ISSN 1512-1232

Development of e-wallet system for Tertiary institution in a Developing country

[1]Fashoto, S.G., [2]Uzoka, FME, [3]Ameen, and [3]Mabayoje ,M.

[1]Department of Computer Science, Kampala International University, Uganda
[2]Department of Mathematics and Computing, Mount Royal University, Calgary, Canada
[3]Department of Computer Science, University of Ilorin, Nigeria

Abstract

The absence of adequate automated teller machines (ATMs) and banks in and around some university campuses has left students high and dry on many occasions. After banking hours, in a situation where ATMs are unable to dispense cash, students are left unable to purchase products they need at that time. The research methodology develops a new prototype for a practical e-wallet whose goal is to allow the instant money transfers between two users. Although the e-Wallet concept has many implementations, we improve the present level of knowledge by joining the online technology and the classic concepts about money restricted to the university students portal/server due to lack of bank network most times on campus. As opposed to the storing of various plastic card details on the mobile device, a single virtual card is suggested. Monetary value can be transferred to the virtual card. The proposed e-wallet system is very essential as it ensure access to funds kept in the virtual account at all-time via the internet; these reduce the dependency on the ATMs. The e-wallet system is a vital tool in the tertiary institutions. It is of benefit to students and merchants within the campus and thus should be properly managed.

Keywords: *Authentication, e-wallet, ATM, Google wallet, modes of transaction.*

1. INTRODUCTION

The use of cash as a mode of payment has been widely accepted in exchange for goods and services. However, we cannot fail to neglect the challenges associated with this mode of payments. The absence of adequate automated teller machines (ATMs) and banks in and around some university campuses has left students high and dry on many occasions. After banking hours, in a situation where ATMs are unable to dispense cash, students are left unable to purchase products they need at that time. The idea of electronic money was first proposed by David Chaum in 1983 but was not fully setup until 1990 when he founded his electronic cash company, DigiCash, in Amsterdam. The first electronic transfer was sent in 1994 (Bentogoa, 2014). Over the years, availability to financial statistics has been greatly improved by Modern-day financial communication systems and has also, considerably, facilitated financial transactions. Nevertheless, users of these systems are faced with reduction in convenience and time productivity due to some unforeseen limitations (Gutman, Beach, Wright, Springs, & Puhl, 2000).

Budgetary frameworks, these days, obtain money related data (e.g., a solicitation for a monetary exchange) from an individual utilizing a committed terminal gadget (an Automatic Teller Machine (ATM), or a point of sales (POS) terminal associated with a central budgetary system). Clients are regularly required to be physically present at the terminal gadget to complete a monetary exchange. Lamentably, the terminal gadget is typically situated at a settled site (e.g.an account office), which is not generally advantageous for clients.

ISSN 1512-1232

E-wallet is a program or web service that allows users to store and control their transaction history, logins, passwords, and shipping address and credit card details, in one central place, and to retrieve these details quickly and securely for future purposes (e.g online shopping), thus bridging the inconvenience experienced by users (Digital Wallet: Wikipedia, 2008).

Banks and other financial institutions that issue these credit cards do retain credit and accumulation hazards in such exchanges, yet regularly balance these dangers with retail exchange expenses, purchaser installment and premium charges.

Deceitful exchanges happen in both the physical and the online business situations. It is significantly more troublesome for the customers to check the validity of the shippers and the other way around because of secrecy in the online environment. In like manner, numerous shoppers do decline to enter Visa numbers on the web. It is not all purchasers that have the specialized skill to investigate a Secure Socket Layer (SSL) testament and to confirm its legitimacy (Law & Yam, 2007). In some universities for instance, banking halls are yet to be setup as the university just moved to her permanent site and ATMs are not always reliable and hence some students become stranded and unable to purchase items or pay their school fees within the school premises.

