

# Design and Implementation of a Secure Online Electronic Transaction (SOET) System for a Cashless Society

Etuh E<sup>1,\*</sup>, Obiniyi A. A<sup>2</sup>, Yusuf O. S<sup>3</sup>, Akinyele O. A<sup>4</sup>

<sup>1</sup>Department of Mathematics and Computer Science, Arthur Jarvis University, Akpabuyo, Nigeria

<sup>2</sup>Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

<sup>3</sup>Department of Physics, Arthur Jarvis University, Akpabuyo, Nigeria

<sup>4</sup>ICT Department, Hephzith Technology, Osogbo, Nigeria

\*Corresponding author: [emma.etuh@arthurjarvisuniversity.edu.ng](mailto:emma.etuh@arthurjarvisuniversity.edu.ng)

**Abstract** Business transaction since inception from trade by barter to modern e-commerce system constantly faced the challenges of how to minimise fraudulent activities around it. With the advent of Internet, trading has become a global activity where the location of one's goods and services is no longer important provided there is a connection to the "market". Serious attention must be given to the security challenges facing the "Market" arising from online authentication mechanisms. Prevalent ones today uses what the user knows (password) or what the user have (token) for authentication, there is a need for a more reassuring proof of identity to make cashless economy a huge success and ensure effective participation in the contemporary E-market. The research work- Secure Online Electronic Transaction (SOET) System integrates the functionality of biometric credential as authentication mechanism to ensure secured transactions over the network in an E-market of a cashless society.

**Keywords:** authentication, E-commerce, E-payment, E-market, E-transaction, cashless society

**Cite This Article:** Etuh E, Obiniyi A. A, Yusuf O. S, and Akinyele O. A, "Design and Implementation of a Secure Online Electronic Transaction (SOET) System for a Cashless Society." *Journal of Computer Sciences and Applications*, vol. 5, no. 2 (2017): 83-89. doi: 10.12691/jcsa-5-2-5.

## 1. Introduction

The transfer of ownership of goods and services from one person or entity to another is referred to as trade. It could loosely be called commerce, financial transaction or barter [1]. The origin of trade can be traced to as far back as the existence of man, the economist postulated that human wants are insatiable [2]; this assertion captures the behaviour of man right from origin always having a quest to getting more, especially new products other than the one that is owned. This led to improvising means of acquiring goods and services without necessarily going through the same rigor of production. It started with the barter system where owned commodities are being exchanged with the needed ones. An instance is a primitive hunter wishing to trade surplus catch for animal skin, or stone implement or other goods. A network that allows trade is called a market. The emergence of Internet in the last decade has greatly transformed the way business activities are being carried out. Trade system grew from barter to the use of money; the money also witnessed changes from one form to the other as time progresses till this present day that goods and services are being exchanged at the transaction point (market) using a mixture of raw/e-money which are the present medium of exchange.

A transaction in digital world is quite technical, the

real/actual market does not deal with virtual people or ghosts (people from unseen world) but with actual people. It is quite easy to identify people in the real/actual market because the participants carrying out the business transaction are physically present, but in the virtual market (e-market) of the global village, the parties in transaction are not physically present. Obviously, since these processes take place in a public and un-trusted network, there are many security issues involved, such as verification of the identities of the participants, or protection of data in transfer [3]. So how to ascertain the authenticity of the party in the virtual market becomes a concern to both parties involved in a virtual transaction.

The introduction of cashless economic policy in Nigeria is a booster to electronic commerce in the present day global village. It does not imply not using money for transaction in an economic system; it is simply an economic system whereby all means of payments are carried out without the use of physical cash [4]. Payments will range from a list of options such as cheques, wire transfers, debit and credit cards, online transactions, and mobile banking and these alternatives to payment best promote e-transaction in the virtual market. Nigeria compared to the rest of the world, as it relates to payments, is still far behind, as a plus to strengthening the e-commerce in Nigeria, the apex bank has introduced a cashless economic policy where limitless cash withdrawal and transaction is restricted, the pilot scheme has begun in Lagos. It is known as 'cashless' policy. According to the

CBN, the cash-less system became necessary to promote the use of electronic means of transaction aimed at making Nigeria a cashless economy [5]. In addition, the policy aims to curb some of the negative consequences of high usage of cash, including high cost of handling (estimated to be about N192 billion this year), high risk of usage and high subsidy [6].

Considering the dangers associated with Internet-based technologies, there are fears that the legal framework needs to be strengthened to protect consumers against fraud, losses and undue charges, while much attention is being given to regulations, mobile payment and the deployment of more Point-Of-Sale terminals, online fraud on e-payment platforms is the greatest threat to the Nigerian payments infrastructure [7]. At a recent e-payments forum, it was explained, how his team tested multiple e-payments networks and found that online fraudsters are outpacing security technology. By simply manipulating some codes, the team was able to obtain airline tickets on an e-ticketing portal and purchase items online through a shopping portal, both by making no actual payment. Something has to be done to raise the bar of security certification and network authentication in electronic transactions because the form of security these portals have is not what they should have in this kind of payment system [7].

