International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-3, Issue- 5, May 2017
ISSN: 2395-3470
www.ijseas.com

A Secure Micropayment System

Musa M. O.[1], Asagba P. O.[2]
[1] Depart. of Computer Science,University of Port Harcourt, Port Harcourt, Nigeria
[2] Depart. of Computer Science,University of Port Harcourt, Port Harcourt, Nigeria

Abstract

Micropayment system is one of the research areas in electronic commerce. It's a system that allows for the payment of very low cost items online. For any commercial system to thrive, trust and security of the system must be guaranteed and security is the basis for trust. Trust in a payment system is a pre-condition for using the system. In this paper, we present the challenges and the security concerns of micropayment systems and the security protocols used to check them. We also designed a web-based micropayment application implementing the security protocols discussed and also allows fund transfer among registered users of the application. The object-oriented methodology is deployed for the developmental process of the application. Java programming language was used in implementing the design. Servlets and Java Server Pages (JSP) were used to implement the web pages. The Database was implemented using MySQL server. The security protocols applied in the application are Cryptography, Authentication and Authorization. We developed an online Stock Photo Application with a recharge pin payment system incorporated into the application

***Keywords**: Security, protocol, cryptography, e-commerce, micropayment*

1. Introduction

The internet began as a result of connecting several super-computer sites in the US with one another so that if any of the sites was destroyed by a nuclear explosion, or malfunctioned, the other sites will continue to function. It was a defence force project in the 1960s call Arpanet. Arpanet was a huge success and it became obvious that it is possible to have geographically dispersed network of computers. Other organizations (Universities, government parastatals and Corporations) with large computer sites began to join this network. As the network grew, its benefits became obvious. Soon organizations outside the US and other countries joined and the network grew larger. Arpanet became an **international network**, hence its name – **internet.**

Advertising, buying and selling of goods and services, and transferring of funds over the internet are some of the many benefits of the internet. Buying and selling of goods over the internet is know today as 'Electronic Commerce' (e-commerce) while transferring of funds over the internet is known as 'Electronic Payment' (epayment) or Online payment.

The conspicuous advantages of e-commerce include its around-the-clock availability, the speed of access, the wide availability of goods and services for the consumer, easy accessibility, and international reach. Its perceived downsides include sometimes-limited customer service, consumers not being able to see or touch a product prior to purchase, and the necessitated wait time for product shipping.Online payment is the foundation for e-commerce. In an ideal electronic commerce, all the steps of a transaction could be performed over the internet. Information could be intercepted and tampered easily in an open network. Hence, how to build a secure and efficient environment for electronic payment is a key issue in electronic commerce development.The issue of security is of immense concern (Asagba et al, 2003).

Generally, there are two types of electronic payment systems; Macropayment and Micropayment. The difference between them is the amount of money they transfer. Macropayment allow transfer of larger amounts of money while micropayment allow transfer of only very small amount of money, say a few cents or a few naira. The need to have different payment systems for large and small payments arose from the fact that the cost of securing a payment system can be more expensive than the expected profit from the

system. In this case, a loss is made and there would be no need for such a system.

Of the two types of payment systems, the security requirement of macropayment system is more rigorous. To date, public key cryptosystem is commonly used in macropayment for authentication and encryption. Besides public key cryptosystem, macropayment schemes use on-line broker activities to detect double spending prior to acceptance of a payment by the vendor. Both the vendor's broker and the customer's broker connect to verify the transaction amount and perform online verification and redemption.(Mini-Shiang and Pei-Chen, 2006).

The computational and storage costs of micropayment schemes are suitable for small payments. For example, purchasing a web page or downloading a paper. Compared with macropayment scheme, the computational times of micropayment schemes is less because it uses the one-way, collision-resistant hashing extensively but not public key cryptosystem. As a rough estimate, hashing is approximately about 100 times faster than the RSA signature verification, and about 10,000 times faster than RSA signature generation (Rivest and Shamir, 1996).

