A Cancelable Biometric Based Security Protocol for Online Banking System

Article *in* International Journal of Computer Science and Information Security, · June 2020

CITATIONS
0

READS
299

3 authors:

Joshua Tom
Elizade University
6 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Boniface Kayode Alese
Federal University of Technology, Akure
173 PUBLICATIONS **566** CITATIONS
SEE PROFILE

Aderonke Thompson
Federal University of Technology, Akure
43 PUBLICATIONS **76** CITATIONS
SEE PROFILE

A Cancelable Biometric Based Security Protocol for Online Banking System

Joshua J. Tom, Boniface K. Alese, Aderonke F. Thompson

***Abstract*. The internet revolution has brought significant benefits to humanity. Undeniably, most businesses in both the public and private sectors now provide their services online through the internet. One of the businesses that have embraced the use of the internet to provide services to their customers is the banking sector. Banks obtain competitive advantage and increased productivity through the adoption of online banking. Bank customers enjoy online banking as it provides them with anytime, anywhere banking experience. Away from the benefits is the issue of security of customer transaction data and customer privacy. Many authors have proposed various solutions to address the online banking security problem but while some focus solely on client authentication, others dwell only on security of the data transfer channels. In this paper, we propose a cancellable biometric based authentication protocol which guarantees secure mutual authentication, customer privacy and offer a secure end-to-end transmission of customer transaction data. The protocol in this paper is designed using Biohashing, a biometric template protection technique and dual cryptographic algorithm that combines Advanced Encryption Standard (AES) and Data Encryption Standard algorithms. With these, we realized strong authentication and secure transaction information exchange protocol for online banking.**

Keywords: Biohashing, Biocode, online banking, cancelable biometric, strong authentication, transaction data, multifactor authentication.

I INTRODUCTION

The inconveniences caused by physical appearance at banks to carry out various banking transactions undeniably constitutes an avoidable nightmare to a majority of bank customers everywhere, the most nagging problem to customers being spending valuable man-hours in queues to pay in cash, do withdrawal, etc. With the development of information technology and internet networks, banks are able to provide services such that bank customers are no longer required to spend long hours in queues in order to carry out a simple banking. The services offered by banks are now provided online to the customers. This have attracted so much attention in recent times since online banking has helped bank operators to handle and manage the persistent long queues at banking facilities and remove the inconveniences often faced by customers. Customers can now conduct financial transactions such as transfer of money between customers in the same bank or to a different bank, checking balance, paying bills, etc. through the websites of their respective banks without need for physical appearance at a bank branch. Customers can now carry out all their banking transactions and enjoy all services provided to them by their banks from the comfort of their homes significantly improving customer bank relationship. Online banking enables a bank customer to reach his/her bank branch from anywhere, anytime, any day without restriction of location, time and condition.

This novel approach to banking is fraught with very serious requirement, customer transaction security and privacy protection. Due to the high patronage of the online banking service, there has

J. J. Tom is with the Mathematics and Computer Science Department, Elizade University, Ilara Mokin, Nigeria (e-mail: Joshua.tom@elizadeuniversity.edu.ng).
B. K. Alese, is a professor with the Department of Cyber Security Science, The Federal University of Technology, Akure, Nigeria (e-mail: bkalese@futa,edu.ng).
A. F. Thompson is with the Department of Cyber Security Science, The Federal University of Technology, Akure, Nigeria (e-mail: afthompsone@futa,edu.ng)..

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

been a corresponding increase in traffic volume on the internet attracting large number of attacks on online banking. This security need is clearly necessitated by the porous and unsecure nature of the internet due to the activities of online gladiators and hackers.

Many approaches to providing security to online banking have recently been proposed by different researchers but most of them either pay attention to authentication at the expense of a secure transaction data transfer between the client side and the bank server side while others focus mostly on protecting the transaction data with little or no attention paid to authentication. Whatever methodology is adopted aims at mitigating the threat posed by the various forms of attacks prevalent on the internet.

Attacks on online banking are divided into two main groups, online side channel attack and offline credential stealing attack. Phishing, malware, brute force attacks, credential stuffing attacks, Trojan horse, fall under offline credential stealing attacks. These attacks can only succeed where the authentication information of a user a long lifespan and probably kept on a potentially insecure device such as the user's PC. Such systems are vulnerable to phishing attacks and malicious software such as keyloggers respectively. To combat malicious software as well as phishing attacks, a strong authentication method must be used [6].

MitM attack, MitB attack, masquerading attack, session hijacking, etc. are few examples of online channel breaking attacks. They do not target users' credentials but hijack live and authenticated banking sessions already initiated by a user and manipulate transaction data. Therefore a secured online banking system protocol must address effectively these two forms of attacks.

As our contribution to solving the seemingly overwhelming online banking security problem, we propose a triple encryption cancelable biometric based online banking security protocol. We carefully analysed different options including cryptographic (encryption/decryption) technology, biometrics, authentication methods, etc. to determine what security mechanism can be selected based on their peculiar characteristics and combine in a workable security architecture to attain a more robust protocol for online banking protection. We come up with a solution that results in a protocol that provides the level of security that is required by online banking systems. This includes multifactor authentication through username, password, and one-time-password with lifetime, cancelable biometric, encryption/decryption using AES, DES, and Blowfish [16] combined in some order. These mechanisms are discussed in details in the next section to give a wider understanding of the methodology as presented in this work.

The rest of this paper is organized as follows: section 2, background study, in section 3, we discuss the building block components. Section 4 parents the proposed online banking protocol**,** section 5 is the related work section while section 6 handles conclusion and future work.

II BACKGROUND STUDY

Every technology that has been introduced often comes with its attendant benefits and bad sides. Information technology and the internet are no exceptions. The internet is a landslide phenomenon that has made distance, time and location irrelevant in communication, a characteristic that has made it an indispensable tool in the conduct of business transactions such as online banking. Because of the

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

numerous benefits of the internet in online banking including reduce costs, ubiquitous mode of services, transactions control, high throughput in less time, etc. the adoption of online banking due advanced technology has drawn malicious attention to online banking causing a plethora of sophisticated form of attacks [32].

