Fraud Detection System using Multi-tiered Authentication Scheme

Soyemi, J.[1] & Hammed M.[2]

[1, 2]Department of Computer Science, The Federal Polytechnic, Ilaro

[1]Jumoke.soyemi@federapolyilaro.edu.ng; [2]mudasiru.hammed@federalpolyilaro.edu.ng

Abstract

The importance of authentication for all online bank transactions cannot be over-emphasized especially in this present age of technological advancement where internet frauds are all over. Online transactions are prone to attack when done with single- or two-ways authentication schemes. Ensuring a strong level of security has to do with a combination of attributes, encryption and authentication channels and credential storage. Although, several types of research were carried out on authentication and security level for web-based transactions, however, few researches have investigated multiple authentication schemes that combine securely and efficiently attribute asynchronously. This study enhanced the expansion of one-tier and two-tier authentication scheme that combines three levels of authentication, which include PIN, one-time password (OTP), a notification from email and graphical password for a web-based banking operation. Multi-tiered authentication scheme makes access to unauthorized banking operation difficult for an adversary. The system attained a high degree of accuracy when tested because adversaries were unable to break the three levels of authentication.

Keywords: Online Banking, Fraud Detection, Security, Multi-tiered Authentication Scheme

1.0 Introduction

A financial application that allows users to carry out transactions from a web-based bank application to the original bank account demands that the user provides entities that mainly identify them and can be declared against already existing objects held by a trusted third party. In multi-factor authentication (MFA), authentication is done by presenting pieces of attributes as evidence using the following categories: knowledge (what the user knows); possession (what the user has), and inherence (what the user is).

The interest in web-based banking services has dramatically increased in recent times. However, the underlying security issues of this type of services is a source of concern because attackers and fraudsters are attracted to whatever has to do with money. The service is also prone to money laundering and illegal funding. It is also vital that web-based banking services are guided by the financial policy established within the country where the services are resident (Achemical, Gharout, & Gaber, 2011).

Most web-based banking systems rely on the use of PIN and Passwords to authenticate a user's identity. These passwords are subject to challenges of management and security. Sometimes, for some users to remember their password easily, they may use an elementary password that can be guessed. In contrast, some others duplicate the same password for different accounts, and some others keep their passwords on devices and some store them on papers. Such passwords and pins can be seen by shoulder surfing, snooping, sniffing, hacking and even guessing (Aloul, Zahidi & El-Hajj, 2009).

Multi-factor authentication for web-based banking systems can employ the user's email address to represent "something that the user possesses"; a PIN to represent "something the user knows" a graphical password and a random one-time password (OTP) for an extra layer of security. "The one-time password is normally a randomly generated alphanumeric or numeric code that is sent to the user's mobile device in the form of an SMS". (Ombiro, 2016). This is made simple because most people have their mobile devices handy with them most of the time to receive the OTP. Nevertheless, the combination of one or more properties for authentication purposes is the strength of a multi-factor authentication system.

This study implemented a fraud detection system using a multi-factor authentication scheme for a web-based banking operation.

2.0 Review of Related Studies

Authentication can be achieved by using what a customer has (Email address) and what they know (PIN). According to Adeoye (2012), research has found out that online banking infrastructure and mobile banking trends show that multi-factor authentication is better than single-factor authentication. The study recommended that a customer's education would be used to educate the user on skimming techniques. That bank provider should not provide liability against PIN credit and debit card losses. The study fails to show how the implementation can be done to increase the security of online banking.

Corella & Lewison (2012) outlined the use of multiple factors for authentication of a web application. In this setup, the online form on the application website will have credentials that are generated during the initial opening of the application. The data set for the credentials is a device handle and a key pair to a public-key cryptosystem. The user suggests the use of RSA in this set up for cryptography. This approach requires improvements to the operating system of the device the user is making use of to allow a single native application to be used securely within the environment not bothering about other non-trusted applications within the device.