## 2. Related Works

The major way of identifying a party in an online system is through authentication mechanism. Authentication means validating the identity of a user who needs to access a set of resources [8]. The evidence provided by a user in the process of user authentication is called a credential [9], different systems may require different types of credentials to verify user identity, and may even require more than one credential. There are various mechanisms for authenticating a user trying to access resources within a computer system environment, authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are: Something you know, something you have, something you are [10]. The most secured form of authentication is identifying a user based on some biological proof of what the user is, this is being referred to as biometric authentication [11].

With the advent of cashless policy of the Central Bank of Nigeria as the technology tends towards cashless economy, there is a need to find a model that is convincingly secure enough for trade activity in the virtual world market. Authentication using what the user knows like user name and password often time has caused a lot of problem: dictionary attack, stolen password, repudiation, and the likes. Averagely, a good percentage of people forget their password especially at a critical time they want to make transaction because of the complexity forced on the password field during registration or online account creation. Some online payment system uses credit card information for online payment but this has some drawbacks as some consumers are unwilling to divulge credit card information over the Internet because they are not certain of its security; this reluctance has hampered the growth of e-commerce hence a need for a better alternative [12].

Survey of User Authentication was made where it was predicted that in the mere future, biometric credentials will become the prevalent mechanism [13]. Continuous Biometric Authentication for Authorised Aircraft Personnel designed for use within the flight deck, which has a matching device called “trusted, hardened, and tamperproof PC” which is needed in the flight deck in order to accomplish live presentation, matching, and acceptance (or rejection) onboard the aircraft [14].

In some countries operating the system, the policy is called ‘mobile wallet’, which is an alternative payment method that allow the use of mobile phone to pay for a wide range of services [15].

A Secure Electronic Transaction Payment Protocol Design and Implementation offers an extra layer of protection for cardholders and merchants, customers are asked to enter an additional password after checkout completion to verify they are truly the cardholder; the authentication is done directly between the cardholder and card issuer using the issuer security certificate and without involving the third party (Visa or MasterCard) [16].

## 3. Materials and Method

A review of related works of online identification/payment systems and security technologies was made to give necessary background thereafter, an online store scenario was developed to model a market plaza where goods and services are displayed for buyers to access. A biometric security mechanism is used for online identification. A potential customer except the window shoppers will have to create an online account with the modelled online bank called E-Naira bank to participate in the transaction. The technological approach to the implementation was based on open source software solutions (WAMP: Window, PHP, Apache, MySql). A 3-tier architecture was employed using PHP (Personal-Home-Page Hypertext Pre-processor) scripting language and Java to render the front-end, Apache HTTP (HyperText Transport Protocol) was used as the Web server (Middleware) and MySQL was used as the data store (Back-end).

There are four major components of the intended system as shown in Figure 1: the shop layer, payment layer, authentication layer, and the processing layer.

### 3.1. The Shop Layer

The Shop Layer consists of all the online stores that support online payment mechanism. It can be any of the credit/debit cards, electronic wallet, or pay on delivery system or the SOET. My Online Store is used to simulate the idea in this regard.

### 3.2. The Payment Layer

Various forms of payment appear in the payment layer of which users are expected to choose the convenient one. The research focuses on SOET option which has a payment gateway where the user is expected to go through in order to pay for the selected item(s) during the online shopping process.