The security of micropayment schemes is apparently not as efficient as that of the macropayment schemes. However, if a micro-payment scheme is designed so that a customer only loses a few cents when his transaction is tampered with and the cost of counterfeiting a coin is either computations or policies are higher than the value of the coin, then the security is considered to be adequate (Chi, 1997). The aim of micropayment scheme is to provide a decent level of security for transactions with more economical time and storage requirement.

2. Micropayment

Micropayment is an electronic commerce transaction of very low volume. It may refer to charging just a few cents or few dollars for digital contents online.In general, we use the word micropayment to describe small-valued transactions, say a few dollars or less. In most cases, micropayments are intended for use with online delivery as well: for example, fifty cents for read-only permission for a magazine article (Treese and Stewart, 1998).

Paypal an email based e-payment system, defines a micropayment as a transaction of less than 12 USD while Visa prefers transactions less than 20 USD, and though micropayments were envisioned to involve much smaller sums of money, practical systems to allow transactions of less than $1 have seen little success.Since it is not possible to make payments of such very little amount using bank cards, micropayment systems are a good means for such sites that want to go micro.

Early Micropayment systems include Millicent, Netbill, and IBM micropayments. Recent micropayment systems include Paypal, Netpay, M-coin, Payclick, Zong and other crypto currency used recently.

2.1 Security Concerns of a Micropayment System

Security prevents and detects attacks on a payment systems and fraud attempts, and protects sensible payment information. It is needed because attacks and attempts for misusing a payment system to commit fraud on the Internet are common (Abrazhevich, 2004). Security is to a certain extent a subjective concept, and felt differently by each user. Users often interpret security as an equivalent for guarantee: customers feel secure if they receive the paid products, while merchants feel secure if they get the money for the delivered products. The main security concerns are the non-repudiation, authentication and authorization, data integrity, and confidentiality (MPF, 2002).

Non-repudiation: Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated(TT,2017).

Authentication; Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. (TT, 2017).

Authorization;Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.

Data integrity; The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity is imposed within a database at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines.

Confidentiality; Data Confidentiality is whether the information stored on a system is protected against unintended or unauthorized access. Since systems are sometimes used to manage sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data. Accordingly, this is an integral component of Security. (Hitachi, 2017).

Today transparent security techniques are used. Take, for instance, the authentication techniques, which in general use an e-mail address and password combination (e.g., Way2Pay), user name and password (e.g., WebCent), an account identifier number (e.g., Micromoney, PaySafeCard), an account identifier and pin code (e.g., Teletik, SafePay). Merchants are transparently identified for each payment by these systems based on their account or registration number (issued by the systems as well).
The majority of systems use the de facto HTTPS web protocol, which provides safe data transmission. This protocol requires authentication of the communicating parties, encrypts and decrypts data. Customers have no trouble using this protocol, because all browsers support HTTPS. Current systems and their MPSOs are obliged by law to generate audit information. Such information can be used to prevent non-repudiation, and trace back and verify payments in case of complaints or fraud attempts.

2.2 The Levelof Security Neededin Micropayment Systems

Micropayment systems only need lightweight security techniques because the risks are manageable due to the limited value per transaction. The earlier systems used security techniques that oscillated between no security at all and heavy security techniques, so they were either exposed to attacks or too expensive and too difficult to understand for their users. Current systems use adequate authentication, identification, non-repudiation techniques, and secure communication channels, which increase the security felt by users. Because of the audit support, customers and merchants are guaranteed that they will receive the paid products (according to their expectation) and the transferred money, respectively.

2.3 Micropayment Security Risks

Below are some of the risks often considered in the design of any micropayment system;
Credit Abuse; an account is used to make repeated payments without intention to pay.
Counterfeiting; a fake payment order is constructed.
Unauthorized Withdrawal; The broker (or an employee) makes an unauthorized withdrawal from an account.
Purchase order modification; A customer issues a payment order intending to purchase one set of goods but the order is intercepted and modified by a third party.
Failure to Credit Payment; the broker debits the customer account but does not credit the vendor account.
Double Spending; a payment instruction is used twice, either by a customer, a vendor or a third party.
Denial of Service; A customer or vendor is denied use of their account.
Repudiation; A party may deny making a payment.
Credit liability; where a customer is extended credit liability must be controlled.
Failure to Deliver; A vendor may accept payment but fail to supply the advertised goods.
Framing; a party is able to convince another that a third party acted in bad faith.

