*International Journal of Research in Engineering and Science (IJRES)*
*ISSN (Online): 2320-9364, ISSN (Print): 2320-9356*
*www.ijres.org Volume 5 Issue 3 ǁ Mar. 2017 ǁ PP.27-39*

# Implementing a Secured E-Payment Authorisation System Using Two-Factor Authentication (T-FA)

Mistura M. Usman[1],Ishola, O.B.[2]
[1]*Department OfComputer Science, University Of Abuja, Gwagwalada-Abuja, Nigeria*
[2]*Department Of Computer Science, University Of Abuja, Gwagwalada-Abuja, Nigeria*

**ABSTRACT:**Most of the current payment methods that can be used in conducting transactions on the Internet have major drawbacks either in terms of functionality, usability, costs or security. The only widely accepted way of securely and reliably authorizing electronic payment transactions is through the use of digital signatures in a public key infrastructure (PKI) framework which is computationally expensive.
This paper presents an electronic payment(E-Payment) authorization system where two factor authentication (T-FA) was utilized for the authorization of payment transactions. The description approach is based on UML notation ,the functional processes are presented as use cases, the classes that make up the system structures were presented and the system was implemented on java technology with MS ASP for the web presentation and MS SQL for the DBMS. The system enables securely authorizing payment transactions using the Internet channel.
**Keyword**:E-Payment, E-payment Security, E-payment System, PKI, T-FA.

## I. INTRODUCTION

Financial institutions and merchants are increasingly interested in automated electronic forms of payment. The reasons for this are simple; the more the payment process is made electronic, the lower the costs of both the technology to process conventional money and the actual manual processing of payments are.
One of the biggest obstacles for the on-line electronic commerce is lack of easily accessible and versatile standard means of electronic payments. The systems in place have all their limitations in terms of usability, security and accessibility, according to [1], the uses of these payment mechanisms are not totally free from problems often, customers experience delay in having access to the services provided through this electronic channels

The Internet is more and more being used for conducting commerce. Wide scale automated electronic commerce requires special protocols and systems. A large number of systems and protocols like this exist already for all areas of the e-Commerce process – browsing and selecting goods, ordering, paying and logistics. Probably the most challenging in terms of reliability and information security is payment, is however, lacking widely accepted standard protocols and methods. This is the most important reason for the fact that B2C e-Commerce hasn't grown as quickly as possible and anticipated by many people [2].

The introduction of technology based payments systems has done a lot to increase the convenience of bank's customers, staffs as well as the society at large [3]. Today, paying and receiving money between buyers and sellers are not necessarily done through raw cash. Such payment can be made using e-payment products such as ATM, internet, Point of Sale terminals (POS), Mobile money solutions and so on and so forth.

Security and privacy are the biggest factors deterring individuals interested in making on-line transaction. Most people fear giving their credit card numbers, phone numbers or addresses not knowing who will be able to retrieve that information without their consent. It is interesting to note that most people don't even give it a second thought when purchasing items with a credit card over the phone, but to ask them to do it from their PC makes them very uncomfortable. New developments in credit card security Secure Electronic Transaction (SET) are taking this fear away by adding encryption to scramble the card number so only the vendor and customer can read it. But still, many people are very concerned about internet security and are reluctant to send their credit card numbers into cyberspace [4].

## II. ELECTRONIC PAYMENT (E-PAYMENT)

E-payment systems are the instruments, organizations, operating procedures; information and communication systems employed to initiate and transmit payments from a payer to a payee and for settling payments that is, transfer money [5].

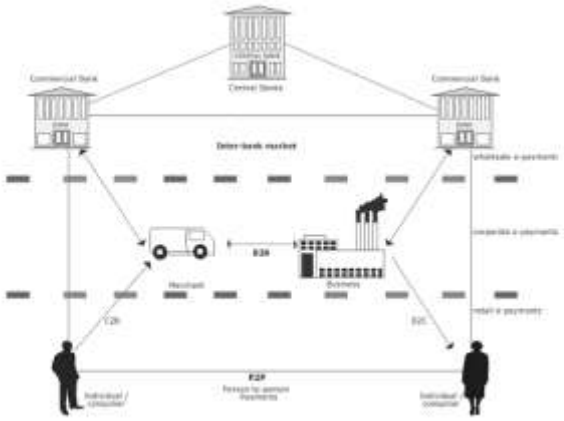

**FIG.I**Scope of E-payment Transaction [6].

## 2.1 E-Payment Channels

An e-payment channel represents the starting point where payment transaction is initiated or originated. There are the apparatus used to safely and efficiently transfer monetary value in exchange for goods and services as well as financial assets [7].

The common channels to initiate an e-payment are:

- Internet based wired system: it is a computer with connectivity to the internet, such as online shopping and payment or business procument in corporate enterprise system.
- Wireless channels: these are through contactless payments, infrared or bluetooth technology this enables broader spectrum of customer to be reached. These channels include: -mobile such as mobile phone and personal digital assistant (PDA), contactless or proximity sensors such as transponders, key fobs,attachments to key rings[6].
- Point of Sale (POS) channels: this is through the traditional face to face technology. POS can be described an electronic terminal that accepts bank debit cards and credit cards to pay by way of direct settlement to the retailers account from the customers banking or credit card provider on a daily basis for a purchases of goods or services.Modern point-of-sale systems are designed to automate all of the data that is vital to business operations. The POS system can integrate inventory and sales records with accounting and bookkeeping software. With such automated features, point-of-sale can carry out report generation tasks, which can take hours by hand, can be completed in just a few minutes [6].