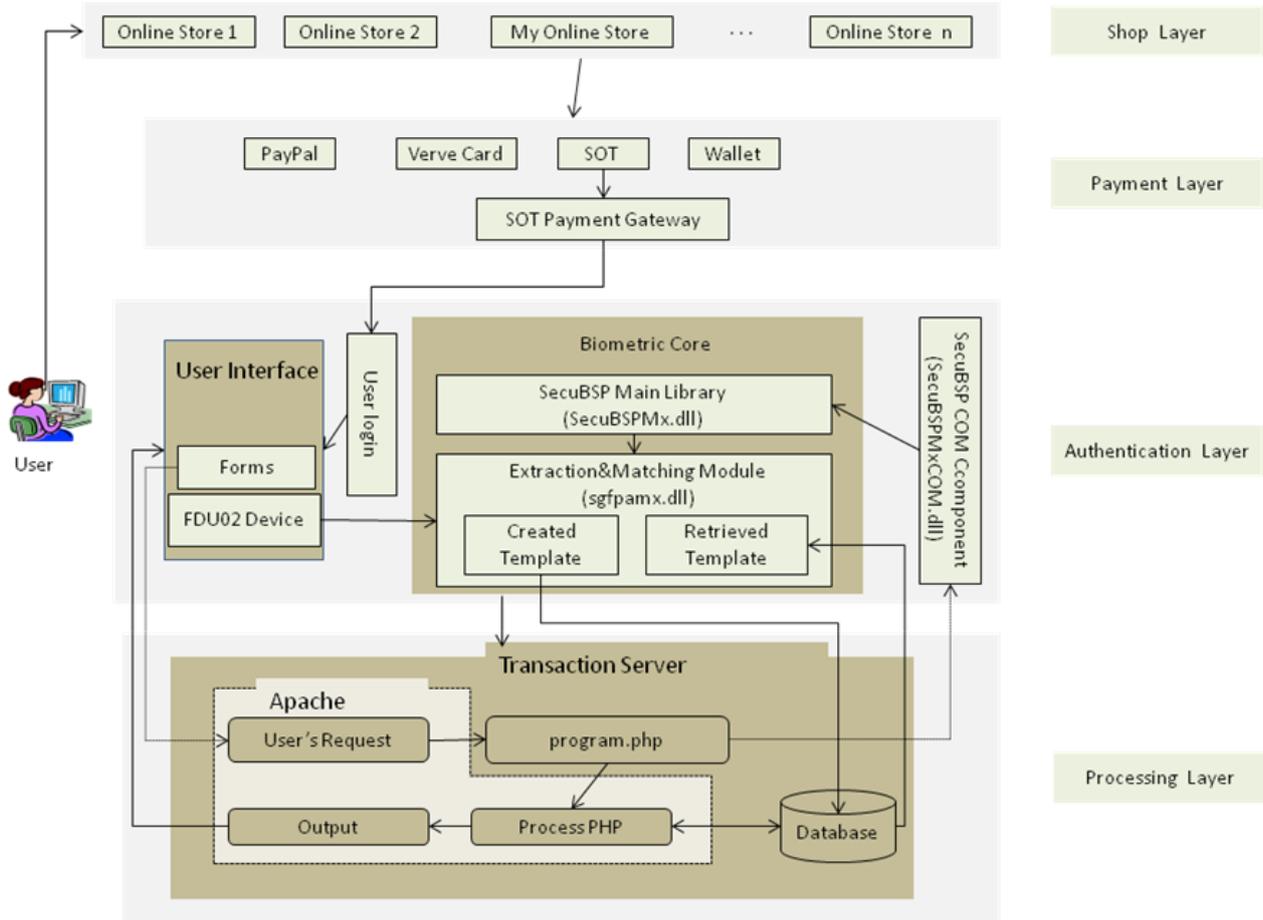


Figure 1. SOET System Architecture

### 3.3. The Authentication Layer

Several components make up the authentication layer to ensure adequate security of the user's account during transaction. These components include the User Login where the user's credential is required to logon to the system, the credential must be the same with the one provided during the enrolment process providing the right credential is vital as access will be denied should the user provide a wrong one. User Interface enables the customer to interact with the system, it hides the underlying functionalities, through a web browser, forms are provided with which the user communicates with the system appropriately and a biometric device that helps the user to input the biometric credential in order to gain access to transaction platform. Biometric Core in the authentication layer comprises of various modules that ensure the effective implementation of biometric credential authentication. The main dynamic link library that implements all the biometric functions is called "SecuBSP Main"; there is also the Extraction and Matching Module that handles the authentication. The "SecuBSP COM" is a Component Object Model-based technologies that facilitates easy integration of biometric credentials by developers using web development or RAD tools.

### 3.4. The Processing Layer

Processing layer is the transaction server that implements the transaction after the user's claim has been

rightly verified. This layer comprises of composite software that manages the smooth instance and implementation of the transaction by the online bank. Several software components like the Apache, PHP web scripting language and MySQL database are found in this layer.

## 4. SOET Database Design

SOET database system is a collection of interrelated files and a set of programs that allow users to access and carryout secure electronic transaction. A major purpose of the database system is to provide users with an abstract view of the data. The security of the SOET system wholly depends on the extent to which the database is secured and this will be a function of the administrator managing the database. Underlying the structure of a database is the data model; a database management system (DBMS) allows a user to define the data to be stored in terms of a data model. Different data models include: the relational, the entity-relationship, object oriented, object-relational, network and hierarchical model. All the models provide a way to describe the design of a database at the logical level.

Most database management systems today are based on the relational data model, which will be used in the system database design.

The central data description construct in this model is a relation, which can be thought of as a set of records. A

relation is customarily referred to as a file and generally perceived and represented by a set of structured tuples. Each tuple of a relation corresponds to a record in a file and attributes correspond to fields within a record. The general form of a relation is given by R [A1, A2, ..., An-2, An-1, An]. The name of the relation is represented by R, while the set (A1, A2, ..., An-2, An-1, An) represents the attributes of the relation R. A description of data in terms of a data model is called a schema. In the relational model, the schema for a relation specifies the name of each field (attribute or column), and the type of each field. As an example account\_holder information in the database may be stored in a relation with the following schema: Account\_holder [Account\_id: int, AccountName: string, Last\_name: string, First\_name: string, Mid\_name: string, email: string, Tel\_Num: int, Sex: string, City: string, State: string, Country: string]. The preceding schema says that each record in the Account\_holder relation has eleven fields, with each field “name: type” pair as indicated. Other database objects used in the system are: Account\_details [id: int, Account\_id: int, AccountName: string, Current\_amt: real, Account\_status: string, Username: string, Password: string, FIRTextData: string real]. Account\_holder [Account\_id: int, AccountName:

string, Last\_name: string, First\_name: string, Mid\_name: string, email: string, Tel\_Num: int, Sex: string, City: string, State: string, Country: string]. Transaction [transaction\_id: int, merchant: string, order\_id: int, order\_amount: int, currency\_iso\_3: string, Account\_id: int, AccountName: string]. Category [categoryID: int, name: string, parent: int, products\_count: int, description: string, picture: string, products\_count\_admin: int]. Ordered\_carts [productID: int, orderID: int, name: string, Price: real, Quantity: int]. Orders [orderID: int, order\_time: datetime, cust\_firstname: string, cust\_lastname: string, cust\_email: string, cust\_country: string, cust\_zip: int, cust\_state: string, cust\_city: string, cust\_address: string, cust\_phone: string]. Products [productID: int, categoryID: int, Name: varchar, description: text, customers\_rating: float, Price: float, picture: varchar, in\_stock: int, thumbnail: varchar, customer\_votes: int, items\_sold: int, big\_picture: varchar, enabled: int, brief\_description: text, list\_price: float, product\_code: char].