Mohamed (2014), proposed a multi-factor authentication system that makes use of a password for login as opposed to using PIN or pattern because in shoulder surfing attack password is safer.

The proposal in the study did not address the convenience and security loopholes that may be created by using the graphical image password for authentication

Antal & Szabo (2015), researched the touchscreen-based swipe patterns for biometric authentication. The study investigated user authentication on mobile devices with touch behaviour and micro-movements of user-created a pattern on a mobile device. The study showed that using sequences of 5 swipe improved the Equal error rate **(**EER) by 0.2%. Although the study did not implement web-based multi-factor authentication, the study showed that single swipes alone with EER values of 0.05 were not enough to permit implementation of an authentication procedure. However, using five consecutive swipes in this procedure increases EER. The research did not consider any other authentication scheme that can be combined with the biometric method.

Sarhan, Hafez & Safwat (2015), considered applications that run on smartphones and communicates with remote service providers to check bank accounts or make some transactions remotely. The study uses two authentication schemes: "two user-chosen passwords (one is known to a bank representative, and the other is anonymous) and bank generated OTP. This approach is two-factor authentication and does not explore the use of biometrics as well as relies on what the user knows and not the other factors like what the user has or is".

Voice Pitch Based Authentication for Android Application was carried out by Jadhav, Shirsat, Bhargude & Kamble (2016). The study proposed triggering an authentication based on a keyword that depends on the speaker recognition power of the devices in use. The research used two methods, "a template-based method and a hidden Markov model (HMM) based method".

Faisal & Garba (2017) proposed an application that uses mobile banking model for Nigeria. The model adopted Bank Verification Number (BVN) policy of the Central Bank which has three levels of authentication: what the user knows (BVN), what the user has (mobile phone's Media Access Control (MAC) and what the user is (fingerprints and finger vein multimodal biometric data).

Shinkar, Sonje, Kamble, Pardeshi, & Dhule (2018), employed QR code validation as a protective approach that uses two-way authentication of passwords and mobile phones. The target of this study was to establish the validation technique with two-factor authentication using mobile devices such as phones to print the QR code and also serve as a user-sign and password.

Prasanalakhmi & Ganesshkumar (2019) noted that there are drawbacks to most -banking authentication scheme that exist used SSL, OTP generation to the mobile phone or email id. The study tried to overcome the drawbacks by using multiple biometric entities to authenticate using three biometric traits.

The reviewed studies above bring to fore the need for multi-factor authentication using more than two attributes (What the user knows, what the user has, and what the user is) in online banking solutions. Although some works have been done on multi-tiered authentication system using several attributes, such research, however, failed to have a mix of attributes that utilizes a combination of common authentication methods, unique mobile device attributes, and email notification messages to enhance online banking solutions security. Most of the studies used finger and iris biometrics. The use of voice biometrics has not been used in the literature review in combination with other authentication methods.

3.0 System Design

The system consists of two phases which include the registration phase and the login phase

Registration Phase

Every user that wants to use the system must first register with his/her details which include: Name, sex, age, address, email address, phone number and user needs to select some familiar images as part of registration. All these information were stored in the system database, and a Personal Identification Number (PIN) is generated which will be sent to such user for subsequent login access to the system.

Login Phase

In the login phase, the web-based application was designed with the following authentication components.

PIN

The system asks the user to use a numeric password. The chosen password must be four characters long, and three similar numbers must not be present. The maximum number of times a PIN will be entered is twice. If an incorrect PIN is entered thrice, the user has the option of using an OTP and OOBA with a graphical password for resetting the PIN.

One Time Password (OTP)

The application generates a random one-time password. The password is composed of alphanumerical characters and expires after a particular time. A second alternate (OTP) is sent over email as an alternate communication channel (out of band communication) for security purposes. The user is asked to enter the password on the web interface manually. The system validates.