## 2.2 E-Payment Instruments

Reference [6], described an e-payment instrument as a medium in which value is recognised in a payment transaction, they are the payment card such as: cash card, chip card , credit card, debit card, delayed debit , pre-paid card retail card and travel and entertainment card.
All these card payment system falls into three categories:

- Pre-paid or stored value card is a kind of the ‘pay first’ concept in which funds in the card can be decrease or increase. In order to increase, the card holder loads the card with monetary value, and a decrease takes place when payment of purchases is made It is otherwise known as electronic purse or e-wallets usually used for smaller payment also known as micropayment[6].a certain amount of money is taken away from the customer (for example, by debiting his or her bank account) before any purchase is made. This amount of money can afterward be used for payments[8]
- A debit card: is a kind of ‘pay now’ concept and it function like a charge card or cash card. It can be either pin-based or signature, the customer’s account is debitedexactly at the time of the purchase[8].

It can also be referred to as direct debit payment and enables the cardholder to have a purchase directly charged to funds on his account in a bank upon the purchase of goods or services [6].

- Credit card : the use of credit card is an example of a 'pay later' concept it give the card holder a line of credit and enable himor her to make purchases or withdraw cash up to a prearranged amount. The credit granted to the card holder is then settled at the end of a specified period either in full or partially. That is, it grants credit or access to funds to the cardholder of which the cardholder is contractually obliged to repay at a later date for the purchase of goods and services [6]. the merchant's bank account is credited the amount of the purchase before the customer's account is debited[8]

## 2.3 E-Payment Life Cycle

The payment life cycle is represented by a series of processing stages and activities as depicted in figure II [6]. There are basically three stages of a life cycle of an e-payment:

**i.** the initiation
**ii.** the processing
**iii** the notification

**Within these three stages various activities are performed.**

- The initiation stage: involves the transmission of instruction by a consumer or a corporate payer to an intermediary (usually a bank) to make a payment. This stage begins with activities such as origination of the payment instruction by the paying entity, and the capture of the payment information by the intermediary (the merchant or the payment gateway or the bank). In initiating a payment instruction, authentication activities relating to the e-payment transaction must be properly received for processing.
- The processing stage: this is the second stage of the payment life cycle it involves the processing of the payment instructions by the bank's in-house processing system or card association interchange validity and authenticating the payer prior to the authorising a debit from the payer's account and creating instructions for clearing and settlement of the account. Once the instructions have been validated and authorised, the transactions are transferred. The funds are cleared and the payee's bank account credited. The data communication link is between the intermediaries.The banks use a clearing and settlement network to transfer the funds
- Notification stage: This is the final stage of the payment life cycle it involves the advising of the payee or beneficiary of the money being received. When parties are advised of the transfer of funds, an e-payment transaction is reconciled and the payment cycle is completed [6].

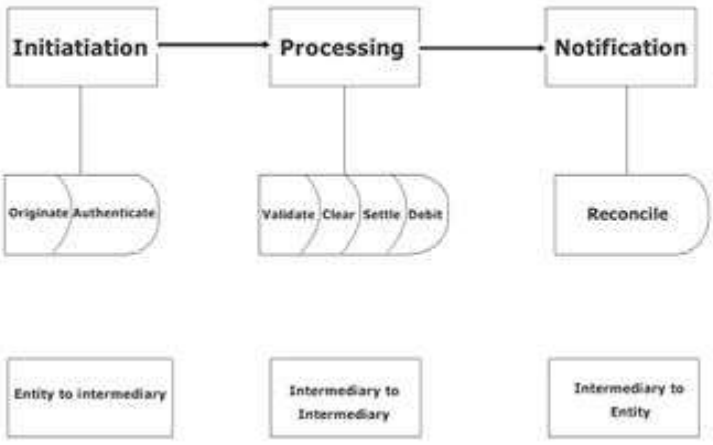


**FIG.II** E-Payment life cycle activities [6].

## 2.4 E-Payment Infrastructure

These are fundamental infrastructure that is required to implement an e-payment system. They form the essential backbone upon which financial solutions and services transmit and process payment instructions to effect transfer of monetary value amongst transacting parties.

They comprise the hardware components and the software solutions that link various payment parties along the payment life cycle. They are different types of infrastructure depending on factors such as the types of channels, the types of instrument, 'the ticket size' the frequency and the volume of transaction all influence the specific configuration of the payment infrastructure [6].

## 2.5 Types of Electronic Payment (E-Payment) Systems

Basically there are different types of E-payment system, based on methods of user identification and the payment instrument used [9].

**i. Internet Payment System**

The term internet paymentrefers to the range of services available that enable the transfer of funds directly between bank accounts, or enables internet merchants to accept and process credit and debit card payments. Most of the electronic payment systems on the Internet rely on a centralized account model, where both the payer and the merchant need to have accounts in the same institution and funds can thus be transferred directly from one account to another. Frameworks that support inter-payment provider transfers have also been defined. In centralized account scenario, the most problematic issues are naturally the ways for funding and debiting the accounts. From the payer's perspective, funding the account is normally done by transferring funds from a bank account or by a credit card to the account at the payment provider. In any case, some other form of electronic payment is normally needed for funding the account. The payment provider normally provides APIs for the merchants for debiting the payers' accounts on-line. The merchants normally get the funds out of their accounts with the payment provider via traditional automated account transfers [9].