The entities include Account\_holder, Product, Account\_detail, order details, product categories, Account\_holder Detail, transaction with their corresponding attributes and relationships as shown in Figure 2.

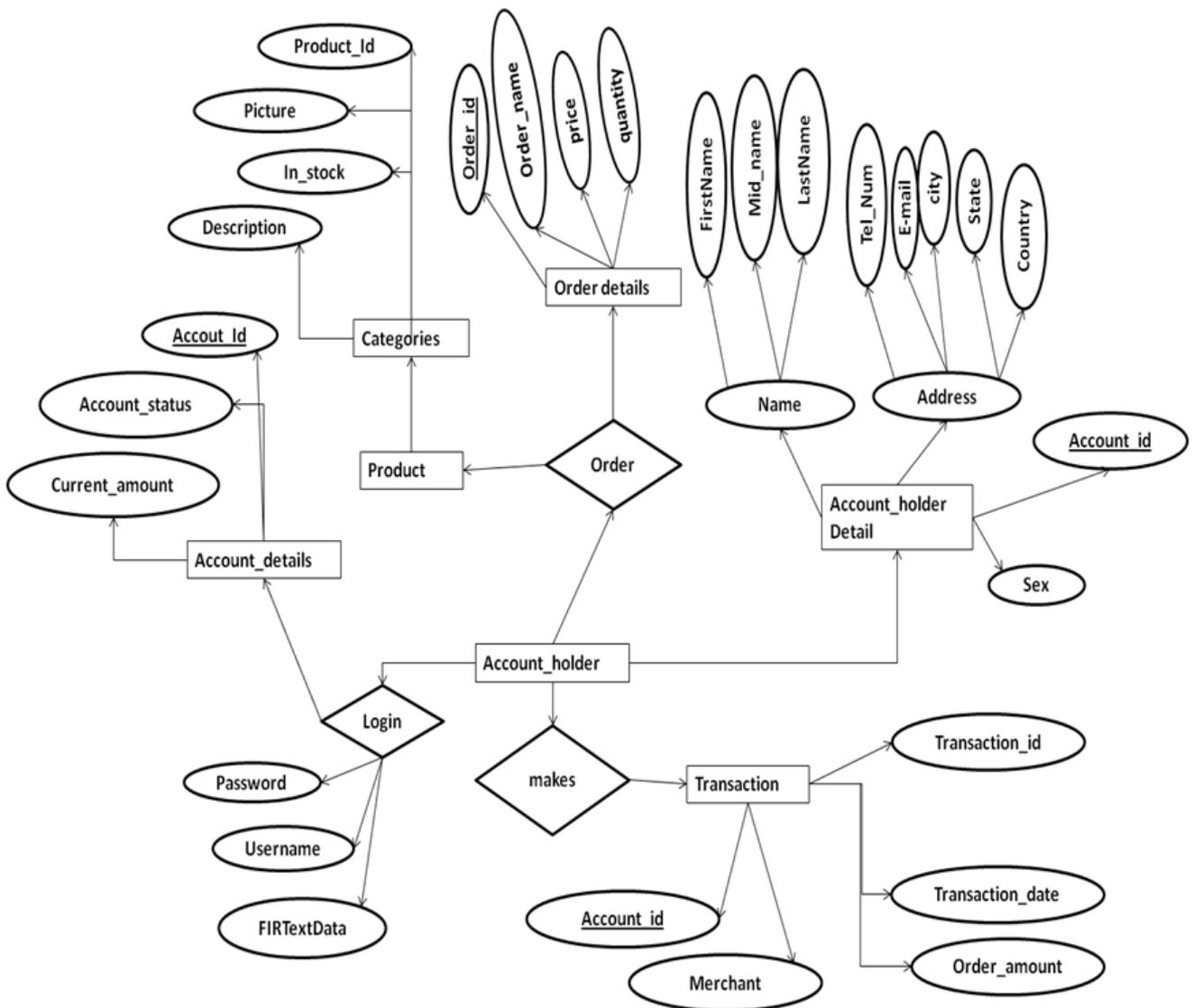


Figure 2. The Entity Relation Diagram of SOET

## 5. Implementation

The interfaces of the system implemented are shown in the Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7 respectively.

Figure 3 is an interface which depicts a customer setting the security feature during registration with the Online bank, on placing the finger, the device captures the fingerprint image and the embedded

algorithm for extraction automatically extracts the feature of the finger and creates an enrolment template for the user.

On getting to the online store after shopping (Figure 4), the shopping cart displays the selected items for to be purchased with the total amount; select proceed to checkout, then fill and submit the contact form. Choose the eBank Naira – the modeled bank that handles the payment as payment option.