Online banking is a banking option which provides bank customers anytime, anywhere banking services as opposed to the traditional banking approach. In online banking, customers take charge of managing their accounts anywhere and anytime using their laptops, PCs or smartphones.

As more and more banks continue to take advantage of the information superhighway, the internet to provide banking services to their teeming customers, the problem of security of customers' transaction information and privacy becomes a nightmare to the financial institutions. The security of information is an important component of bank's drive to promote and deliver banking services through the internet and at the same time protect customer confidentiality, integrity of information, and accountability. The main problem in providing online banking services to customer is the ever increasing cybercrime and how to curtail them [33]. Information security's focus is aimed at protecting the information transmitted through the network such as the internet by safeguarding three important properties of information namely confidentiality, integrity, and availability by applying appropriate security policies [30]. Therefore, the issue of bank customers' security is so critical to the continued success of online banking in the face of advancement and proliferation of attacks against online banking systems. Hence banks must integrate security of customer transactions and privacy against malicious threats as part of their services offering to the customers.

As stated earlier, online channel breaking attack launched by attackers by intercepting messages exchange between the bank customer and the banking server. For instance, the malicious user can masquerade as the server to the customer and as a customer to the banking server. Previously, IPSec and SSL could help to mitigate against channel breaking attacks [7]. But with the recent rise in the sophistication of attack vectors, channel breaking attacks are more difficult to track as it uses session hijacking, pharming, phishing and visual fraud. In addition, a secure protocol for online banking must also protect against man-in-the-browser (MiTB) attack (content manipulation form of attack which is prevalent in application layer, the second layer of the TCP/IP protocol model) and the browser redirecting the bank customer to fake websites that look exactly similar to the bank's legitimate site. Majority of the attacks on online banking are launch through the user (bank customer) as they are most vulnerable link in the online banking chain, therefore new online banking systems should be built to consider as paramount the issue of user/server authentication and the system designed in such a way that its security is independent of the online customer.

Any online banking security solution must aim to provide banking customers with robust solutions whose design have information about latest hacking techniques and implement security policies aim at protecting the online banking customer data and privacy as well as the banks themselves. This is achievable by carefully analysing and selecting the best security mechanisms and knitting them together to form well-articulated security architecture. However, if adequate attention is not paid to the very

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

details of a protocol design during implementation, a good protocol can still be vulnerable even the commonest of attacks [31].

Authentication is the primary and fundamental operation to protect a remote user's data [13]. An authentication scheme, as a first and last line of defence, implements a way for a client to be authenticated by server and the server to proof to the client that it is the authentic server. This is referred to as mutual authentication as shown in figure 1. In any authentication protocol, the client's credentials are checked against a credential database at the server side to determine whether both credentials match. The authentication credentials of users must be protected from third parties to ensure privacy of users [8].

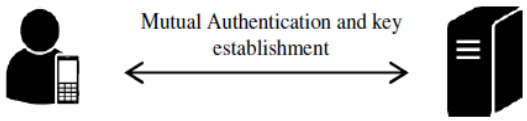


Fig. 1. Mutual Authentication Architecture [8]

Although there are several different approaches to authentication, they are either a one-factor a multi-factor authentication scheme. There are three main schemes into which authentication systems fall, namely what you know, what you have, and what you are which can be combined in a manner as required by the authentication policy.

Authentication may involve the use of a single authentication known as one factor authentication or it may require the use of two or more authentication factors referred to as two factor (2FA) or multi-factor authentication (MFA). Single-factor or one-factor authentication (SFA) is a method for identifying a user requesting access and securing access to a given system through only one category of credentials. Usernames and passwords which are vulnerable to theft, compromise through social engineering or require more entropy to mitigate or completely remove any vulnerability or predictable to guessing, brute force attacks, dictionary attacks or other common methods. Another type of authentication called multifactor authentication (MFA) uses more than one factor of authentication for verification to ascertain a legitimate transaction. The idea is to achieve multiple or layered defence and hence increased difficulty in attempt to access a computer system or network without proper authorization [29]. It is a very important component for identity and access management. In addition to username and password, MFA requires multiple credentials, example using a password, username as well as one time password (a temporary password that expires within a stipulated time frame), biometric data, security question, etc. MFA is effective providing increased security level. In this approach to authentication, if a cybercriminal compromises one credential he will be frustrated when required to present the next factor for the next level of identity verification.

The number of factors used in authentication recently increases with increase in the sophistication of criminal attack vector in order to make it more difficult for cybercriminals to compromise user data and privacy. Two-factor authentication is no longer adequate for a strong authentication system giving room for increase in factors used for the purpose of authentication to three, four or even five factors hence forcing the authentication factors to go beyond what the users know and what the user have to what the users are by way of biometric identity like a fingerprint, speech pattern, gait, iris, voice, etc.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Multi-factor authentication uses what the user knows and what the user has in conjunction with the biometric characteristics of the user.

Biometrics had previously played a very useful role in identification and recognition and recently it has been deployed in system and information security. Biometrics refers to an identification and authentication technology that involves transforming a biological, morphological or behavioural characteristic into a digital impression. Its goal is to attest to the uniqueness of a person from the measurement of an unchangeable or immeasurable part of the human body [19]. Biometrics is broadly divided into two, behavioural biometrics and physiological biometrics. Behavioural biometrics is concerned about how a person's body functions. This type of biometrics includes signature recognition, voice recognition and keystroke. Physiological biometrics is based on an individual's behavioural traits. This type of biometrics consists of eye vein, ear, finger vein, face recognition, fingerprint and gait recognition. Others include DNA matching, footprint and foot dynamics.

According to Ref. [19], the fingerprint biometric technique is the most popular biometric technique in used now. This is because no two individual's fingerprint can match. Like all the other biometrics technology, a person's fingerprint can be identified and verified with data saved beforehand. It is used in forensic investigations. The fingerprint biometric is now highly considered in online banking security. The fingerprint biometric system can be used in a variety of applications, systems and technologies for authentication and identity verification [13]. Fingerprint biometric technology is advantageous in terms of less cost of deployment, offers strong security, easy setup and is most popular biometric technique. Also its ease of operation, handling and management at users' end make its application quite attractive. In addition biometric authentication information (e.g. fingerprint biometric template) provides non-repudiation of they are non-sharable and non-transferable [2].