**ii Credit Card Payment System**

This payment system is widely accepted by both consumers and merchants throughout the world, and is the most popular methods of payments especially in the retail markets [10]. This form of payment system has several advantages, such as good transaction efficiency, acceptability, convenience, mobility, low financial risk and anonymity. Added to all these, to avoid the complexity associated with the digital cash or electronic-cheques, consumers and vendors are also looking at credit card payments on the internet as one of possible time-tested alternative. But, this payment system has raised several problems before the consumers and merchants. including lack of authentication, repudiation of charges and credit card frauds. It also seeks to address consumer fears about using credit card such as having to reveal credit information at multiple sites and repeatedly having to communicate sensitive information over the Internet [10].

Credit cards have payments set against an account with a pre-agreed repayment scheme. The scheme is inherent to all account based schemes, and is thus useful to understand. Both the credit card issuers and the acquirers are members of a card association, e.g. Visa or MasterCard. Normally both of them are banks. The merchants have association with the acquirer, who provides the necessary infrastructure for the merchant for accepting credit card payments. The general schema doesn't change even if the transactions were direct debits from a bank account or a pre-paid account.Payments using credit cards can be made both when being physically present and e.g. over telephone or Internet – i.e. when the card holder and the merchant aren't colocated.

This is called a MOTO (mail order / telephone order) payment transaction. Clearly this form of payments using credit cards increases the risk borne by the merchants – the merchant doesn't have any means to positively prove the transaction actually took place if the cardholder decides to repudiate it afterwards [11].

**iii Electronic cash systems**

Reference [12], most of all financial transactions are paid with cash, even when the value of these transactions are quite low. Electronic cash (e-cash) systems provide an electronic analog for physical cash. In short, a bank issues, and customers use e-cash to purchase goods or services from merchants that accept this form of payment.Three parties are involved in an e-cash system, they are: the issuing bank, the customer and the merchant. The customer and merchant have accounts with the samebank. However, the customer and merchant may also have accounts withdifferent banks. In this case, the banks are referred to as the issuer and the merchant's bank is acquirer. The customer withdraws some e-cash. He or she the issuer, transfer somemonetary value from his or her account to the e-cash issuing bank.Following this value transfer, the bank issues and sends a correspondingamount of e-cash to the customer. The customer in turn,storesthe e-cash locally. the customer uses the e-cash to purchase some goods or services and transfers the corresponding amount of e-cash to the merchant the merchant redeems the e-cash he or she has just received from the customer the merchant may also transfer the e-cash to his or her bank (the merchant's bank), and this bank may, in turn, redeem the money from the e-cash issuing bank. In this case, the issuing bank transfers money to the merchant's bank for crediting the merchant's account [12].

## III. ELECTRONIC PAYMENT(E-PAYMENT) SECURITY

There are different ways of securing online transactions which include:

### 3.1 Secure Socket Layer (SSL)

Secure Socket Layer (SSL): Thisis a session layer protocol that was developed by Netscape for securedexchange between a client and a server [13][14][15].

It is a standard for Internet security and implementedin most browsers and by most web servers. SSL is designed to provide securityfunctions independent of the application. Since it works at a higher layer than IPSec,identities can be resolved to the level of an individual. By the same token,SSL by itself cannot prevent an observer from knowing who is communicating

since IP addresses will be added at the lower layers.SSL designates two types of participants: clients and servers. Clients alwaysinitiate a communications session with a server. The server is required to provideauthentication information to the client (a certified public key) if requested. Theclient, however, is not required to provide a certified public key to the server. Ifthis is the case, the applications using SSL may require some other means of authenticatingthe user (such as a user ID and password/PIN). Once the session hasbeen negotiated, SSL provides a secure (encrypted) and authenticated communications channel between the client and server. So with SSL, even though the information is protected, an intruder can stillglean information about the participants in a transaction. SSL is relatively fast and provides transparent security to the user. It however, does not provide the mutual authentication and digital signature capacity that are required for a truly secured transaction[16].

### 3.2 Secure Electronic Transaction (SET)

The Secure Electronic Transaction (SET) is a protocol developed by MasterCard and Visa for secure bankcard transactions [14][17].

According to Gordon Agnew the Secure Electronic Transaction, SET, protocols were developed to overcome the possibilities of fraud in credit card transactions over the Internet.SET provides a high level of security and privacy for the participants. This is mainly due to the extensive use of public key certificates and digitally signed and verified messages

SET defines two major interfaces – the one between the cardholder and the merchant and that between the merchant and the acquirer (called the payment gateway in the SET context). SET relies on a certification hierarchy, based on the X.509 PKI. Original SET makes use of client software (SET wallet) installed on each cardholder's PCs. The software is primarily used to perform digital signing and authentication operations as well as the key and certificate management. This has several important implications. Trust in the system relies on the deployment of a full public key infrastructure. If SET is to be used on a wide-scale basis, certificates have to be issued to all users. This is an enormous and expensive task. On the other hand if the PKI is not in place, then SET will not be used by a largenumber of users. Public key operations (signing/verifying, wrapping/unwrapping) are computationallyintensive, and certificates are large in size and require significant bandwidth to transmit [12].

SET is a payment protocol, but very complex, multiple servers need copies of all certificates. No one uses Set the reason for this fact is that the SET protocols are complex and difficult to implement. Furthermore, the deployment of SET requires an existing and fully operational PKI which is hard to achieve [12].