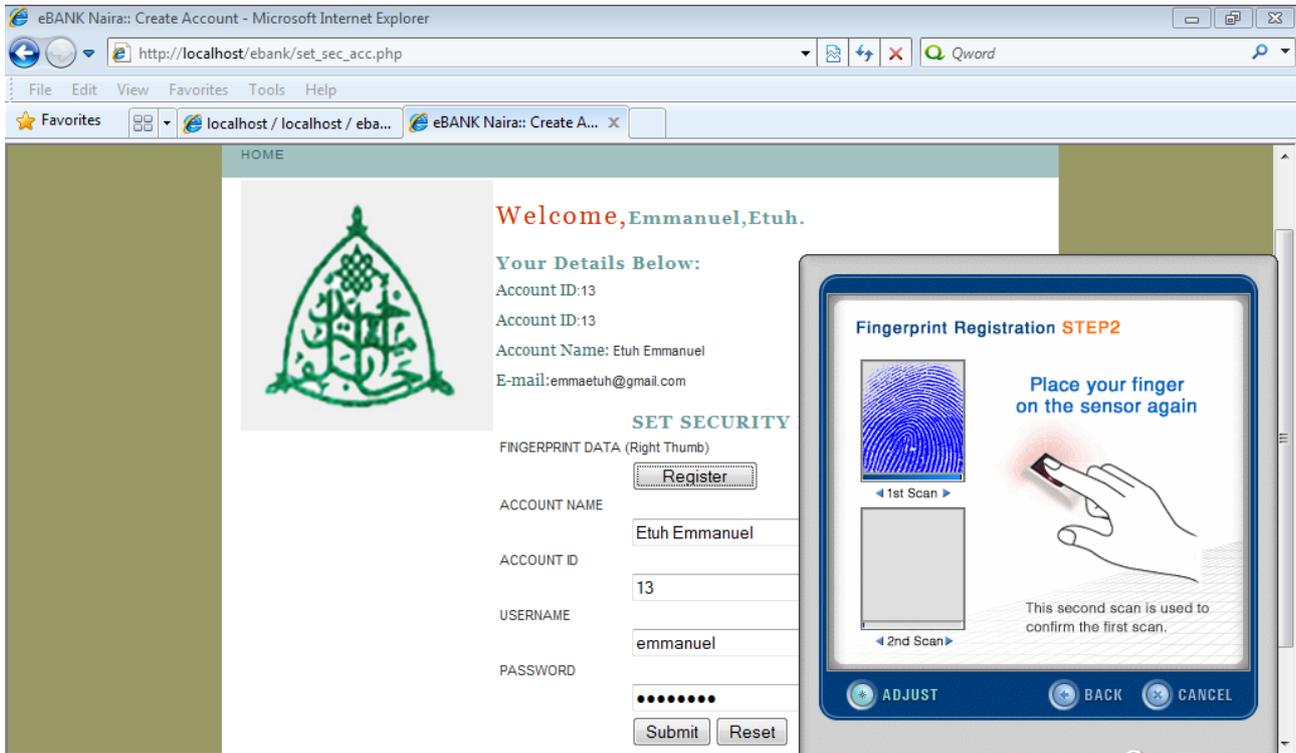


Figure 3. Enrolment phase

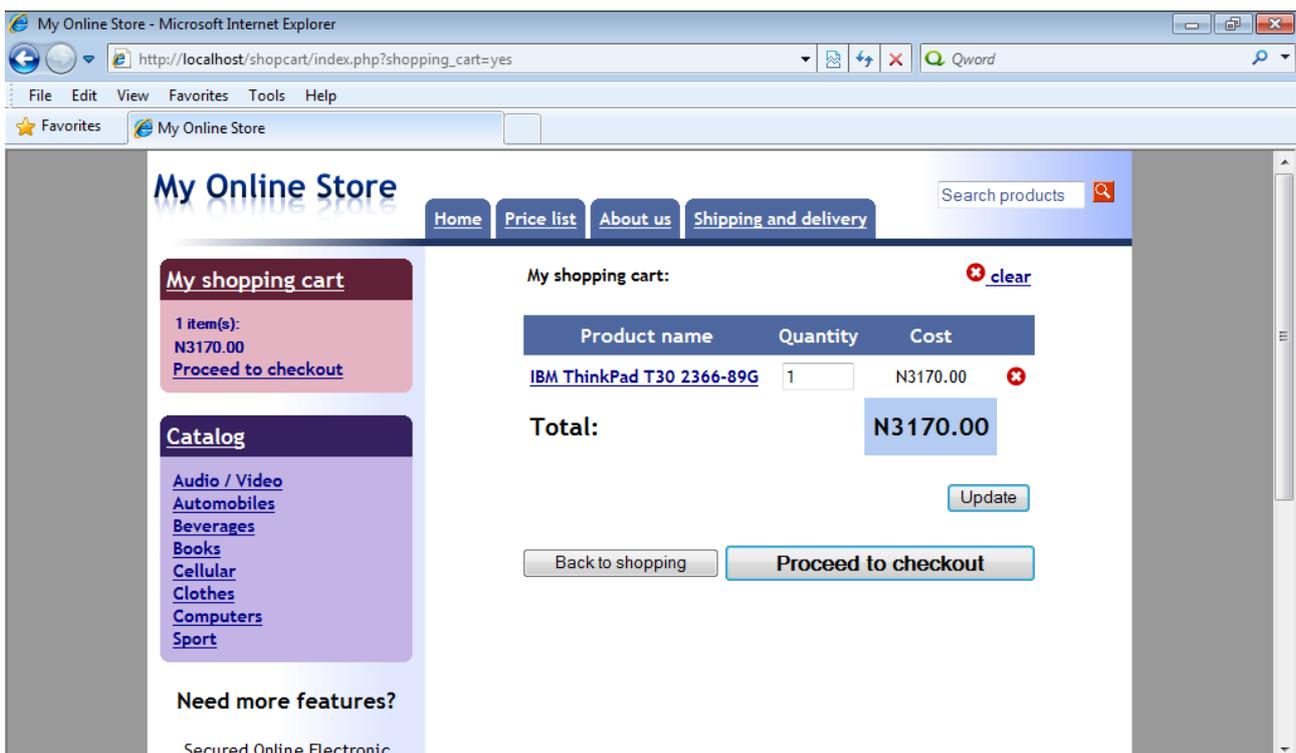


Figure 4. Online store shopping

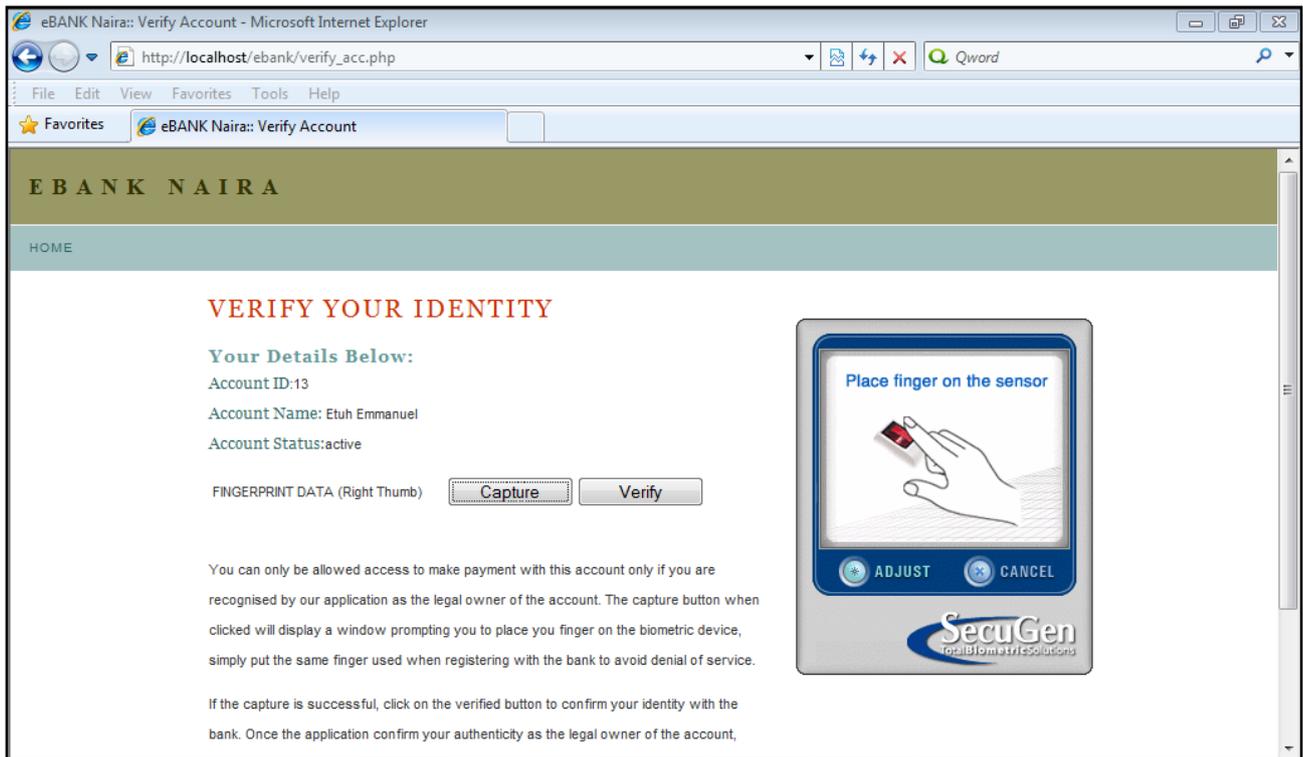


Figure 5. SOET identity verification

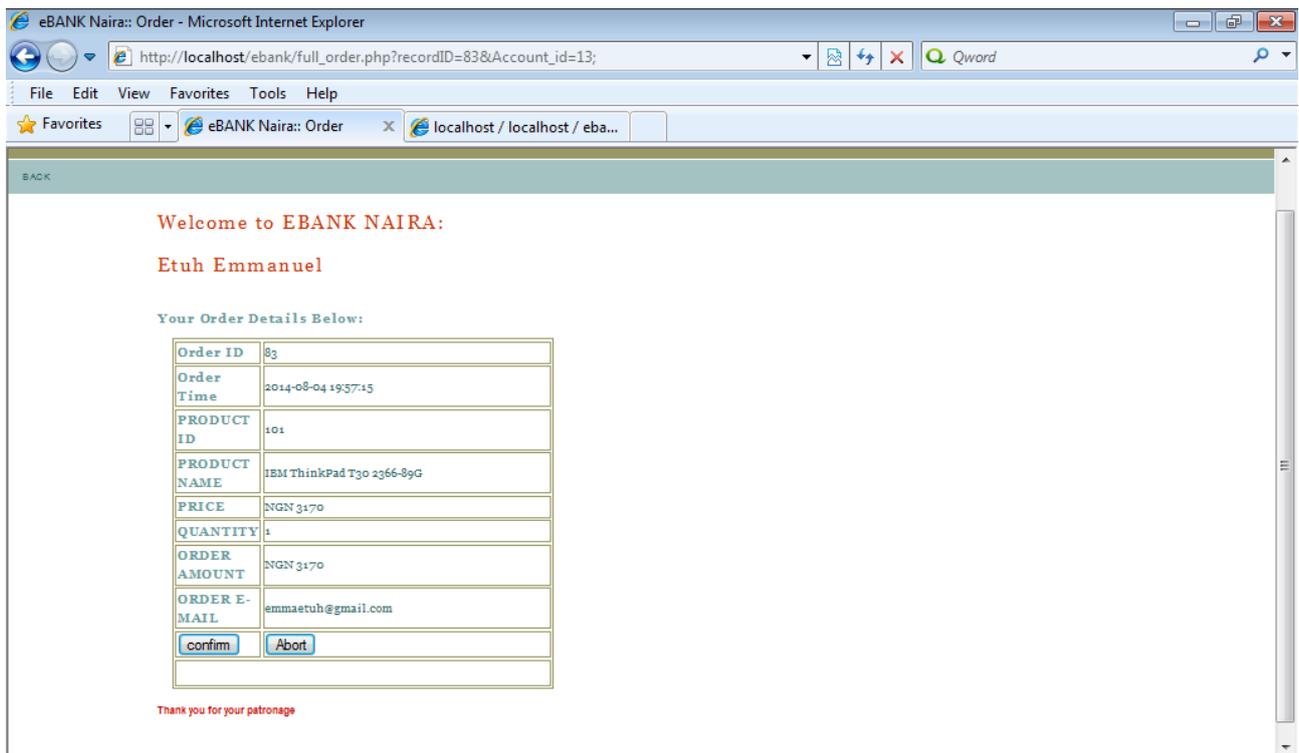


Figure 6. Transaction detail

If the choice is the E-bank naira, on passing through the payment gateway, the system prompts the user to place the enrolment fingerprint on the sensor to ascertain the veracity of claim. The user is expected to place the exact finger used during enrolment in order to be identified as the right owner of the account. If a different finger is used instead, the user will be treated as an imposter and will be denied access outrightly, but if

successful, the account detail with the details of order made by the user is displayed for confirmation (Figure 6). At this point, the user can either confirm or abort the transaction.

If the user chooses to proceed with the transaction by selecting the “confirm” button, the amount of the order is deducted from the user’s account and the current update of the account is communicated to the user.