Graphical Password

A graphical password is generated, and the user must remember the combination of images being used for the password. The graphical password is used to authenticate the transaction at the background when the right combination of images is given. Where the user authentication fails based on the other two authentication methods above, the graphical password would be used. After the authentication of the graphical interface, the OTP is then sent to an email for the user and accessing it will authenticate the user and allow the creation of a new PIN.

The user of the web-based banking application enters the PIN on the web application interface to initiate the connection to the webserver application. At the webserver, the PIN is authenticated and validated against the minimum requirements. The application can be configured to allow both web OTP authentication and a message sent to the user's email address for the OTP for authentication to make the OOB authentication more secure. On authentication of the OTP, the user gains access to the web-based banking application payment platform on their device to carry out any web-based banking transaction.

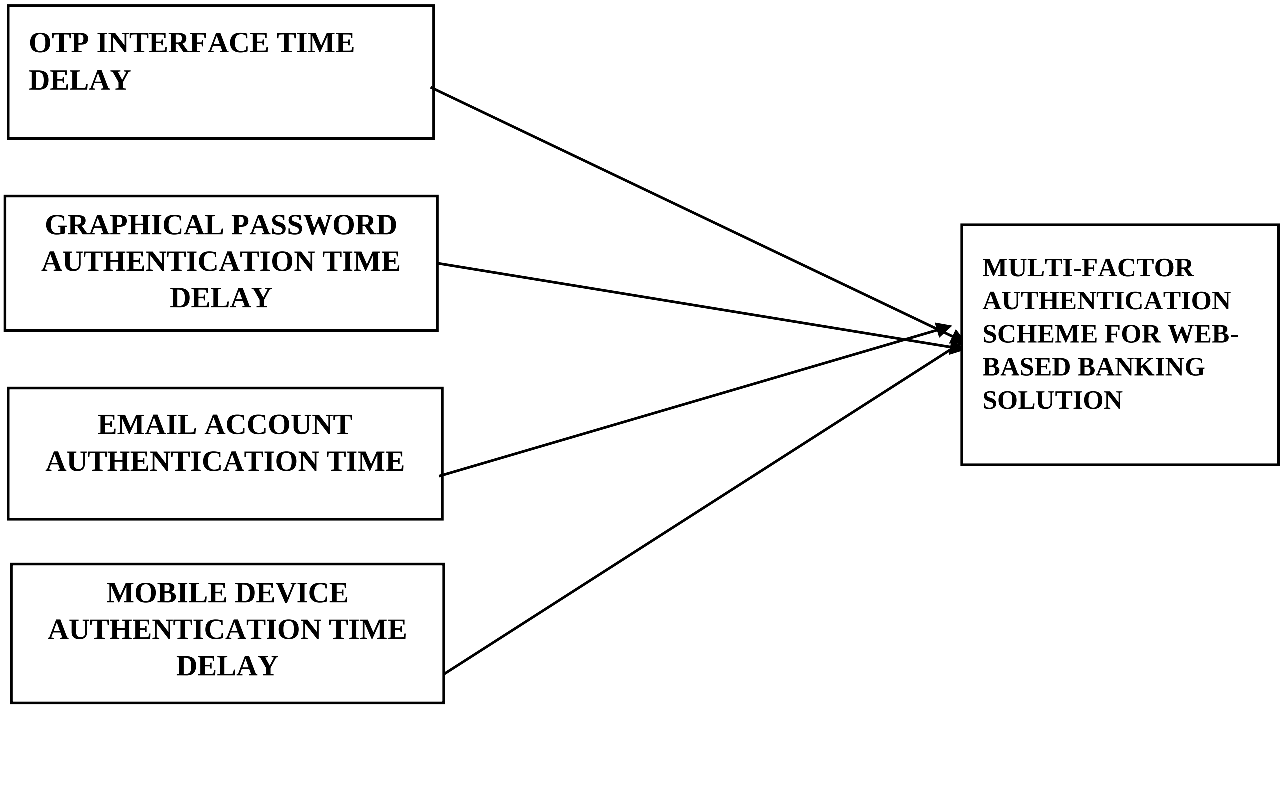

OTP INTERFACE TIME DELAY
GRAPHICAL PASSWORD AUTHENTICATION TIME DELAY
EMAIL ACCOUNT AUTHENTICATION TIME
MOBILE DEVICE AUTHENTICATION TIME DELAY
MULTI-FACTOR AUTHENTICATION SCHEME FOR WEB-BASED BANKING SOLUTION