2.4 Security Measures Employedin This Software Development Project

The following are some of the security measures employed in this software development project;
Auditing; involves monitoring of user activities while online by the Administrator. This helps to track fraudulent activities by users and such accounts are blocked.
Password Based Authentication; not everyone that visits the site has access to making purchases, users or buyers must be registered with valid Email addresses as their user names and the correct passwords must be entered to make purchases. This helps to authenticate users.
Encryption; Passwords are encrypted with 128bits AES (Advanced Encryption Standard) Encryption.

Even the Admin has no access to user's passwords in a case where the application is hosted on a foreign server. Passwords are encrypted before being stored in the data base.

Role Based Access Control; Access to the web pages are role based. There are pages accessible only by the Administrator (for instance, the Audit Log) for security and management purposes.

Password Complexity Verification; Acceptable password during user's registration must comply with certain rules: a minimum of 8 characters, at least a number, a special character (#, $, *, @, !, &). It must not contain any words related to the username or surname.

Login Attempt; Accounts automatically gets locked after three wrong login attempts. Only the Administrator can resolve a locked account.

Roles/ Privileges of the Administrator

- Can view Audit logs
- Unlock user accounts
- Configure password expiration periods
- Can recover passwords; users with locked contacts the Admin, the admin enters the user email in the password recovery page, the software confirms the validity of the email and the password is automatically sent to the user's email address.
- The Admin can view all transactions made.
- The Admin generates pin for making purchases which is sent to the user email after payment is confirmed.
- Uploads stockphotos with their price tags. Uploaded images appears as thumbnails on the Home page. Once a stockphoto is uploaded, an image entry is created in the database with the details of the image. A thumbnail is created from that image. The thumbnail and the image itself are stored in the image entry.
- The Admin is also able to view uploads.

Roles/ Privileges of the User

A user is able to upload a purchased pin; if loaded pin are valid, then the monetary value of the loaded pin is added to the user's available credit. If invalid pins are entered in a row, after three failed attempts, the account is automatically locked. Users are able to view only their own transactions.

3. Design of the Micropayment System

The design involves the synthesis of the components necessary for use in the development of the system. The design serves as a direction to all the necessary components and there flow of operations required in the system implementation.

In the design presented in figure1 the user shops for items from the displayed items in the merchant shop. Some on the items desired are selected into the shopping cart from where payment are made to the merchant through the merchants payment gateway. During the payment the customer gets charged some amount which usually does not go to the merchant but rather to the payment gateway provider. The payment made gets to the merchant bank account or wallet depending on the type of payment. If the payment is fiat currency it gets to the merchants Bank account but if it is crypto currency it gets to the wallet.

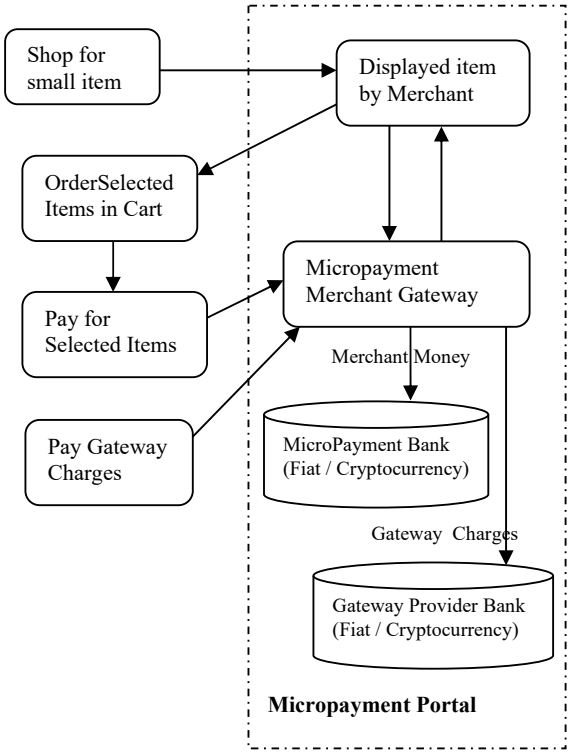

Fig 1: Micropayment System Design

On the other hand the charges get to the gateway provider that provided the payment platform from

where the payment is made. The charges often are the challenges that micropayment suffer mostly from the the hand of gateway providers and payment platforms.

