A Biometric Identification Based Scheme for Secured E-Payment

Okediran O. O. *, Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. & Bashorun M. A.
Department of Computer Science & Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

*Corresponding author: Okediran O. O.
Department of Computer Science & Engineering,
Ladoke Akintola University of Technology,
Ogbomoso, Oyo State, Nigeria.
E-mail: oookediran@lautech.edu.ng

Received: April 2, 2013, Accepted: April 26, 2014, Published: April 28, 2014.

ABSTRACT
Means of electronic payment are of diverse forms, some of which are mostly an extended version of the existing offline method. Much attention has not been paid to proper authentication for users, non-repudiation from the merchant to the users, and adequate protection from unauthorized use of payment data at the merchant or Payment Service Provider (PSP)’s end. The quest for additional security measure in identification process in online e-payment systems has brought about the need for the development of an improved e-payment system. This paper presents a scheme for biometric identification for electronic payment system tailored towards the payment of fees in tertiary institutions that addressed the challenges emanating from the present e-payment systems.

Keywords: e-payment, biometrics, authentication, credit card, debit card.

INTRODUCTION
Electronic payment (e-payment) system refers to the automated processes of exchanging monetary value among parties in business transaction and transmitting this value over the information and communication technology networks, [2]. Examples of electronic form of payments are scratch cards, electronic cheque, electronic cash, smart cards and so on which have been used for exchange of goods and services over the internet electronically.

The advent of electronic payment systems, regardless of the adopted system opened the doors to a lot of risks due to the fact that the process of identification mostly require replay of personal information across the internet. These forms of identification sometimes include entering of PIN’s, account numbers, name and address of payers, [15]. The risks attached to this kind of authentication are too numerous to be overlooked. The account details could be intercepted, eavesdropped on, amount paid can be compromised and intercepted information can be used for obtaining loans and withdrawals from account holder. Fake PINs can be generated to fool the electronic medium into acknowledging payments whereas none has ever been made, PINs can also be forgotten or stolen thereby locking out individuals from accessing his or her rightful accounts. Online database can be breached just like it happened to “CD universe” (a web based CD store) when a hacker broke through their security system and gained access to 300,000 credit card account numbers resulting in the web site being shut down [7].

The attending problems to identification for e-payment have raised the alert level for security in the course of e-payment. And this has led to a lot of security initiatives like Secure Electronic Transaction protocol (SET), Secure Socket Layer (SSL) and so on. These has helped considerably, but it has been found to fail in several ways and at times where the culprits are the employees’ of the financial organizations handling payment instructions, where such individuals are able to hack or intercept payment instructions, identification process and clone similar portals for e-payment or generate fake PINs [12]. Also, identification for e-payment deals mainly with the security at the point of entry that is identifying the user who is about to gain entry whereas the above mentioned security initiatives are more pronounced on the protection of data integrity that is, what is sent over the internet. Therefore, there is a need of a more robust authentication system for e-payment systems where additional identification is based on “who you are” and not the usage of information that can be intercepted faked and compromised. This in turn informs a shift in focus during the quest for security for online payment to biometric identification.

Biometric system identifies people by measuring some aspect of individual anatomy or physiology (such as hand geometry or fingerprint), some deeply ingrained skill or other behavioral characteristics (handwritten signature) or something that is a combination of the two [5]. This implies that even if an employee of an organization has access to a client’s record, no fraud can be perpetrated without the presence of the clients, in
that the biometric traits captured from the individual for authentication is not present to complete the authentication process for fraud to take place, most especially with the inculcation of "liveness factor" into present day biometric technology which can determine whether the biometric traits used for authentication is a live one [10]. However, Biometric identification is of many forms and care must be taken to choose one with wide acceptance, less difficult in enrolment and cost effective.

REVIEW OF EXISTING E-PAYMENT METHODS

Online electronic credit-debit card payment system

In this e-payment system, credit cards holders are granted a revolving credit line which enables the holder to make purchases and or cash advance up to a prearranged limit [13]. The online credit card payment system extends the functionality of existing credit card as online shopping payment tools as shown in Figure 1 below. It is the most popular methods of payment especially in the retail markets. Here, data transfer is protected by the Secure Socket Layer (SSL) protocol whose major duty is to ensure the encryption and integrity of a transferred message [11].