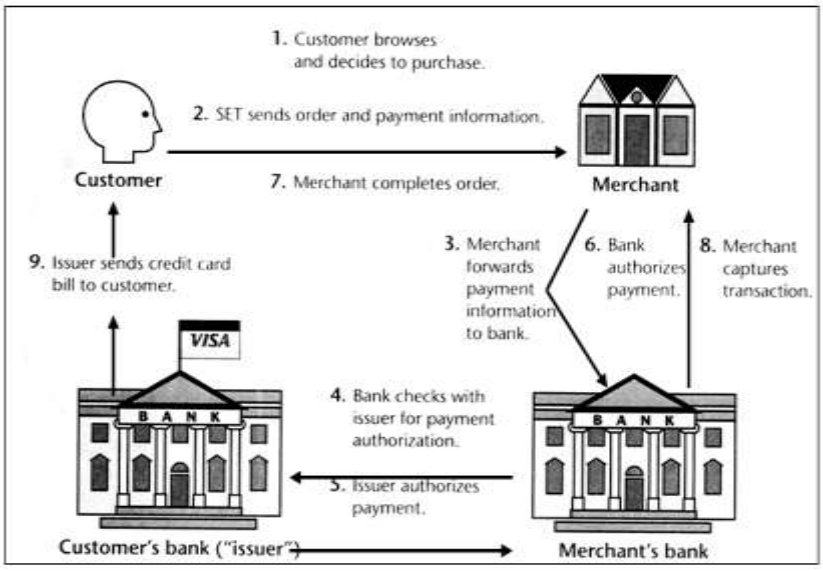


**FIG.III** Secure Electronic Transaction (SET) flow [18]

### 3.3 Card verification value (CVV)

As an intermediate solution to the problem associated with PKI deployment, Visa International and MasterCard both use the last three digits of the number that is printed on the back of each credit-card as a proof of physical ownership. Visa International is using the term card verification code (CVC) to refer to this number, whereas MasterCard is using the term card verification value (CVV) [12].

CVV is an authentication procedure established by credit card companies to further efforts towards reducing fraud for internet transactions. It consists of requiring a card holder to enter the CVV number in a transaction time to verify that the card is on hand. The CVV code is a security feature for "card not present" transactions (e.g., Internet transactions), and now appears on most (but not all) major credit and debit cards. This new feature is a three- or four-digit code which provides a cryptographic check of the information embossed on the card. Therefore, the CVV code is not part of the card number itself.

The CVV code helps ascertain that the customer placing the order actually possesses the credit/debit card and that the card account is legitimate. Each credit card company has its own name for the CVV code, but it functions the same for all major card types.

The back panel of most Visa/MasterCard cards contain the full 16-digit account number, followed by the CVV/CVC code. Some banks, though, only show the last four digits of the account number followed by the code. To aid in the prevention of fraudulent credit card use, we now require the 3 or 4 digit code on the back of your credit card. This is however, subject to replay attack.

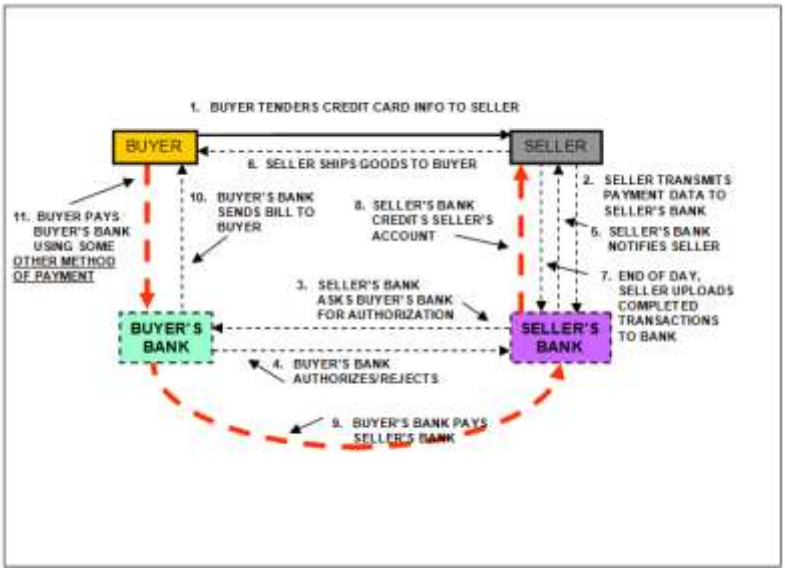


**Fig. iv.**Credit Card Transaction Flow [18].

## IV. DESIGN FRAMEWORK/ CONCEPT

**Two Factor Authentication (T-FA)**

Two factor authentication, also known as( T-FA)/ 2FA or two step verification is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication in which an extra form of security are required, not only a username and password but also something that only the user has on them a kind of piece of information only they should know or have immediately to hand - such as a physical token [19].

Using a username and password together with a piece of information that only the user knows makes it difficult for any intruders to gain access and steal that person's identity.

### The Design

The system is to enables authorization of electronic payment transactions using T-FA. The need for the system arises from: 1. the issue of fraud in credit card payment which the existing system as not address because customer are not properly authenticated, and 2., the most feasible way to achieve secure payment transactions seems to be through the use of a public key cryptography based scheme which is computationally expensive.