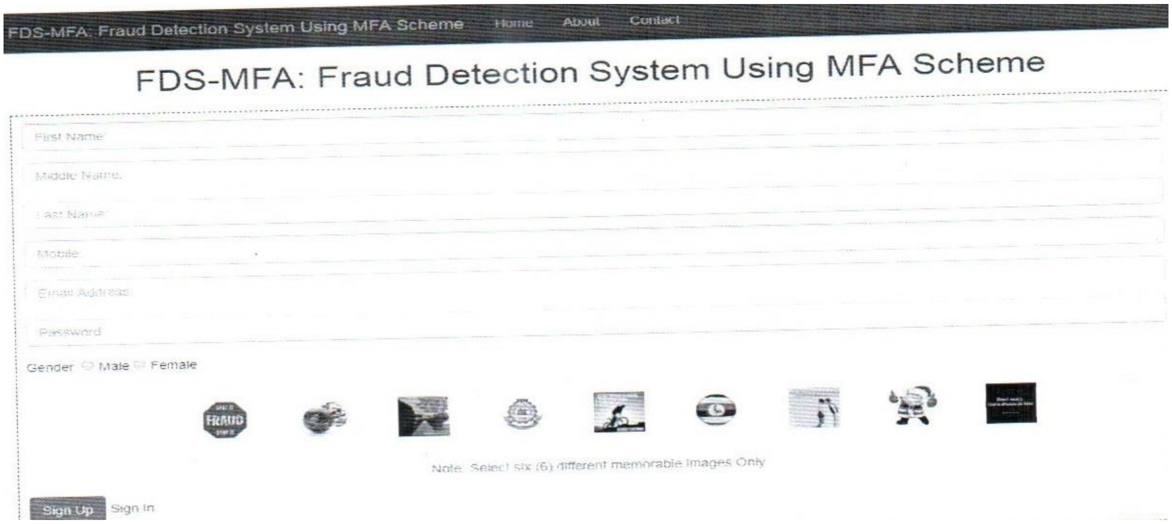
Figure 1: Conceptual framework representation

4.0 System Implementation

The software Integrated Development Environment (IDE) used include sublime Text 3, IntelliJ IDEA 2016.2.2. For Databases Relational Database Management System (RDBMS), SQLite database and MYSQL database version 5++ were used. JAVA 8, PHP and JSON were the programming languages used. The software Integrated Development Environment (IDE) used include sublime Text 3, IntelliJ IDEA 2016.2.2. The software was designed to be able to rectify any fraudulent activity on any user account and also inform users by sending notifications if the security is being breached or tampered with.

The developed system is a web-based fraud detection application that detects fraud of a third party using a multi-factor authentication scheme for the banking operations to decrease the rate of fraudulent activities being carried out online. This system provides security for users wherever they are with the assurance that their account cannot be accessed without their consent. The fraud detection process involves the use of user email and passwords, user phone number, graphical password and an OTP.

Figure 2 is the registration page, and it is the first stage and step to be carried out by the user before the login page would be launched. For a user to register, there is the need to fill in the registration content correctly, provide a PIN that would be easily remembered by the user, pick-six graphical image password that can be remembered easily in a random manner. An OTP would be generated and sent to the users mobile device through the phone number that was registered.



FDS-MFA: Fraud Detection System Using MFA Scheme

First Name

Middle Name.