In credit cards payment system, merchants can use it in two versions: with or without an intermediary. The version without intermediary assures message encryption and integrity but exposes both parties to other risks. As a customer communicates their card number and expiry date directly to a merchant, the card number can be taken from an insufficiently protected server of the merchant or illegally reused. Moreover, the existence of the merchant is not ensured. The merchant in turn does not have a guarantee that the buyer exists and that they will not repudiate the purchase afterwards [14]. The version with an intermediary assumes the participation of a third trusted party, which guarantees the existence of the vendor as well as denies them access to the buyers’ card data. It increases security on the customer side assuring them the merchant authentication and data confidentiality. Nonetheless, the latter is still not able to identify the buyer. This asymmetry can be eliminated by integrating into the technology the system of an electronic signature. The electronic signature allows the authentication of the buyer. As for Debit cards, that is with the debit approach, the buyer needs to have a positive balance of the account before payment as it is deducted immediately (Pay now), (Visa Debit cards, ATMs). With the Credit approach, charges are posted against buyer’s account and billed to the buyer later (Visa Credit Cards generally).

At present, two emerging solutions seem quite interesting: dynamic e-cards and payment via sound waves. Dynamic e-cards allow banks to generate a one-use card and cryptogram number and expiry date every time the card user buys online [1]. This solution does not require any additional applications and significantly minimizes the risk of transaction but ignore convenience. The second solution facilitates the identification and authentication of a card user via unique sound waves generated by the card. However, this system is still in the development phase. Figure 2 is an example of the online version of the credit card form, which is not quite different from that of the Debit Card form and it shows lack of proper authentication on the part of both the buyer and the merchant, most especially when the buyer is paying for services or downloadable products i.e. digital products where the billing address cannot be corroborated.

![Credit Card Payment Form Sample](image)

Figure 2: Credit Card Payment Form Sample

Online electronic cash payment system

Initially, electronic money included three types of payment systems: virtual money, the electronic wallet and the virtual wallet. However, the methods based on virtual money (digital currencies) were abandoned after a short trial period. Nowadays, only two of them are in use [1]. The electronic wallet is based on smart card technology, which is used to store data about the customer's funds. Money is loaded into the e-wallet by transfer from the cardholder's account. In this way, bank is not involved in the transaction at the moment of purchase. Smart cards are used to target mainly the market of micro-payments. At present, they can be used at points of sale, vending machines, parking meters and ticket machines, public payphones, set-top boxes for interactive television and for online transactions, and so on. The integration of this system into internet payments requires installing on the customer side smart card readers. Smart Cards are Credit Card sized plastic cards that have embedded chip with microprocessor and memory capabilities. In e-payment, smart cards are used either as storage devices for much greater information than credit cards with inbuilt transaction processing capability [13], or to enhance e-payment security.

To use smart card offline, it is necessary to have a smart card reader, a hardware device that communicates with chips on the smart card [11]. The reader can be attached with PCs, electronic cash registers, automated teller machines.
(ATM) and so on. Smart cards used for the storage money are actually variations of debit cards that substitute the previous magnetic strip based debit card. These are actually stored-value cards in which prepayment or currency values are electronically stored on the card chips. First, the card has to be loaded with specific amount of money.

This can be done by downloading cash from the bank account or exchanging cash for tokens which can then be used to pay the merchant. The card can then be replaced with more digital cash when the previous money is used up [14]. This card also contains some kinds of an encrypted key that is compared to a secret key contained on the user’s processor. Some smart cards have provision for allowing users to enter a Personal Identification Number (PIN) code. The simplest and the most realistic way to achieve this, is to build such readers into mobile phones. Such solutions can accelerate the development of ‘pay-as you- use’ services such as online games, music ticketing or mass transit systems [1]. Systems based on the virtual wallet are quite similar to electronic wallets. The only difference is that money is stocked on software using tokens instead of on a smart card [14]. Such a system is usually managed by a bank or a bank card issuer. Having created an account, the buyer only has to enter their ID and password at the moment of transaction. Smart card can hold hundred times more data, including multiple credit card numbers and information regarding health insurance, transportation, personal identification, bank accounts and loyalty programs, such as frequent flyer accounts [6]. However, these days smart card technology is being used for debit cards too e.g. ATM cards. The virtual wallet is used for micro-payments via Internet. Nowadays, electronic cash has been broadened to include dedicated account scratch cards [3]. Figure 3 depicts a typical online electronic cash system.

![Figure 3: Online Electronic Cash Payment System](image)

However, the dedicated account scratch cards and debit cards, under the online electronic cash system are widely accepted in Nigeria most especially in tertiary institutions in Nigeria for the purchase of application forms and payment of fees electronically. Ladoke Akintola University of Technology (Lautech), Ogomoso, Nigeria whose electronic payment of fees will be taken as our case study has this method of e-payment system.