The Figure v, presents the E- payment authorisation system concept

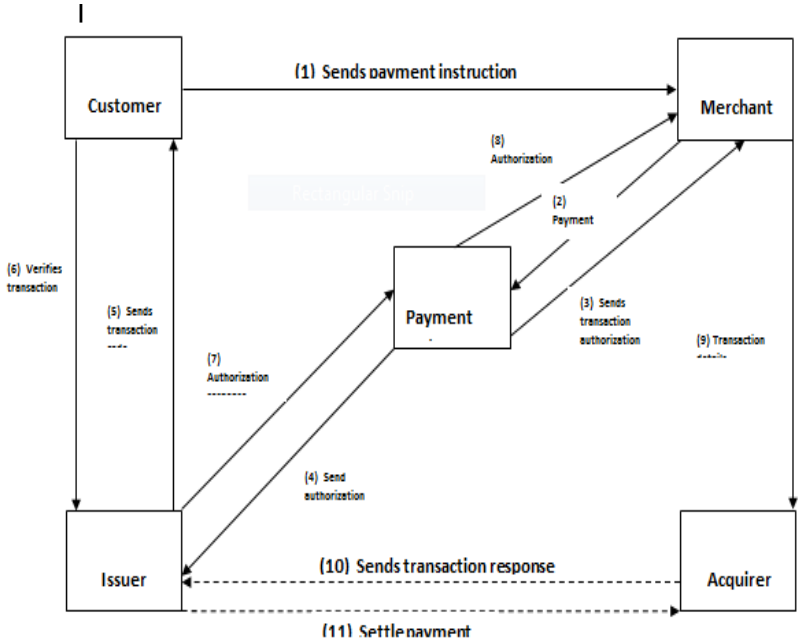


**Fig. v** E- Payment Authorisation System

**The diagram can furtherbe described in thefollowing process steps:**

1. Customer gives to merchant payment instruction
2. Merchant send payment request to payment system
3. Payment system sent transaction authentication code to merchant
4. Payment system sends payment request to issuer for authorisation
5. Issuer sends transaction detail including an authentication code to customer transaction account
6. Customer is verified by the issuer by supplying the transaction detail with the four randomly generated position challengers.
7. Issuer verifies this detail, sends authorisation/cancellation to the payment system.
8. Payment system sends payment request response to merchant
9. Merchant completes the order.
10. Merchant sends transaction detail to acquirer to capture the funds.
11. Issuer settles acquirer

Actors and Use Cases

**The five core use cases used by the system are:**

E-Registration
Payment request creation
Payment request verification
Payment authorization
Payment Request Status

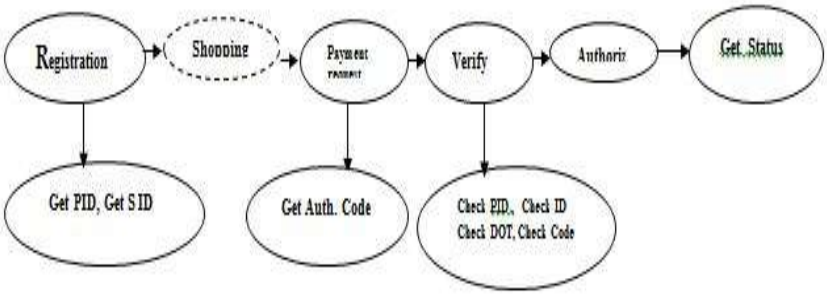


**FIG. VI** The system process flow

Putting these five use cases together in the sequence completes an E-payment transaction authorisation. The use case of Shopping is not included in the scope of the system. Naturally, the customer is expected to go for shopping before payment can be made. This should be by the merchant system will have implemented that. Figure VI illustrates the sequential relationships between the use cases in form of a process chain. In the figure, the ones in bold denote use cases implemented by the system. The dash is implemented by external system.

4.2.1 Actors

There are three main actors that participate in the use cases: the customer the merchant and the issuer. The customer has three roles, registration, shopping and the payment verification. The merchant also plays two roles, create the payment request and confirms the status of the payment request before delivering the goods the issuer plays the role of customer verification and sending authorisation to the payment system. There are four different systems interacting in the process chain. The systems are:

E-Payment System

Registration System

Merchant payment request System

Verification System

The role of the E-payment system in relation with the other is that of an integrator, the payment system co-ordinates the payment transaction processing between the actors and the systems. The Figures illustrates the relationships of the actors and systems.

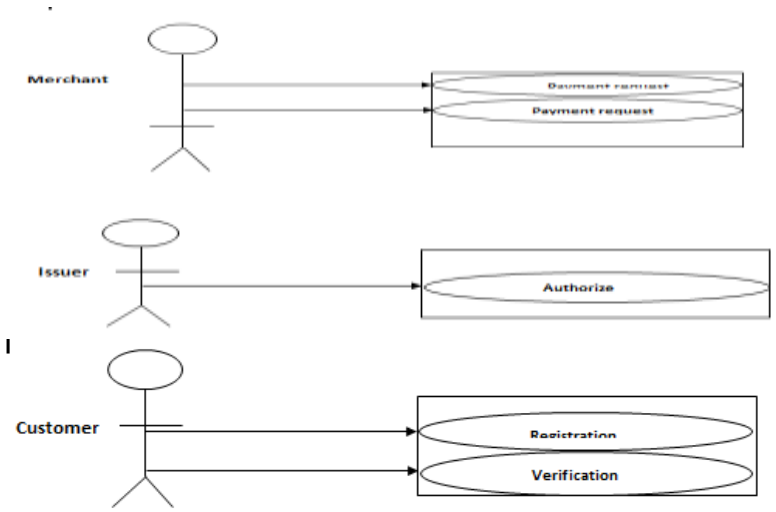


FIG. VII. Actors and Use Cases

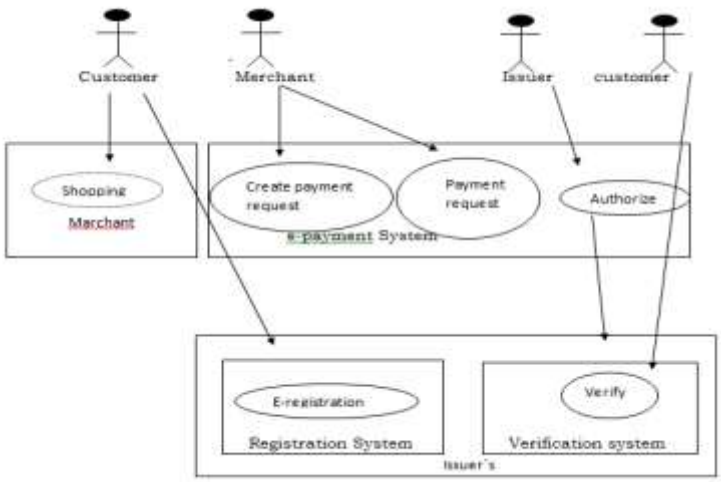


**Fig.** viii The Use Case Diagram for the System

**4.2.2Use Case**

The five individual core use cases are described in the following subsections.