However, biometrics is not altogether free from malicious attacks which are peculiar to biometrics [9]. Unlike usernames, passwords, OTPs, personal identification numbers (PIN) which can be changed if compromised, the most worrisome public concern about use of any biometric for authentication is the associated privacy risks due to its static nature. The biometric data may come under attack and intercepted by an attacker who uses it to masquerade as a legitimate party in an authentication process. Biometric data also need to be secured as any breach the biometric data can result in rendering it permanently damaged and unusable [10]. This is because the moment a stored biometric data is compromised it is rendered insecure for authentication purposes for the entire life of the user [20]. A person's fingerprint can be captured from the imprints of his finger on surfaces he has touched and his fingerprint can be synthesised. This allows for the possibility of constructing artificial fingerprints [28]. There are generated artificial fingerprints as result of synthesised dummy fingers [27], and commercial software are available which can generate fingerprints [26]. Hence the biometric data should be cancelable and dynamic to make it to be cancelable, changeable or revocable at each transaction while the original biometric data is secured and unhampered.

Cancelable biometrics is a technique for biometric template protection. The other technique is called biometric cryptosystem. Cancelable biometrics is a method of intentional, systematic and repeatedly

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

distorting biometric features to secure the original template. Cancelable biometrics scheme possesses three basic properties; (1) revocability in biometrics for authentication systems, (2) security for the biometric information, and (3) verification performance improvement [5]. Cancelable biometrics also referred to as feature transformation [11].

Many feature transformation approaches have been developed in order to introduce cancelability or revocability in biometric systems among which is biohashing used in this paper. Other are cancelable biometric schemes include Cartesian, polar and functional transformations, cancelable filters, and revocable biotokens. The Biohashing algorithm is explained in the next section.

III Building Block Components

A. BioHasing Description and Algorithm

BioHashing method introduces a distortion of the biometric signal using a chosen transformation function to generate a BioCode. The distortion is achieved by means of carrying out biometric feature extraction on the biometric fingerprint template and then using a chosen transformation function to transform the fingerprint biometric data to obtain the "FingerCode". After that the FingerCode is combined with a random seed (One-Time-Password generated through a hardware token, etc.) through a hash operation to produce a "BioCode" which is then used for user authentication.

The raw fingerprint data (template) is transformed into FingerCode using a feature extraction method. BioHashing algorithm involves the transformation of the FingerCode into a binary vector (BioCode). To achieve this, the FingerCode is projected orthogonally against a random seed, in this case the OTP from the bank hardware token, to generate the BioCode.

During authentication the BioCode computed at the customer's side (now serving as a symmetric secret key) is compared with the BioCode computed at the bank side using same factors used at the customer's end. Now, a Hamming distance is calculated and quantisation against a specific threshold is determined. The FingerCode to BioCode transformation uses the algorithm in figure 2.

B. Secure Customer Transaction

The need for the security of transferred customer transaction information in any online banking solution cannot be overemphasized. Cryptography has always been the mainstay for defending the secure data transmission [25]. This need to secure the communication channels is necessitated by its vulnerability to a great number of attacks. The main task of cryptography is to defeat all forms of threats capable of jeopardizing the safety of transmitted information [16]. Cryptography uses protocols that prevent attackers from accessing data hence providing confidentiality, integrity, authentication and non-repudiation. Cryptography is of two types, asymmetric key cryptography and symmetric key cryptography. Only the latter is described in this paper. Symmetric cryptography uses same key for encryption and decryption. At the sender's end, the plaintext is encrypted with a secret key resulting in a ciphertext sent to the receiver. The receiver decrypts the ciphertext with the same secret key to recover the plaintext.

In the area of cryptography, many encryption algorithms have been published which are already in use. Ref. [12] carried out a comparative survey on symmetric key and asymmetric key algorithms. The result showed that symmetric key schemes outperformed asymmetric algorithms such as RSA in terms of speed. In addition, the memory space

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

required by symmetric algorithms was found to be lower than that required for implementing asymmetric encryption algorithms.

C. *Security and Privacy Requirements*

In online banking, the actors include the bank customer (BC), payment originating bank (POB) and payment destination bank (PDB). The customer has a username and password (or account number), an ATM card PIN, and hardware token issued by his/her bank and want to make payment transactions, check balances, etc. through the bank's website. The protocol proposed in this paper is concentrated in the enrolment and mutual authentication of the bank customer and in the secure transmission of transaction data between the customer and the bank. To ensure that we achieve the above feat, we specify requirements to provide the security and privacy which will be considered in the enrolment, authentication and transaction data movement phases of the proposed protocol. The requirements are (i.) confidential transaction data, (ii.) integrity of transmitted transaction data, (iii) authentication of customer by the bank, (iv.) authentication of bank by the customer, (v.) confidential customer information, (vi.) unlinkability of different transaction by the same customer, and (vii.) customer personal data control.

Biohashing Algorithm:
Input: FingerCode, F and seed (OTP from bank token)
Output: BioCode, B

1. For $i = 1, \ldots, m$, $m \leq n$ pseudorandom vectors v_i of length n are generated (from the random seed) and are gathered in a pseudorandom matrix.
2. generate n orthonormal vectors $V_1, \ldots, V_m$ from the m vectors V_i of the matrix using Gram-Schmidt algorithm
3. For $i = 1, \ldots, m$, compute m scalar products $pi = < F, V_i >$ using the FingerCode , F and the orthonormal vectors V_i .
4. Output the m-bit BioCode $B = (B_0, \ldots, B_m)$ is finally obtained, using the following quantization process:

$$B_i = \begin{cases} 0 & if \quad p_i < t \\ 1 & if \quad p_i \geq t \end{cases}$$

where t is a given threshold, generally equal to 0.

Fig. 2. Algorithm of the Biohashing Technique

IV. Proposed Online Banking Protocol

D. *Proposed Protocol Architecture*

The architectures of the different components of the protocol developed in this paper are given in figure 3, 4 and 5.