**Description and Challenges of the Present E-Payment System**

The existing method is the payment by scratch cards where the student pays at the bank and obtains a scratch card for the amount paid. Armed with the scratch card which contains a covered panel of secret pin numbers and an uncovered serial numbers both of which has been uploaded to the server prior to the time of purchase, the student visits the school’s portal online to make payments as requested. At the school’s portal, the student enters the PIN revealed under the panel where the server compares the PINs with the preloaded PINs and the serial numbers if it tallies, the tuition fee button is then highlighted for payment and the student can proceed for registration. This system which is a subset of e-money method of e-payment systems operates based on trust due to the fact that the pin (the number in the covered panel) is generated and uploaded with the serial number by a human operator. This payment how has the following shortcomings:

- **Problem of physical card costs which either takes its toll on the students by paying extra or on the service provider.**
- **Retailer’s Commission paid by the school.**
- **Limited interoperability where the students or their parents must get to the school to make a purchase of the card before going online to enter it at the school’s portal.**
- **Prone to fraud due to generation of fake PINs, where PINs are entered without any payment being made.**

**METHODOLOGY**

**Design Methodology**

The developed scheme is based on fingerprints as the authentication technique right from the bank, where the student is enrolled at the opening of a new account with the bank and funding it or upgrading the existing account by adding fingerprint’s templates and also funds it. With a preloaded ATM card (Debit Card) the student proceeds to the school’s portal online to pay the acceptance fee as a new student using the fingerprint and the ATM card numbers which has been linked to the account number as directed on the portal. This enables the student to proceed for the payment of tuition fee after which registration can be processed. However, a returning student after completing the bit about entering ATM number and authorization with fingerprint, the system skips the acceptance fee module for him to the tuition fee payment process as explained above after which the registration process begins. The fingerprint serves as the authorization factor and it shows that the user is the card owner.

On the acceptance of the fingerprint, deduction is made from the student’s account and this enables the student to proceed for the payment of tuition fee after which he can complete the registration online.

**System Architecture**

The framework for the biometric identification for e-payment is as shown in Figure 4. The developed biometric e-payment system consists of two parts: the server and web clients. The server houses the account details, transactions and biometric details of the users at the various banks that the user may chose to transact with (BIES SERVER 1). Since the system will be accessed by the students of Ladoke Akintola University of Technology, Ogomoso, Nigeria, for payment of all necessary fees to the Institution, another server houses details of users that are known as students, both new entrants and returning students (BIES SERVER 2). The multiple “biometric bank readers” indicates that the system is independent of any bank (more than a type of bank can access the system). The web clients are points at which the students...
access both the school’s portal and in the process of payment also access the bank with the users’ ATM.

**Figure 4: Developed Architectural Framework for Biometric Identification for Secure E-payment.**

**Implementation and Results**

Hypertext markup language was employed in the Microsoft visual studio integrated development environment. The overall system was developed on the Microsoft .NET framework using Visual Studio.NET (visual C#) and MS SQL Server 2008. Third party software used is the GRTfinger SDK. The system is of two parts, namely: The Bank server’s side and the Web clients’ side for the school portal. Some of the graphical user interface of the developed system is depicted in Figures 5 - 8. The developed system was evaluated based on users’ assessment by a computer network administrator and fifty students. Three metrics which includes System Ease of Usage (SEU), System Novelty Index (SNI) and System Degree of Relevance (SDR) were used for evaluation. The response mean of the SEU, SNI and SDR were 3.89, 3.96 and 3.86 respectively on a rating scale of 1 to 5 as depicted in Figure 9. This shows that users find the system relatively easy to use, as the technical knowhow requirement to use the system is considerably minimal; it also shows that the system has an appreciable degree of integrity and it is relevant in the delivery of secured and credible electronic payments.

**Figure 5: Customer information interface**

**Figure 6: Biometric information interface**

**Figure 7: Login Creation Interface**

**Figure 8: Validation of Payment Account Interface**

**Figure 9: Evaluation Metrics for the Developed Scheme**
CONCLUSION

Evolution of means of payment through the various forms of the offline method to the online methods have presented problems of proper authentication for users, non-repudiation from the merchants to the users and adequate protection from unauthorized use of payment data at the merchant or Payment Service Provider’s end. Consequently, there is a need to proffer solution to this attendant problem of e-payment systems. This paper has detailed the development of a biometric identification scheme for electronic payment. It is believed that the developed scheme will reduce fraudulent practices in the payment of fees in tertiary institutions to a greater extent.

REFERENCES