Use Case: E-registrationThe customer has to register an account with the E-Payment system before shopping or make purchases on such account.

**Use Case: Payment Request Creation**

After the customer has selected the goods and proceeded to the payment phase in the merchant system, the merchant system creates a payment request data entity and submits it to the payment system. Each individual payment request entity has a unique identifier both in the merchant system and the payment system. Those identifiers can be used to reference the individual requests in later stages of the transaction. The Payment System registers the payment transaction into persistent data storage and generates authentication code for the merchant.

**Use Case: Payment Request Verification**

When the merchant has registered the payment request into the payment system, the issuer verifies if such customer exist, and if the customer actually made such transaction, the customer is then throw a challenger to respond ( the SID, PID, transaction code, DOT, transaction S/N) in the verification system.

Use Case: Payment Authorisation

If a positive acknowledgment is received from the verification system, authorisation is sent to the payment system, which the merchant confirms using the authentication code generated during the payment request.

**Use Case: Payment Request status**

The merchant queries the payment request status from the payment systemby using a ViewStatusRequest. The response is sent as a paymentStatusResponse.The core of the E-Payment System is the payment server. It co-ordinates the transaction and the work flow in the system. It also binds together the different systems involved.

**4.3 System Structure**

In figure ix, the core of the system is illustrated in UML form.