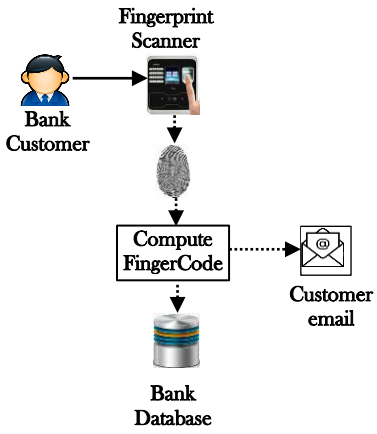


Fig.3 . Registration/Enrolment Phase of the Protocol

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

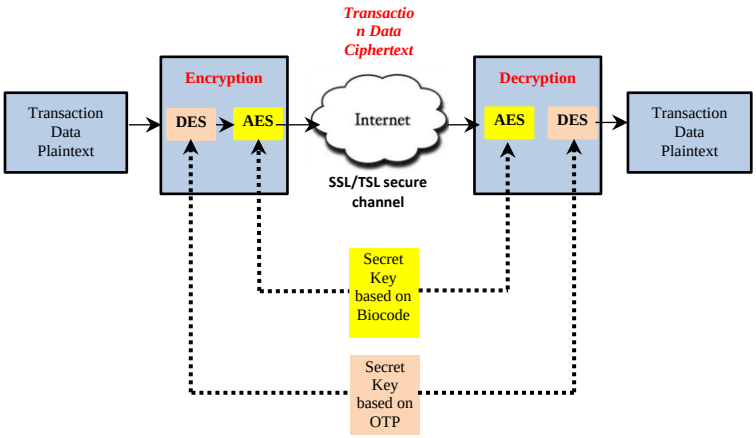


Fig.4. Transaction Data Transfer Phase of the Protocol

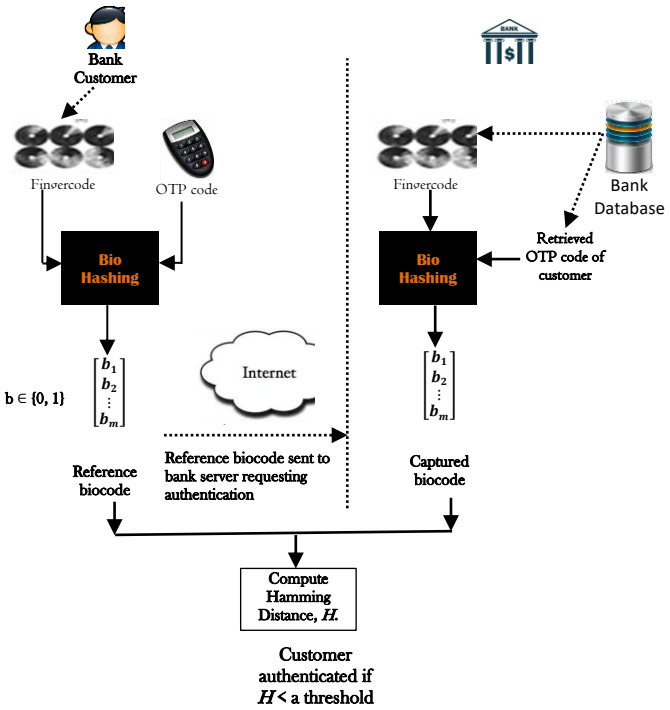


Fig.5. Authentication Phase of the Protocol

E. Methodology

The protocol proposed in this paper based on multifactor authentication and multiple encryptions is presented in this section. The protocol uses two main components, namely a technique for biometric template protection called cancellable biometric based on Biohashing scheme and triple encryption scheme based on DES, AES, and Blowfish encryption algorithms. Our protocol consists of three phases. Phase 1 is the registration/enrolment phase, phase 2 is the authentication phase and phase 3 is the transaction data transmission phase. Here is the detail of the protocol.

Registration Phase: This step is done in the bank branch at account opening stage or when the customer request for online banking service. The bank customer's fingerprint (P) is obtained using a high resolution fingerprint scanner. Feature extraction is performed with P as input using a feature extraction technique known as Gabor Filter resulting in a fingercode (F) as output. Gabor filter is used for texture analysis for the improvement of the image. The fingercode is also sent to the customer's email address and downloaded to the customer's computer to enable customer side generation of biocodes. We emphasize that the customer's original fingerprint should be destroyed immediately after registration and should not be saved anywhere either at the customer's end or at the bank's end to avoid compromise through offline credential stealing threats. In this paper, we used the FCV2002 fingerprint dataset and Python 3.8.2 to demonstrate the fingerprint feature extraction using Gabor filter given by equation 1,

$$G(x,y,f,\theta) = exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\right]\right\}\cos(2\pi f x') \quad (1)$$

where $x' = x\sin\theta + y\cos\theta$, $y' = x\cos\theta - y\sin\theta$ and σ is the width of the Gaussian envelope along x' and y' axes, f is the frequency of the sinusoidal plane along the direction θ from the x-axis and θ is the orientation of the Gabor filter.

We rotated the fingerprint image through steps of 22.5^0 to obtained 8 different orientations. This is to address the issue of the various variations which

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

might be to poor finger positioning on the fingerprint scanner. We generated a bank of 8 Gabor filters, one for each fingerprint orientation where a fingerprint in each orientation has 80 scetors. The fingercode (feature vector) $V_{i\theta}$ is computed as given in equation 2,

$$V_{i\theta} = \left(\frac{1}{n_i}\right)\left(\sum_{1}^{n_i} |F_{i\theta}(x,y) - F_{i\theta}|\right) \quad (2)$$

where n_i is the number of pixels in S_i and $P_{i\theta}$ is the mean of pixel values $P_{i\theta}$ of $P_{i\theta}$(x, y) in sector S_i.