Last Name

Mobile

Email Address

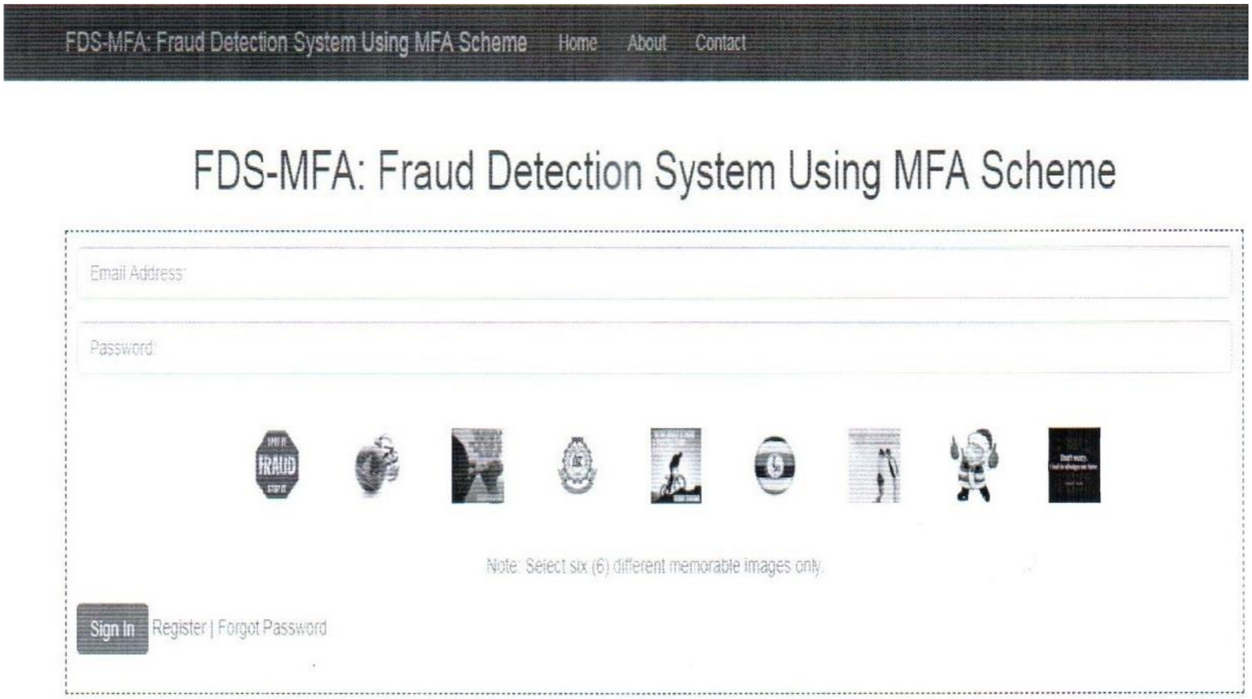
Password

Gender ○ Male ○ Female

Note: Select six (6) different memorable images Only

Figure 2: Registration page

Figure 3 is the login page, and the second phase and step that is carried out by the user before the activity page would be displayed. Once a user is registered, the only attributes to be filed are the email address and password, selection of images according to the manner of selection during registration. An OTP would be generated and sent to the mobile device of the user; the user enters OTP and logs in.