3.1 Transaction requirements of the Stockphoto Micropayment Software

It is not everyone who visits the site that places order or purchase photos. Certain requirements must be met by the site users.
These requirements include the following;

- Users must register with their Surname, Name, valid Email address and password.
- Users must login with their user name (i.e their email address) and password.
- Users are required to buy their pins for making purchases at the banks specified.

Users load pins and can now make purchases.
In the figure the Administrator is contacted via the contacts on the homepage in cases where there are difficulties.

- The user is presented with a download of the full stockphoto. Else, an error message is displayed for insufficient credit transactions.
- If the transaction is successful, a role is added to the transaction table.
- The transactions are visible to the user and administrator.

4. Implementation and Program Output

The selling of photo is a good example of an important service that may require micro payment and it have been selected as a Use Case for the implementation of the micro payment system in these paper. The user or customer loads the site and make a request after selecting a desired picture from the group of pictures displayed on the site. The system then offer a page that is linked to the system gateway from where payments can be made. The merchant gateway pays the merchant fee to the merchants account integrated to the payment gateway. In figure1 the Stock Photos screen shots of the program implementation can be clearly seen.

Users are required to buy their pins for making purchases at the banks specified.
Users load pins and can now make purchases.
In the application the Administrator is contacted via the contacts on the homepage in cases where there are errors or difficulties.

All thumbnails of stockphotos and their price tags are displayed as well as a link to enable a user make purchases are displayed on the Home Page.
The thumbnail is a reduced picture quality.
Once a user clicks on the “Buy Now” link, if the user is not logged in, he is prompted to do so.
User’s credit balance is checked and the amount on the price tag of the picture being purchased is deducted.

The user is presented with a download of the full stockphoto. Else, an error message is displayed for insufficient credit transactions.
If the transaction is successful, a role is added to the transaction table.
The transactions are visible to the user and administrator.

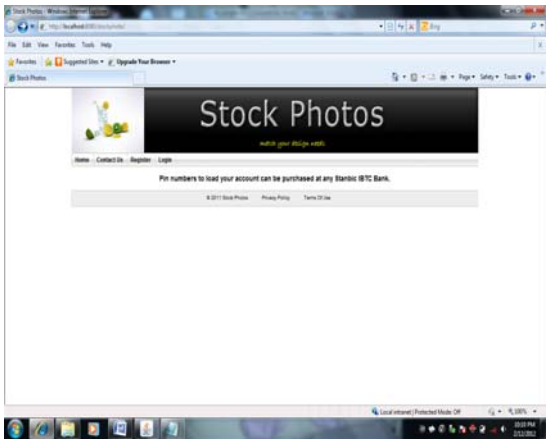

Fig 1; Home page

On opening site, the home page as shown in figure 1. A viewer is given options to either register, login and has access to the Administrator’s contacts. Information on where to purchase pin to load accounts is also on the screen.

If the Administrator logs in, the Audit logs are automatically displayed, he is privileged to view User Accounts, Transactions, Manage Images and Log Out as shown on the screen shot below;

4.1 The Audit Logs

The system also provides a page that can be used for audit log to view transactions once they are carried out on the system. In figure 2 a sample audit log of the system is provided. The page clearly show the serial number, log activity, date and other useful information on the log. The administrator will find the log useful in understanding the detail interaction and other activities going on in the system and when error occur it can be easily traced and fixed.