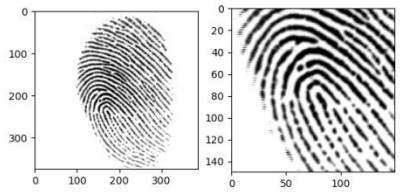


Fig.6a. fingerprint reference point

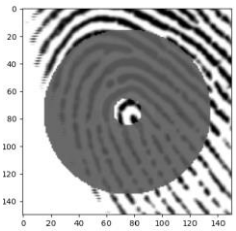


Fig.6b. region of interest divided into sectors

Fig.6c. One of the 8 Gabor filters

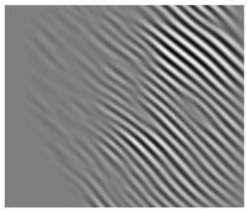


Fig.6d. Gabor filter applied to fingerprint image for enhancement

Authentication Phase: The bank customer request online banking service from his/her bank by computing a biocode using the OTP code from the hardware token and the fingercode sent to his/her email address. Once the biocode is computed, it is sent to the bank server together with other input e.g. account number, and secret password or PIN. This communication is done through the SSL/TSL secure connection. At the bank side, the bank server uses the customer account number, pull out the customer's fingercode from its database and compute the captured biocode. The computation of the biocodes at both ends use the same mathematical model. The computation proceeded as follows; first we coded an OTP generator module using python to generate a OTP value as seed to the PRNG and generated a matrix of 80x8 pseudorandom numbers,. Next, we compute the projection of vector vk onto vector uk using the Gram-Schmidt algorithm to orthogonalize and orthonormalize the vector respectively with,

$$u_k = v_k - \sum_{j=1}^{k-1} \text{proj}_{u_j}(v_k) \quad (3)$$

$$e_k = \frac{u_k}{\|u_k\|} \quad (4)$$

where $\mathbf{u}_k$ is the required system of orthogonal vectors, and the normalized vectors $\mathbf{e}_k$ form an orthonormal set and $\mathbf{v}_k$ is the set of pseudorandom numbers. After

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

that we compute the scalar (dot) product of fingercode, F and the orthonormal vectors, $\mathbf{e}_k$ as

$$\langle \mathrm{F} \cdot \mathbf{e}_k \rangle = \sum_{i=1}^{k} F \cdot \mathbf{e}_k \qquad (5)$$

Finally, we obtained the desired biocode by applying the following quantization model to the output from the scalar product calculation,

$$B_i = \begin{cases} 0 & if \quad p_i < t \\ 1 & if \quad p_i \geq t \end{cases} \qquad (6)$$

After computation of the capture biocode at the server side, the server compares reference biocode

```
>>>
= RESTART: C:\Python38\GaborFilterPython\fingercode_python\fingercode-master\finger.py
this database already exists.....
2/101_1.tif
success
167 233
------
[95, 93, 88, 85, 109, 89, 116, 121, 121, 107, 115, 111, 114, 103, 103, 105, 59, 45, 44, 45, 70, 73, 75, 89, 71, 90, 93, 91, 91, 93, 86, 55, 71, 57, 55, 56, 55,
71, 96, 103, 102, 100, 96, 93, 86, 84, 75, 72, 50, 36, 35, 36, 37, 54, 97, 100, 96, 82, 80, 82, 53, 61, 53, 43, 104, 103, 107, 102, 99, 99, 117, 118, 117, 118,
114, 113, 106, 108, 107, 114]
------
------
-
-
-
------
------
[122, 117, 114, 117, 102, 99, 116, 124, 121, 120, 121, 120, 123, 122, 120, 122, 113, 106, 98, 88, 85, 97, 88, 105, 101, 110, 114, 117, 117, 114, 103, 110,
112, 109, 102, 92, 85, 84, 88, 105, 109, 113, 113, 115, 114, 110, 111, 108, 113, 111, 106, 102, 96, 95, 96, 105, 106, 106, 114, 116, 115, 116, 113, 115, 118,
117, 110, 111, 105, 97, 100, 106, 119, 117, 115, 119, 120, 120, 121, 118]
------
start saving the result....
execute.....
commit....
close...
```

Fig.7. A fingercode generation output using Python

with the capture biocode for a possible match by computing the hamming distance between the Finger Codes. Customer authentication is successful if this value is lower than a specified threshold set by the bank. The bank server then sends the OTP value generated and used by the customer for computing the reference biocode to authentication itself to the bank customer as the authentic server.

Transaction Data Transmission Phase: Most of the works done in the area of online banking security are focus primarily on user authentication with little attention paid to the security of user transaction information. In this paper, we address the security of user trsnsmitted information. After successful mutal authentication, all transaction information are sent encrypted using symmetric cryptosystem approach and proceeds as follows.

1. The bank customer generates a fresh OTP and computes a new biocode
2. Generate a secret key using the OTP as a seed
3. Encrypt transaction data with AES encryption algorithm with the OTP based secret key
4. Encrypt the AES ciphertext with DES encryption algorithm using the biocode as a secret key
5. The DES ciphertext is sent to the bank server

At the server side,

1. After receiving message from the bank customer, the bank server fetches the OTP

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

used by the customer and generate a biocode associated with the OTP

2. It then generates a secret key and biocode using the OTP which are same as those generated by the customer
3. Decrypt the DES ciphrtext with the biocode as the secret key using DES decryption algorithm to recover the AES ciphertext
4. Using AES decryption algorithm, decrypt the AES ciphertext with the OTP as the secret key to obtain the plaintext

We implementwd the AES algorithm and the DES algorithm with Python and then combined the two algorithm into one algorithm to provide a stronger level of security for the protection of customer transaction data in online banking. The three algorithms were execution for 4 times with differenct data sizes as shown in Table I. We compared the executuion time of the two algorithm with the combined algorithm used in this paper and found that the extra time difference AES and our combined DES-AES algorithm can be traded for security.