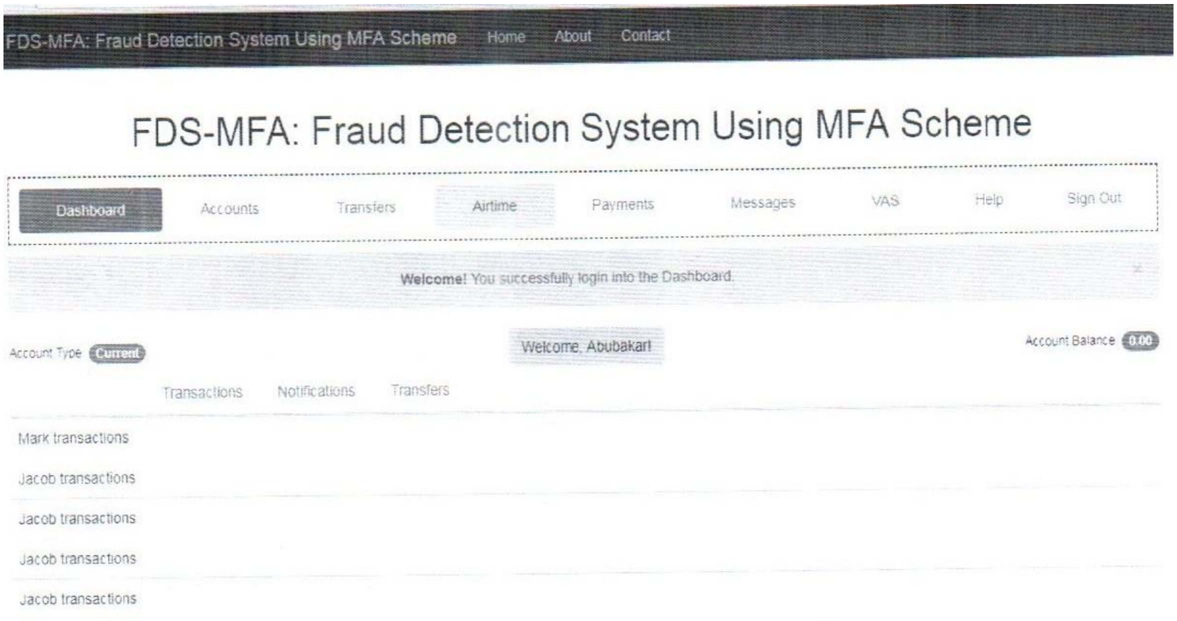

FDS-MFA: Fraud Detection System Using MFA Scheme
Home
About
Contact
Email Address:
Password:
FRAUD
Sign In
Register | Forgot Password

FDS-MFA: Fraud Detection System Using MFA Scheme

Note: Select six (6) different memorable images only.

Figure 2: Login page

Figure 3 is the Activity page where activities carried out is popped up immediately after login. It comprises of actions that would be carried out by the user quickly they are signed in.



FDS-MFA: Fraud Detection System Using MFA Scheme

Welcome! You successfully login into the Dashboard.

Welcome, Abubakar!