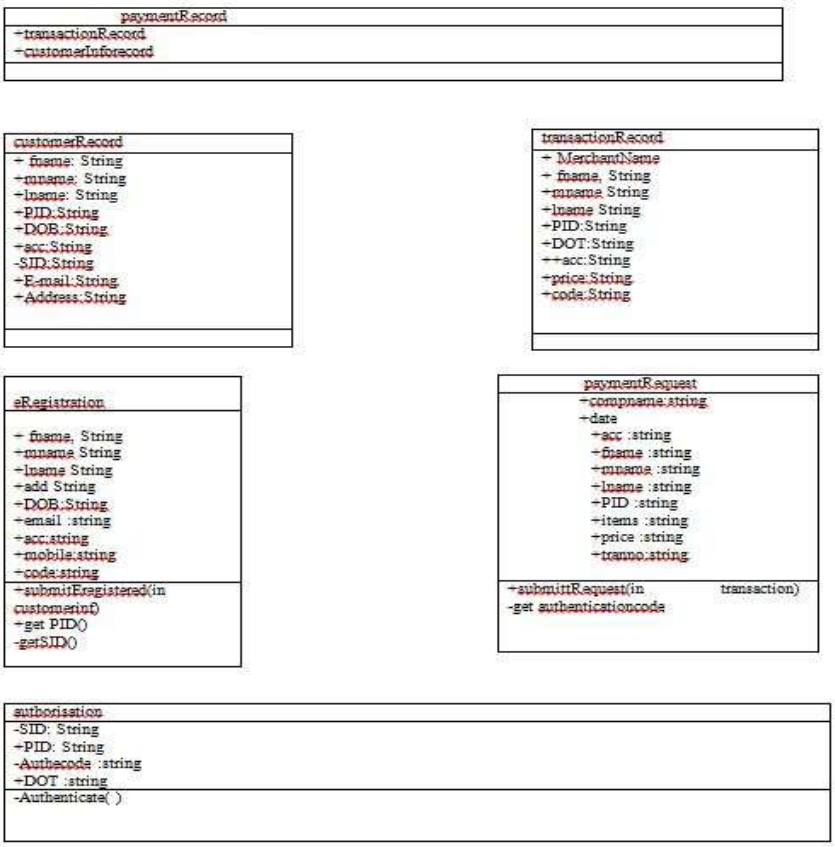


**FIG. IX**The central classes of the System

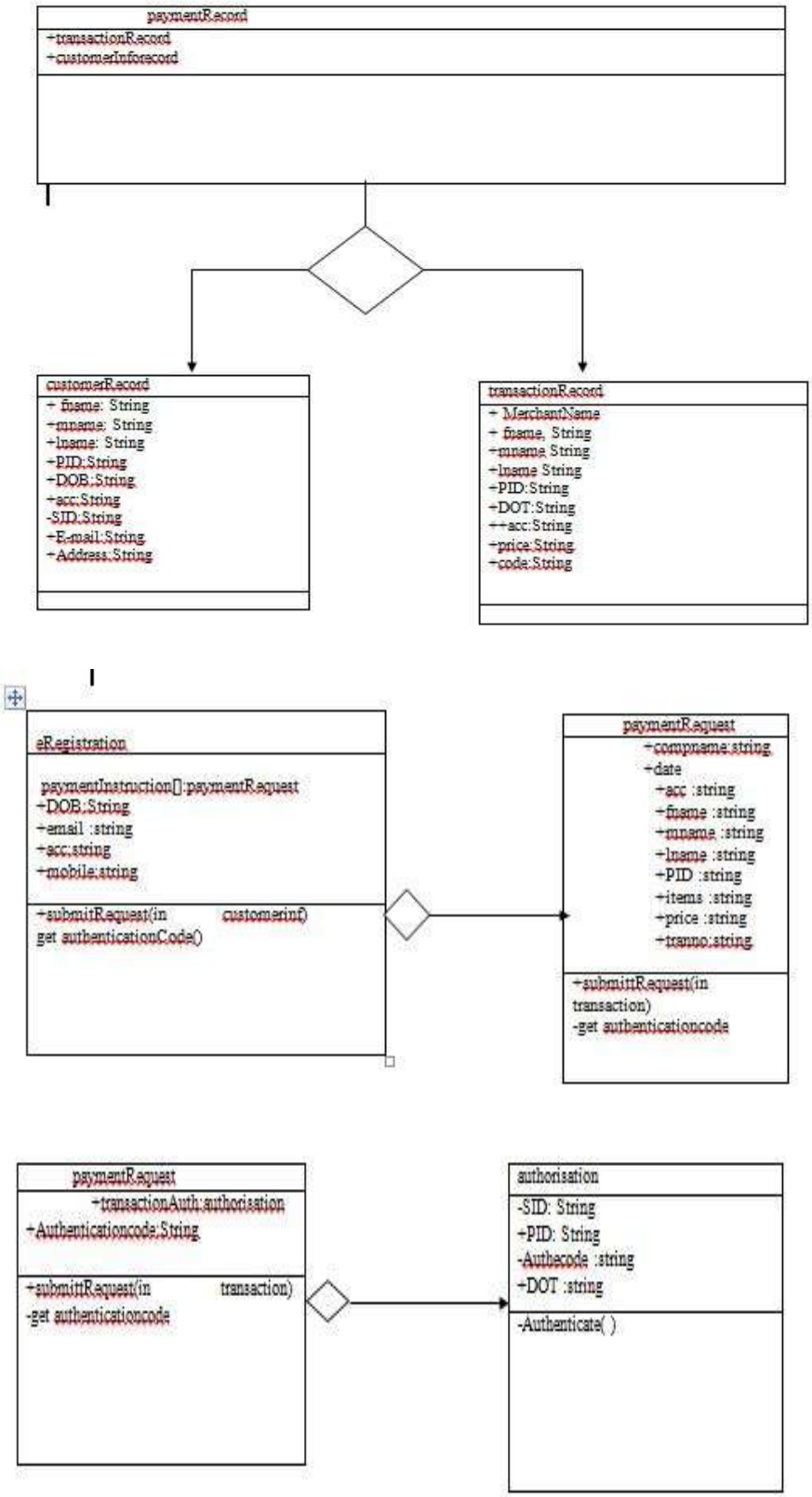


**FIG. X** The Relationship between classes

E-Payment System As Shown In Figure XI Below, IntregrateThe Whole System


**FIG.XIThe**E-Payment System

**E-registration**

The Customer registration as shown in figure xii, allows the customer register an account with the E-Payment system before shopping.

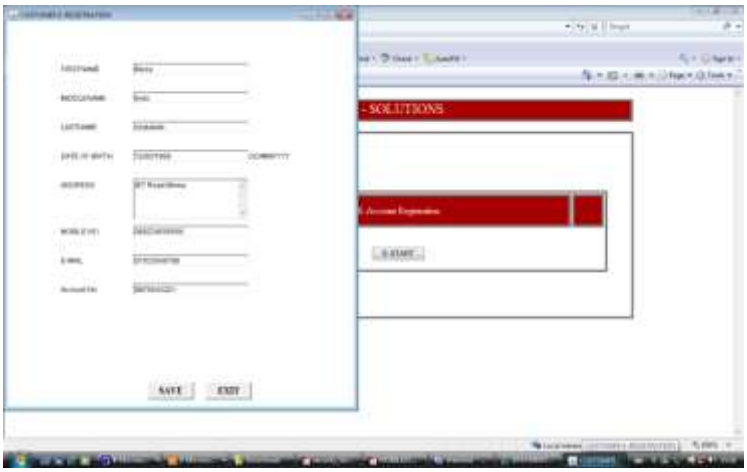


**FIG. XII**Customer E-Register Form

**Create a payment request.**

The merchant should be able to create a payment request with all relevant details of the payment, as described. When a merchant submit a properly formatted payment request, the payment request is accepted else Payment request is rejected, as shown in Fig.xiii and Fig.xiv


**FIG.XIII**Create a payment request.

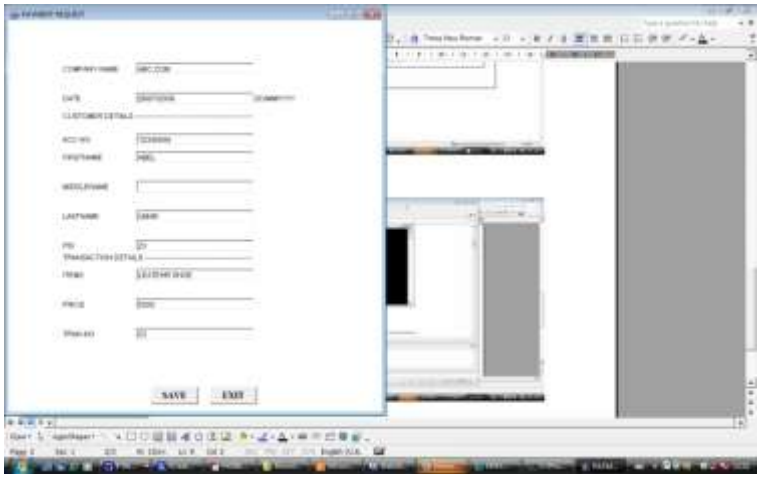

**FIG.XIV**payment request creation with payment details

Payment Request Verification/ Authorisation

The issuer verifies the customer by throwing a challenger (SID, PID,DOT, code) if valid a positive acknowledgement is sent to the payment system transaction is then authorized.