TABLE I
EXECUTION TIMES OF DES, AES, AND PROPOSED COMBINED DES-AES

s/n	file size	aes	des	Combined DES-AES
1	549bytes	0.12479	0.32758	0.54601
2	1.07kb	0.26520	0.60838	0.92041
3	1.6kb	0.37440	0.81118	1.07641
4	2.14kb	0.51479	1.15440	1.62241

F. Security and Privacy Analysis

The proposed protocol ensures secure mutual authentication of the actors in the protocol protecting against an attacker masquerading as either the bank customer or as the bank server since the attacker cannot have the all the parameters used to obtain a valid biocode of the customer such as the OTP from the hardware token and the customer fingercode. The dynamic nature of the biocode and the one-time-password does not allow any replay attack to prosper and MitM attack and MitB attack are also frustrated as the OTP secret is never transmitted online but either generate fron hardware token or send through the GSM channel to the customer's phone. The biocode has the property of being non-invertible so intercepting the biocode cannot lead to recovery of fingercode from it. This is provided by the strong authentication of the biohashing scheme. By the use of the biocode in the encryption and decryption schemes during transfer of transaction information, confidentiality of the customer information and the transaction data are assured.

In our scheme, there is no online key exchange; all secret keys are side-generated by each party in the protocol and are dynamic, hence third parties have no access. Even if the fingercode of the customer is stolen or compromised, it is useless to the attacker since the attacker cannot generate a valid biocode without a valid OTP hence the protocol is secure against offline credential stealing attack through malware. The double encryption known as DesAes in this paper provides robust security to transmitted transaction data. The keys used for encryption and decryption are not static but dynamic and updatable where a different key is used at different stage of the DES-AES algorithm.

These algorithm together increase the level of security multiple times ensuring end-to-end security of transmitted transaction data. Our experiment shows that combining AES and DES in this paper does not have any significant increase in time complexity of the solution. Different transactions of the same customer cannot be linked since the generated biocodes and OTPs have lifetime within which they are active, hence different biocodes and OTPs are used for different transactions. This

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

guarantees customer privacy and unlinkability requirement of the protocol in this paper.

V. Related Work

Many researchers have addressed the online banking security problem. This arises from the proliferation of attacks on online banking occasioned by the services provided by most banks offering convenience to bank customers through online banking.

Ref. [24] proposed a cancelable user authentication system for Internet of Things (IoT) using iris biometric and steganography technique. Their objective was to provide user authentication and security of the iris data. The security of their scheme was based on hiding the secret key. The work introduced dynamic keys as seed to the cancelable biometric scheme to solve the problem of using a user-specific key for feature transformation and hide the user specific keys using steganography to enhance system security. However, their scheme cannot entirely be adopted for online banking without modifications since it addresses only user authentication.

Ref. [23] carried out a formal classification of attacks and vulnerabilities that affect online baking systems. From their analysis of current security models, the paper registers its contribution by proposing guidelines for designing secure internet banking systems that resistant to the analysed attacks. They presented attack modelling and described efficient attacks against currently used security solutions. The paper takes a critical look at different current banking security models and expounds on their vulnerabilities and suggested some countermeasures.

Due to rising concerns against use of biometric with regards to lack of secure storage and misuse of biometric data, Ref. [22] carried out a survey on biometric cryptosystems and cancellable biometrics which are two schemes of biometric template protection. In their work, they reviewed state-of-the-art approaches together with the operation modes of each approach which enable them to make in-depth discussions and give future prospects of the approaches reviewed. Among the approaches reviewed in their paper which we have particular interest are password hardening [1] and biohashing [2].

Ref [3] carried out a review on and analysis of different existing methods of biometric based authentication system and cancelable biometric systems from where they proposed a secure method for cancelable biometrics that employed a non-invertible function based on Discrete Cosine Transformation and Huffman encoding. The result of their work showed that cancelable biometrics has the potential to improve the security and confidentiality of a traditional biometric system though cancelable biometric systems are yet to receive the level of real life implementation in comparison their traditional counterparts.

Ref. [21] cryptanalyzed two cancelable biometric schemes namely Gaussian Random Projection (GRP) and Uniformly Random Permutation (URP) based on index-of-max. In the paper, the authors proposed several attacks against GRP and URP. Their results showed that both schemes were prone to authentication and linkability attacks. As a contribution, they proposed a better reversibility attack against GRP-IoM using linear and geometric programming methods though not yet practical.

Ref. [4] proposed a PIN-based cancelable biometrics applied to fingerprint with an additional random value (e.g. a PIN code or a password). Their

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

scheme achieved 0-EER and templates diversity. The authors adopted a minutiae-based extraction procedure, using Gabor filters in their experiment on the public-domain FCV2002 dataset. They claimed that the resulting biohashing system is secure since the PIN is considered to be known only by the user. This claim is however not true because the PIN can be compromised through social engineering and once that is done the PIN can be used to reverse the hashcode to recover the original fingerprint template. Secondly, traditional passwords and PINs can be illegally acquired by direct observation.

Jin et al. (2004) did a similar work to that proposed in [4] which is very interesting. The paper proposed an authentication system that combined a tokenised pseudo-random number with a fingerprint feature through an iterated inner products using wavelet and Fourier–Mellin transform. The posited that getting the user specific code was nondeterministic because of its dependence on both the tokenized random data and user fingerprint extracted feature hence protecting the user and the system for instance against biometric fabrication.

Ref. [20] made a study of cancelable biometric techniques with the aim to address the problem of possible permanent compromise of biometric template. The authors proposed a correlation-invariant random filtering (CIRF) with provable security. Their objective was to construct a method that could generate cancelable fingerprint templates based on the chip matching algorithm and the CIRF. They proved that CIRF have perfect secrecy because there is no information leakage of the original feature through the biohash.

Ref. [19] proposed a revocable multi-biometric scheme to secured multi biometric data with the main objective to present the BioHashing technique as practical solution for biometric data protection and try to study the impact of this technique on multi biometric data. The authors focused attention on BioHashing method which is a recent technique that can address simultaneously the invasion of privacy issue and the security. They introduced an improvement in the level of characteristics to obtain very satisfactory results. It combines fingerprint multi sensor features of a single human finger. Their motivation was sparked by the benefits of multimodality to unimodal biometric systems achieved by fusion of several biometric systems. The main contribution of the paper is to put the main weaknesses related to biometrics and address the methods of protection of the biometric model and then focus on the protection of multi-biometric data.

Ref. [18] proposed an encryption protocol for secure transmission the SMS from one mobile user to other using the Blowfish encryption algorithm. Their objection was to achieve the cryptographic goals including confidentiality, authentication and integrity of the messages. The scheme in their paper provided security to the message making different from the traditional messaging schemes.