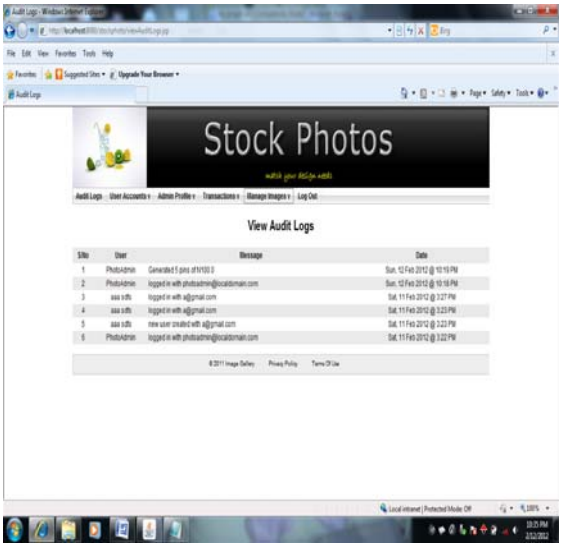

Fig 2: Audit Log Page

If a client logs in, he is privileged to make purchases, view his own transactions and profile, and manage his credit and logout. It is from this page that the user can check for the pictures that he may desire to purchase. If the picture he desire is not available in that page, the user can also navigate to the next page to check for the availability of some pictorial items.

Selected items can be made ready for payment so that the system shopping cart gets their price ready for the client to make payment to the merchant. In most cases the payment may be placed in the site where the link to the gateway is made. In other cases payment is made directly on the site of the payment gateway provided which is usually more secured than the merchant sales or display site.

In Figure 3, the system show that some pictures are displayed on the site for clients to select.

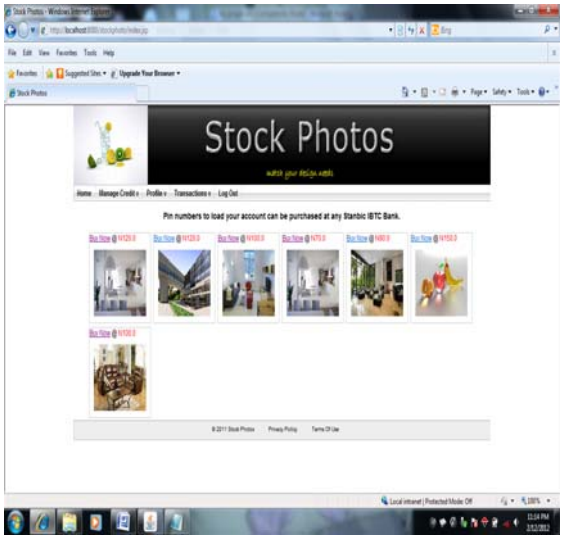

Fig 3: Displayed Photo items on site

In figure 4 the credit management page is illustrated where the client is expected to use in pin loading and other related activities. If a client chooses to manage Credit, then he has the options to load pin, account Balance and Transfer Credit as shown in figure 4. The information in the site used in managing clients account is feed from the merchant gateway the information provided accrue from the payment method used by the gateway in transacting in the system whether it is card payment, cryptocurrency or other form of payment.

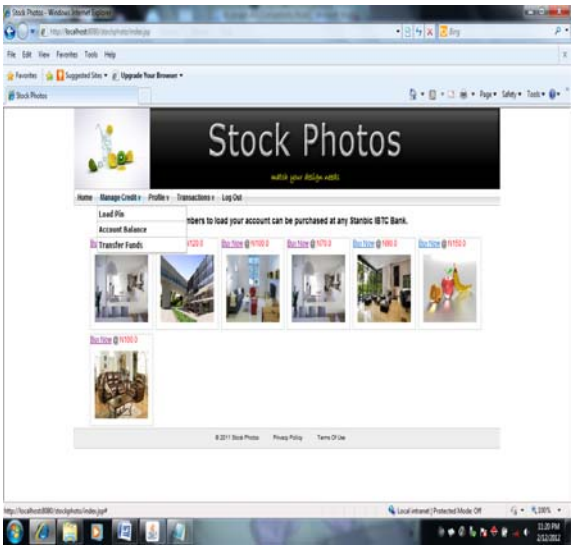

Fig 4: Credit Management Page

If the transfer funds option is clicked, the recipient's Email and the amount to be transferred are requested as seen in figure 5.