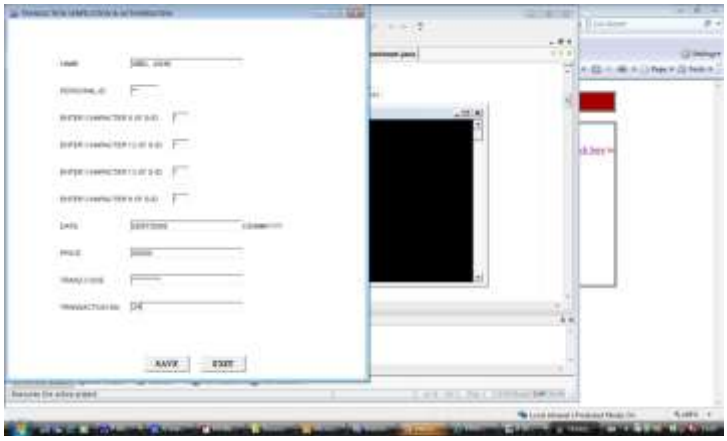

**FIG.XV.**Payment Request Verification/ Authorisation

Payment Request Response

The request response as shown in figure xvi, allows merchant to check the status of payment requestthat was sent.


**FIG. XVI** Payment Request Response

## V. CONCLUSION

Generally, the only way to properly carry out authentication and authorization in the digital Media is through the use of public key cryptography. To make use of public key cryptosystems in a large scale is through setting up a public key infrastructure. Which is associated with a number of problems such as: usability anduser friendliness.

This paper presents an electronic payment authorization system where T-FA was utilized for the authorization of payment transactions. – the system is easy to use and available regardless of time, place and whether you are doing business over the counter at a supermarket or on the Internet. The description approach is based on UML notation – the functional processes are presented as use cases, the classes that make up the system structures were presented and the system was implemented on java technology with MS ASP for the web presentation and MS SQL for the DBMS. The system enables securely authorizing payment transactions using the Internet channel.

## REFERENCES


[1]. Olakah, 2012. Benefit, challenges and prospects of a cashless economy. Journal of The Chartered Institute of Bankers of Nigeria, Lagos. Jan-March: 11.

[2]. Mobile Internet Established players gain most out of mobile Internet, Mobile Internet,Vol. 2, No. 2 2000.

[3]. Kelvin, O., 2012. Mobile money for financial inclusion.Journal of Macro Finance, Africa, Nett, Lagos, 4: 14.National Bureau of Statistics, 2012. Annual Statistical Reports, 13: 11.

[4]. Scott, R. (2006) Description and Evaluation of Different Types of E-Payment Systems http://www.tec.informatik.uni-rostock.de/IuK/lehre/settlement - seminar/InternetPayment.html

[5]. Imafidon, A., 2013. Challenges of E-banking and payment systems in Nigeria. Journal of The Chartered Institute of Bankers of Nigeria, Lagos, April-June. pp: 39.

[6]. Tan, M. (2004): E-Payment: The Digital Exchange Singapore University Press. Singapore Pg 3-18.

[7]. Oloruntoyin, S.T. and D.O. Olanloye, 2012. The role of information communication technology (ICT) on national development.International Journal of Economic and Development Issues, 1&2(11).

[8]. O'Mahony, D., M. Peirce, and H. Tewari, Electronic Payment Systems forE-Commerce, Second Edition, Norwood, MA: Artech House, 2001.

[9]. Tudor, R. (2001) E-Payment, cards,cellphone payment or biosystem what to use ECJ research <www.ecommercejournal.com>

[10]. Laudon, C. Kenneth and Traver, Carol (2002), E-Commerce, New Delhi: Pearson Education.

[11]. O'Mahony, D. ,Peirce, M.andTewari, H., (1997): Electronic Payment Systems for ECommerce, Artech House, United States, , page 245.

[12]. Oppliger, R. (2003): Security Technologies for the World Wide Web second edition Artech house Norwood Pg 249-264

[13]. Elgamal T., Treuhaft J., Chen F., "Communications on the Intranet and over the Internet" http://home.netscape.com/newsref/ref/128bit.html#SSL [accessed 22-12-2016].

[14]. Freier A., Karlton P., Kocher P., "The SSL protocol", version3.0, Internet draft, 1996. http://home.netscape.com/eng/ssl3/ssl-toc.html.

[15]. MasterCard and Visa, Inc.(1997), SET Secure Electronic Transaction specification book 2: programmer's guide, version 1.0 [Online], 1997. http://www.setco.org/set—specifications.html. [accessed 17-12-2016].

[16]. Gordon Agnew Secure Electronic Transactions:Overview, Capabilities, and Current StatusA&F Consulting, and University of Waterloo, Ontario, Canada Payment technologies for E-Commerce Kou, w.(Ed) 2003 IX 334 p http://www.springer.com/978-3-540-44007-9

[17]. Visa International and MasterCard (1997). Secure Electronic Transaction (SET), version 1.0.31, 1997. http://www.visa.com/cgi-bin/vee/sf/set.

[18]. Shamos, I.M. (2004): Electronic Payment Systems www.ecom.cmu.edu

[19]. Securenvoy - what is 2 factor authentication?". Retrieved 24-12-2016.