Ref. [17] analysed and compared some well-known cryptographic algorithms AES, DES, RSA, Blowfish are and evaluated their performances to demonstrate the basic differences between the existing encryption techniques. The result of their analysis showed that Blowfish was preferable than AES for better performance with respect to average time. They also described and compared Byte – Rotation Encryption Algorithm (BREA) with those above.

Ref. [16] proposed a method of using both cryptography and steganography techniques. With cryptography they performed three levels of encryption using AES, DES and Blowfish algorithms

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

and with steganography, the authors used the LSB, DWT and DCT techniques to embed the data file in audio, video and the image respectively and before transmitting the secure data to towards its destination. Ref. [15] proposed a three-level security, multi-factor authentication based internet banking system using a combination of a dongle, Kerberos authentication system, AES for encryption and decryption and biometric identification. In the paper, the Kerberos system provided authentication of the client process (user) to prove its identity to a verifier, the application server, and hence the transmission of data across the unsecure link is avoided. AES provided an improve level of security. Ref. [14] proposed a security model for online banking at the client side, data transfer stage and the bank server side to combat identity theft and fishing. To achieve the level of security required in their model, the authors employed the use of dongle, fingerprint biometric in addition to the use of password and username at the client side. They used advanced encryption to provide a strong security for the sensitive transaction data. However, the protocol developed in their paper could be vulnerable to offline credential stealing attacks as the username and password can be stolen. Secondly, the biometric data of the client can easily be compromised and once that happens, the fingerprint of the client is rendered unusable for the rest of the client life. Ref. [12] presented a multi-factor authentication scheme using biometric fingerprint as a key parameter for online banking systems. The remote authentication scheme in their work made use of elliptic curve cryptosystem for public key encryption and decryption. The proposed approach in the paper not only helps to protect the user sensitive data from the malicious use and also preserves the security and privacy of the user credentials and access keys from the cloud insiders and outsiders.

VI. Conclusion/Future Work

There is no gain stressing the merits of online banking as it has become almost indispensable in conducting most business transactions. Nevertheless, the number of attacks and threats against online banking leaves it a nightmare because of the huge financial loss suffered by banks and customers alike. A secure mutual authentication online banking protocol offering both customer privacy and security of customer transaction inform has been proposed in this paper. We employed the use of biohashing, a cancelable biometric template protection technique to protect the customer fingerprint biometric for a stronger authentication. In addition, our protocol combines the DES and AES cryptographic algorithms into one algorithm to achieve a strong level of security for the protection of customer transaction data.

The benefits of the proposed protocol is that (1) it does not make additional requirement on the bank and the customer in terms of hardware apart from those in use already (2) the cryptographic keys used during transfer of customer sensitive data are dynamic, nondeterministic and safe, hence cannot be compromised by malwares like Trojan, keyloggers, etc. Also, online side channel attack like MitM attack and MitB attack cannot be successful because the keys are never transmitted by the parties involved in online banking protocol (3) there transparency in the authentication process due to the use of the customer fingerprint based information hence no third party can masquerade as the customer or the bank.

The problem with this protocol is increased complexity as a result of the processes involved in computing the biocode which is renewed as a new

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

transaction is initiated. But increase in the level of security of the online banking system is more important as it leads to increased customer safety while carrying out banking transactions online and increased customer trust for the bank and at the long run promote the corporate image of the bank.

In the future, the cancelable biometric template protection technique used in this paper, biohashing protocol can be optimized to reduce the time complexity of biohashing algorithm implementation to make the proposed protocol suitable for resource-constrained devices such as smartphones in case of mobile bank customers.

REFERENCES

[1] F. Monrose, M. K. Reiter, S. Wetzel "Password hardening based on keystroke dynamics." Proceedings of 6th ACM Conference on Computer and Communications Security, CCCS, 1999, pg. 73-82.

[2] A. T. B. Jin, D. C. L. Ngo, and A. Goh "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." Pattern Recognition, 2004, 37:2245-2255.

[3] B. Choudhury, P. Then, B. Isaac, V. Raman, M. K. Haldar "A Survey on Biometrics and Cancelable Biometrics Systems." International Journal of Image and Graphics, vol. 18, issue 1, 2018, pp. 1850006, ISSN 0219-4678.

[4] P. Lacharme, and A. Plateaux "PIN-based cancelable biometrics." International Journal of Automated Identification Technology (IJAIT), vol 3 issue 2, 2011, pp.75-79, hal-00984027.

[5] S. G. Kanade, D. Petrovska-Delacrétaz, B. Dorizzi, "Cancelable biometrics for better security and privacy in biometric systems." ACC 2011: 1st International Conference on Advances in Computing and Communications, Kochi, India, 2011, pp. 20 - 34, 10.1007/978-3-642-22720-2_3, hal-01302046.

[6] A. Hiltgen, T. Kramp, T. Weigold "Secure internet banking authentication." IEEE Security and Privacy, vol. 4, 2006, pp. 21–29.

[7] N. Doraswamy, D. Harkins, "IPSec: the new security standard for the Internet, intranets, and virtual private networks." Prentice Hall, 2003.

[8] J. J. Tom, B. K. Alese, O. S. Adewale, O. S. and A. F. Thompson "Efficient Anonymous Key Exchange Protocol for Roaming in Wireless Networks." International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882. Vol.7, Issue 2, 2018, pp. 66-73.

[9] R. M. Bolle, J. H. Connel, Connel, N. K. Connel, "Biometric perils and patches." Pattern Recognition vol. 35, 2002, pp. 2727–2738.

[10] R. Ang,, R. Safavi-Naini, and L. F. McAven, "Cancelable key-based fingerprint templates." In C. Boyd & J. Gonzalez Nieto (Eds.), Australasian Conference on Information Security and Privacy, 2005, pp. 242-252. Germany: Springer.

[11] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle "Generating cancelable fingerprint templates." IEEE Trans. Pattern. Anal. Mach. Intell., vol.29, no.4, 2007, pp.561–572.