Mark transactions

Jacob transactions

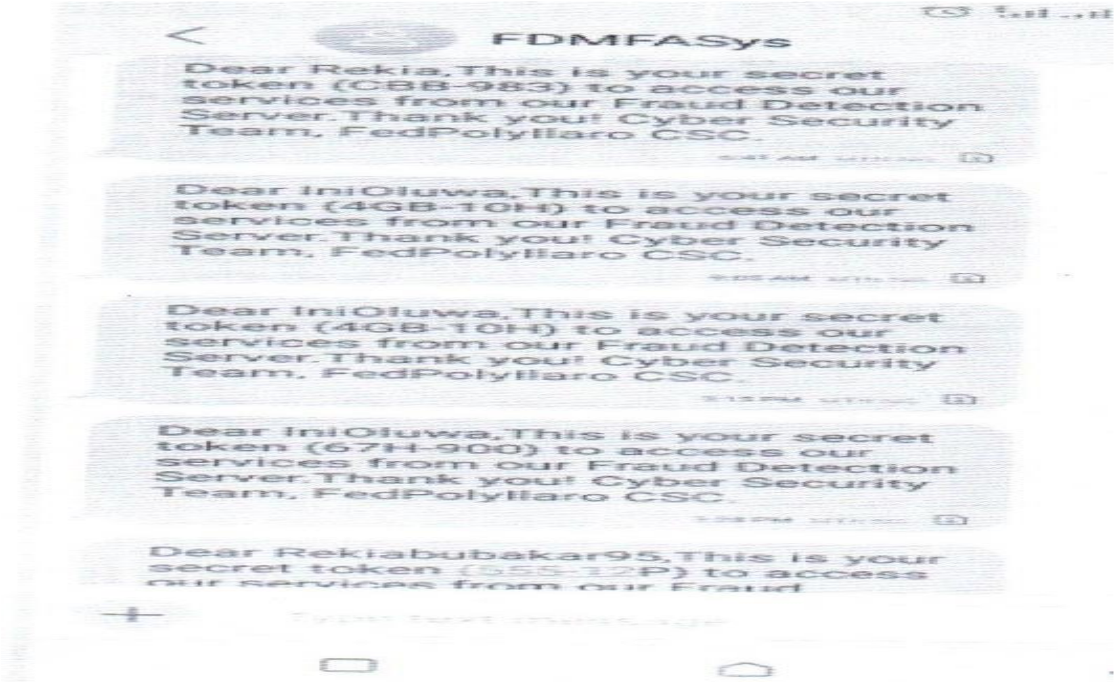
Jacob transactions

Jacob transactions

Jacob transactions

Figure 3: Activity page

Figure 4 is the stage where OTP for login is sent to the user's mobile phone through the phone number provided by the user.



Dear Rekia,This is your secret token (CBB-983) to access our services from our Fraud Detection Server.Thank you! Cyber Security Team, FedPolyIlaro CSC.

Dear IniOluwa,This is your secret token (4GB-10H) to access our services from our Fraud Detection Server.Thank you! Cyber Security Team, FedPolyIlaro CSC.

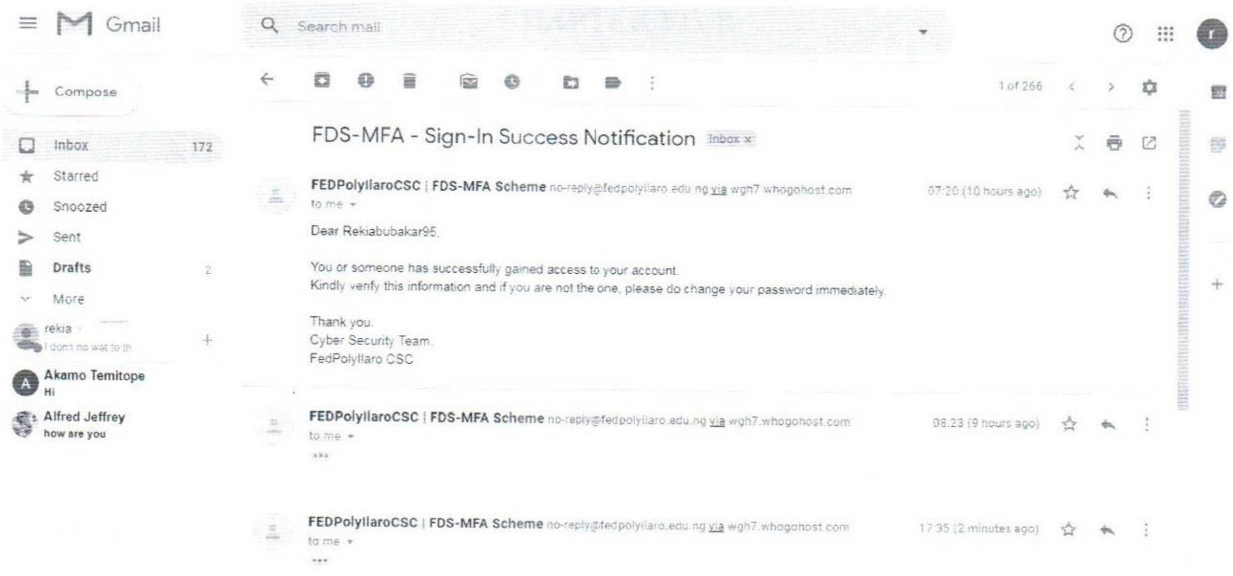
Dear IniOluwa,This is your secret token (4GB-10H) to access our services from our Fraud Detection Server.Thank you! Cyber Security Team, FedPolyIlaro CSC.