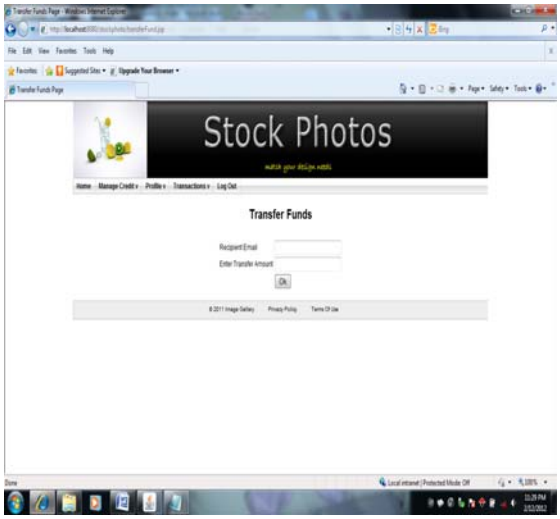

Fig. 5: Fund Transfer Page

The transfer is made using the email address supplied as no two persons are allowed to use the same Email address. All actions are automatically recorded in the audit logs so that the admin will keep watch of the activities as explain in the previous section.

The fund transfer page interfaces with the merchant gateway to get both the merchant fund and the payment commission to be transferred. The merchant fund gets to the merchants bank account or wallet address and the payment commission gets to the gateway companies bank account or wallet address depending on the payment type used in the transaction.

5. Conclusion

The key benefit of the micropayment is that little transaction charges are ensured. Payment gateway that charge little transaction need to be used. Not so much should be spent in trying to secure a micropayment system, when the cost of securing a system becomes more expensive than the system itself, then the organization is at loss. Micropayment systems only need lightweight security techniques because the risks are manageable due to the limited value per transaction. A micropayment system is said to be secured if the cost of fraud is more expensive than the possible value to be gained by cheating.

The concept of micropayments would not die down totally, nor would it entirely bloom, in spite of all the advantages that micropayment techniques appear to offer. Micropayments were targeted at a higher quantity of customers by providing items in a relatively lower selling price. In all we have designed and implemented a micro payment system that can be improved upon and used in sales of low cost items online by merchants and online sales persons as well as small scale traders.

Acknowledgments

We want to acknowledgment the staff of Oyol Computer Consult, Inc for formatting the work and presenting it in the template format of the journal and for editing the text. We also thank Mr Musa for sponsoring and financing the research and the paper publication .

References

Abrazhevich, D. (2004); Electronic payment systems: A user-centered perspective and interaction design, PhD Thesis, Technical University of Eindhoven, ISBN 90-386-1948-0.

Asagba P. O.; Nwachukwu E. O. and Uzoh O.F. (2003), Current State of Electronic Payment Systems in Nigeria, Proceedings

of the Nigerian Computer Society, Vol 14 No. 1 June 2003.

Chi E. (1997); Evaluation of Micropayment Schemes.

Min-Shiang H. and Pei-Chen S.(2006); A study of Micropayment based on One-way Hash Chain, International Journal of Network Security.

Mobile Payment Forum (2002); Enabling Secure, interoperable, and user friendly mobile systems, White Paper, December 2002.

Rivest R. and Shamir A. (1996); PayWord MicroMint: Two Simple Micropayment Schemes.

Treese G. W. and Stewart L. C. (1998); Designing Systems on Internet Commerce.

Tech T. (2017) Nonrepudiation, Tech-Target Security definitions, searchsecurity. techtarget.com/definition/nonrepudiation (accessed 2017)

TT (2017) Authentication, Tech-Target Security http://searchsecurity.techtarget.com/definition/authentication(accessed 2017)

Hitachi (2017) Confidentiality (http://hitachi-id.com/concepts/confidentiality.html) accessed 2017

Musa M. O. Musa is a young researcher and a lecturer in Department of Computer Science, University of Port harcourt, Rivers State Nigeria. She has research interest in Computer Science – ecommerce, and computer application in society as well as in Program development. She has some papers and some books which she has contributed as co-author.

Asagba P. O. Asagba is a Professor of Computer Science in Department of Computer Science, University of Port harcourt, Rivers State Nigeria. He is a specialist in computer security and database management. His research interest is vast and cover ecommerce and data integrity check. He has over 40 publications in journals and several books that he authored.