[12] M. Agrawal "A Comparative Survey on Symmetric Key Encryption Techniques." International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05, 2012, pg. 877-882

[13] S. Nagaraju, and L. Parthiban "A Secure Authentication and Authorization Scheme for Online Banking Systems in Cloud." International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.76, 2015, pp. 484-490

[14] N. A. Sharaaf, M. N. Haamid, S. S. Samarawickrama, C. N. Gunawardhane, K. R. Kuragala, Dhishan Dhammearatchi "Improved E- Banking System with Advanced Encryption Standards and Security Models." International Journal of Scientific & Technology Research, Vol. 5, Issue 10, 2016, pg.22-27.

[15] E. R. Nwogu, "Improving the security of the Internet Banking System Using Three-Level Security Implementation." International Journal of Computer Science and Information Technology and Security, vol. 04, no. 06, 2014, pp. 1-1.

[16] P. K. Singh, P. Tripathi, R. Kumar, D. Kumar "Secure Data Transmission." International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 04 | Apr -2017, ISSN: 2395-0072 pg. 217-222.

[17] M. E. VekariyaMeghna "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms." International Journal of Computer Engineering and Science, 2014, pp. 1-8.

[18] M. Thomas, V. Panchami "An Encryption Protocol for End-to-end Secure Transmission of SMS." International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015

[19] F. Bedad and R. Adjoudj "Secured Multimodal Biometric System." Journal of Multimedia Processing and Technologies, vol. 9, issue no 3. 2018.

[20] K. Takahashi, S. Hirata "Cancelable Biometrics with Provable Security and Its Application to Fingerprint Verification." IEICE TRANS. FUNDAMENTALS, VOL.E94–A, NO.1. 2011, pg. 233 244.

[21] K. Atighehchi, L. Ghammamy, K. Karabinaz, and P. Lacharme "A Cryptanalysis of Two Cancelable Biometric Schemes based on Index-of-Max Hashing." 2019. arXiv:1910.01389v3 [cs.CR]

[22] C. Rathgeb and A. Uhl "A survey on biometric cryptosystems and cancelable biometrics." EURASIP Journal on Information Security, 2011.

[23] L. Peotta, M. D. Holtz, B. M. David, F. G. Deus, R. Timóteo de Sousa "A Formal Classification of Internet Banking Attacks and Vulnerabilities." International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1, 2011, pp. 186-197.

[24] W. Yang, S. Wang, J. Hu, A. Ibrahim, G. Zheng, M. J. Macedo, M. N. Johnstone, and C. Valli, "A Cancelable Iris- and Steganography-Based User Authentication System for the Internet of Things." Sensors 19, no. 13, 2019, pp. 2985.

[25] M. K. S. V. Shrivastav "An Effective Approach to Information Hiding for Secure Message Transmission." International Journal of Computer Trends and Technology, 2013.

[26] D. Maltoni, D. Maio A. K. Jain, S. Prabhakar "Handbook of Fingerprint Recognition." Springer, New York, 2003.

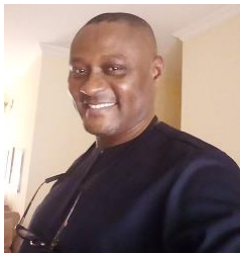
[27] J. L. Araque, M. Baena, B. E. Chalela, D. Navarro, P. R. Vizcaya, "Synthesis of fingerprint images." In: Proc. 16th International Conference on Pattern Recognition. 2002, 422–425.

[28] C. Hill "Risk of masquerade arising from the storage of biometrics." Master's thesis, Australian National University, 2001.

[29] T. S. Mohamed "Security of Multifactor Authentication Model to Improve Authentication Systems." Information and Knowledge Management. ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol.4, No.6, 2014, pp. 81-86.

[30] L. A. Gordon, M. P. Loeb "The Economics of Information Security Investment." ACM Transactions on Information and System Security, Vol. 5, No. 4, 2002, pp. 438–457.
[31] O. Delgado, A. F´uster-Sabater, and J. M. Sierra "Analysis of new threats to online banking authentication schemes." ACTAS DE LA X RECSI, SALAMANCA, 2008.
[32] B. K. Alese, A. F. Thompson, O. D. Alowolodu, B. Oladele "Multilevel Authentication System for Stemming Crime in Online Banking." Interdisciplinary Journal of Knowledge, Information, and Management, 2018, pp. 79-94.
[39] I. A. Sheikh, P. Rajmohan "Internet Banking, Security Models and Weakness." International Journal of Research in Management & Business Studies, Vol. 2 Issue 4, 2015, pp. 17-22.

AUTHORS' BIOGRAPHIES



Joshua J. Tom received his Ph.D. degree in Computer Science from Federal University of Technology, Akure, Nigeria in 2018. He received M.Tech. degree in Computer Science from Federal University of Technology, Akure, Nigeria in 2012, and his B.Sc. degree in Computer Science from University of Uyo, Uyo, Nigeria in 1997. He is currently a research fellow and lecturer in the Department of Mathematics and Computer Science, Faculty of Basic and Applied Sciences of Elizade University, Ilara-Mokin, Nigeria. His current research interests are information and cyber security, cryptography, artificial intelligence, security of cyber-physical systems, internet of things, and software engineering.

Boniface Kayode Alese is a professor of Information and Cyber Security. He obtained his Ph.D. Computer Science 2004, M.Tech Computer Science. 2000 and B.Tech (Ind. Mathematics) 1997 and currently works at the Department of Cyber Security, The Federal University of Technology, Akure. Boniface does research in Information and Cyber Security, Computer Communications (Networks), Quantum Computing and Fault Tolerant Computing.

Aderonke Thompson is the Head of Cybersecurity Sciences Department, Federal University of Technology, Akure (FUTA) Nigeria. She holds a Bachelor of Technology (B.Tech) in Computer Engineering in 1998 from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, Master of Technology in Computer Science in 2005 from the Federal University of Technology, Akure, Nigeria and Ph.D. in Computer Science in 2014 from the same University. Her research interest includes Computer and Network Security, Cybersecurity, Biometrics, Algorithms, Machine Learning.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500