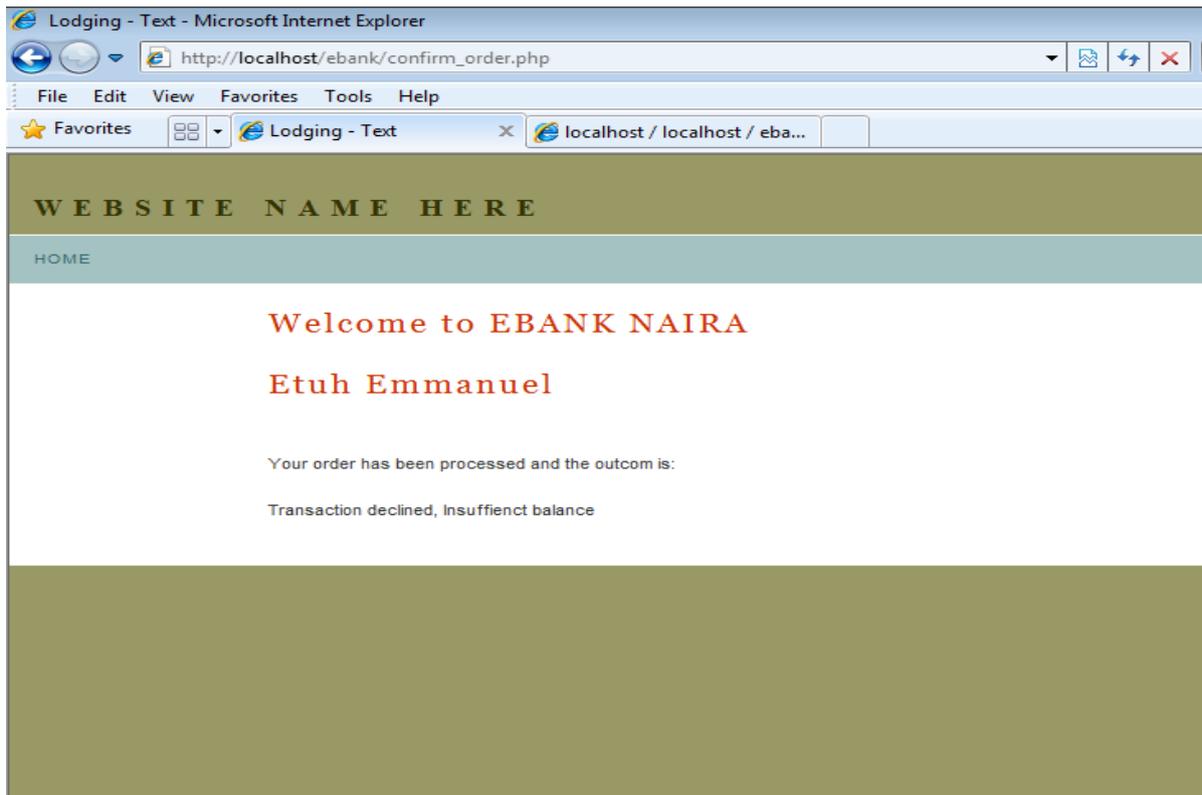


Figure 7. Transaction Outcome

## 6. Conclusion and Future Work

With an increasing reliance on online technology, business transactions of all types are increasingly being handled online and remotely. This exceptional growth in electronic transactions has suggested the need for a faster, more secure and more convenient method of user verification method than passwords and tokens can afford.

The framework brings virtual business transaction to what is obtainable in the actual world since authentication is based on human trait, this will go a long way to making online transaction safer and secure thereby increasing users opinion and patronage in the cashless society.

Further improvement can be made to extend the work to mobile application platform, other works like shop boot can be integrated to help the customers derive maximum satisfaction in the market, also as technology advances, the biometric authentication can be made multimodal to enable alternative to identity verification.

## References

- [1] wikipedia. (2012). *trade*. <http://en.wikipedia.org/wiki/Trade.htm> 2012 [Apr. 26, 2012].
- [2] Lebergott, S. (1993). *Pursuing happiness –. American consumers in the Twentieth Century*. Princeton University Press, pp 69.
- [3] Hassler, V. (2001). *“Security Fundamentals for E-Commerce”*. Massachusetts: Artech House pp 28.
- [4] Ezumba, S. *“The Transition to a Cashless Economy in Nigeria”*. <http://www.reinventrebuild.com/nigeriaone.php> 2011 [Feb. 6, 2013].
- [5] CBN. *“Further Clarifications on Cash-less Lagos Project*. Retrieved from Central Bank of Nigeria, 2006-2011”. <http://www.cenbank.org/out/pressrelease/gvd/cashlesslagos> Project.pdf May 6, 2011 [Nov. 19, 2013].
- [6] Ikhilae, E., Jibueze, J., and Igbonwelundu, A. P.” *Wanted: Laws on cashless economy”*. <http://www.thenationonlineng.net/2011/index.php/law/43356-wanted-laws-on-cashless-economy.html> 2012 [Feb. 6, 2012].
- [7] Deichler, A. *“Fraudwatch: A Threat to a Cashless Economy”* [http://www.afponline.org/pub/res/news/Fraudwatch\\_\\_A\\_Threat\\_to\\_a\\_Cashless\\_Economy.html](http://www.afponline.org/pub/res/news/Fraudwatch__A_Threat_to_a_Cashless_Economy.html) 2011 [Feb. 6, 2012].
- [8] Forouzan, B. A. (2007). *“Data Communications and Networking”* (Fourth ed.). New York,: McGraw-Hill Companies, Inc.New York, pp. 352.
- [9] Todorov, D. (2007). *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. USA: Taylor and Francis Group, LLC. pp. 7-10.
- [10] Pfleeger, C. P. (1989). *Security in Computing*. Upper Saddle River, NJ 07458: Prentice Hall, Inc. pp. 196-241.
- [11] Blackburn, D., Miles, C., Wing, B., Shepard, K., Atkins, J., Basu, S., et. al. *‘Biometrics “Foundation Documents”*., from National Science and Technology Council’s (NSTC) Subcommittee on Biometrics’ [http://www.biometrics.gov/Documents/Blackburn\\_Australia\\_Conference\\_May08.pdf.org/biometrics.pdf](http://www.biometrics.gov/Documents/Blackburn_Australia_Conference_May08.pdf.org/biometrics.pdf) May 08, 2005 [Apr. 03, 2013].
- [12] Ratha, N., Connell, J., & Bolle, R. (2001). *Enhancing security and privacy in biometrics-based authentication systems*. *IBM systems journal*, 40, 615-634.
- [13] Magno, B. M. *“Survey of User Authentication”*. Naval Postgraduate School Monterey, M Sc Computer Science, California, 1996.
- [14] Carrillo, C. M. *“Continous Biometric Authentication for Authorized Aircraft Personnel: A Proposed Design”*. M Sc Thesis, Naval Postgraduate School Monterey, California, 2003.
- [15] JVL. (2012). *Isis Mobile Wallet*. Retrieved December 15, 2012, from American Express: <http://www.onlineamericaexpress.com/mobilewallet> 2012 [Dec. 15, 2012].
- [16] Ismaili, H. E., Houmani, H., & Madroumi, H. (2014). *“A Secure Electronic Transaction Payment Protocol Design and Implementation”*. *International Journal of Advanced Computer Science and Applications*, pp. 172-180.