseph Kobina Panford. *Enhancing Security in the Banking Sector using Biometric and Cryptography. A proposed framework for BACCSOD in Ghana.* 2016