Dear IniOluwa,This is your secret token (67H-900) to access our services from our Fraud Detection Server.Thank you! Cyber Security Team, FedPolyIlaro CSC.

Dear Rekiabubakar95,This is your secret token (555-12P) to access our services from our Fraud

Figure 4: OTP Verification page

Figure 5 consists of notifications that are sent to the mail; these messages include error messages, success messages, and messages requesting a change of password.



FDS-MFA - Sign-In Success Notification

FEDPolyIlaroCSC | FDS-MFA Scheme no-reply@fedpolyilaro.edu.ng via wgh7.whogohost.com 07:20 (10 hours ago)
to me

Dear Rekiabubakar95,

You or someone has successfully gained access to your account.
Kindly venfy this information and if you are not the one, please do change your password immediately.

Thank you.
Cyber Security Team.
FedPolyIlaro CSC

FEDPolyIlaroCSC | FDS-MFA Scheme no-reply@fedpolyilaro.edu.ng via wgh7.whogohost.com 08:23 (9 hours ago)
to me

FEDPolyIlaroCSC | FDS-MFA Scheme no-reply@fedpolyilaro.edu.ng via wgh7.whogohost.com 17:35 (2 minutes ago)
to me

Figure 5: Email Notification page

5.0 Conclusion

This study makes available a fraud detection system that employed a multi-factor authentication system to detect online banking fraud. Multi-factor authentication based on device and human interaction were used to secure the online financial transactions synchronously, thus enabling the user and provider a seamless provision of security and financial services over a device. Further protection can be provided through encryption and storage of data in distributed sites reducing the risk of identity theft.

References

Achemlal, M., Gharout, S., & Gaber, C. (2011). Trusted platform module as an enabler for security in cloud computing. In *2011 Conference on Network and Information Systems Security* (pp. 1-6). IEEE.

Adeoye, O.S. (2012). Evaluating the performance of a two-factor authentication solution in the banking sector. International Journal of Computer Science Issue, 9(4), 457-462.

Aloul, F. Zahidi, S. & El-Hajj, W. (2009). Two-factor authentication using mobile phones. Computer Systems and Applications. Journal of information processing system, 5(56),1-10.

Antal, M., & Szabo, L.Z (2015). Biometric Authentication Based on Touch Screen Swipe Patterns.
Journal of Procedia Technology, 22(7),862-86

Corella, F., & Lewison, K (2012). Strong and Convenient Multi-Factor Authentication on Mobile
Devices. Journal of information communication technology, 11(19),1-31

Garba, F. A. (2016). A new secured application-based mobile banking model for Nigeria. *Int. J. Comput. Sci. Inf. Technol. Secur.(IJCSITS)*, 1-8.

Jadhav, P., Shirsat, P., Bhargude, P., & Kamble, S. (2016). Voice Pitch Based Authentication for Android Application, 6(3), 3019–3021

Mohamed, T. S. (2014). Security of Multifactor Authentication Model to Improve Authentication
Systems. *Information and Knowledge Management Journal*, *4*(6).

Ombiro, Z. B., (2016). *Mobile–Based Multi-Factor Authentication Scheme for Mobile Banking* (Doctoral dissertation, University of Nairobi).

Prasanalakshmi, B., & Pugalendhi, G. K. (2019, June). Two-Way Handshake User Authentication Scheme for e-Banking System. In *International Conference on Intelligent Computing and Communication* (pp. 135-141). Springer, Singapore.

Sarhan, H., Hafez, A. A., Safwat, A., & Hegazy, A. A. (2015). Secure android-based mobile banking scheme. *International Journal of Computer Applications*, *118*(12).

Shinkar, N., Sonje, S., Kamble, S., Pardeshi, P., & Dhule, P. (2018). Two Way Authentication for Banking Systems. *International Research Journal of Engineering and Technology (IRJET)*, 5(11),1464-1466