This study creates a web-based university electronic wallet (e-wallet) system. The e-wallet system would serve as a substitute for purchasing the products the students are unable to purchase without the availability of cash or ATMs or are unable to pay school fees. The system aid students to purchase products from designated university stores and cafeteria without the need for direct exchange of cash, and also afford students the opportunity to save some money in their e-wallet during their stay in the university.

The electronic payment systems have to meet several minimal characteristics in order to be efficient (Lee, 2011); (1) Atomicity: this takes into account the fact that during the transfer no existing money is lost and no new money is created; (2) The impossibility of the non-repudiation: none of the actors involved in the transaction can decline his responsibility conferred by the electronic signature.

Section 2 presents the review of related works, the types of authentication, modes of transaction and technology involved. Section 3 presents the methodology, basic process flow, conceptual framework and the architecture of e-wallet system. The implementation of the work is presented in Section 4 while conclusion and recommendation are presented in Section 5.

2. REVIEW OF RELATED WORKS

Wallets have been around for centuries, used to carry and protect objects of value. In the early times, wallets were made of cloth, secured with a rope or string, which allowed a range of items including cowries to be carried around (Clark, 2001).

Man's versatility has brought about a requirement for a convenient holder to securely convey coins and/or other installment routines. As hundreds of years have gone, we have seen an enduring change to the structure and utilization of the wallets. Average wallets now are in whimsical calfskin structure, yet the issues of portability still exist. People still have instances of lost or overlooked wallets.

At this moment, the industry of e-payments is focused on e-transfers based on card emulation and there are many successful implementations described in (Hun, 2008; Izhar, 2011; Tang, 2009). All of these systems are focused on card or bank account emulations and that means that the user has to connect with the bank to generate a money transfer (ISIS, 2012).

The advancement in information and communications technology (ICT) brought about the production of debit/credit cards that are used on ATMs today. This innovation, however progressive, has its drawbacks: card rejection by some ATMs; loss of card quality due to poor handling by card owners; in the event that the cards get lost, stolen or damaged, the card owner would not be able to carry out cash withdraw or cash deposit in the physical sense however cash deposit and cash transfer or other online transaction can still be done using available e-payment

ISSN 1512-1232

platform on the web provided the card owner remember his/her 4 digit PIN associated with the lost or damaged card; etc.

The freedom from the physical presence of these cards would be the next step in the revolution of payments all over the world. The virtual world, via the internet has created a new dimension to human mobility; people can now access their items of value from any access point connected to the internet some of these access points includes personal digital assistant (PDA), personal computers (PC), mobile phones and even game consoles. Personal details and monetary value can now travel with us without restrictions to the physical world. Electronic wallet details now resides at a secure, trusted location on the global network and can be accessed at any internet ready access points (Clark, 2001).

An individual's electronic wallet account serves as a virtual representation of that individual on the internet.

Assuming an individual (Mr. A) has an electronic wallet account. If a transaction is being carried out on Mr. A's account, how do we know for sure that it is Mr. A that is carrying out the particular transaction, seeing that Mr. A isn't physically available for verification. This is where the issue of authentication comes in.

A report by (Clark, 2001) states that a major problem faced in technological advancement is "taking of all that humans are accustomed to with them to the digital world". This well applies to the electronic wallet system as there is a need in digitizing the method of exchange and recognition of identity and freeing them from physical boundaries.

User authentication has been a base for verifying the identity of users. A summary on types of authentication procedures used over time includes:

- **Names**: Names were a suitable way of identifying individuals in a small community. A person's name is closely linked with their existing status or reputation and it served as 'pledge' when entering transactions back in the days.
- **Seals**: these were fixed on envelopes, letters or documents indicating that contents were confidential and the information contained within was meant strictly for the recipient. If the seal on the envelope was broken before it got to the recipient, it meant that the information has been compromised and had become null and void.
- **Physical Keys**: These grant access to authorized individual. Keys give a certain level of authentication to individuals. The security of item protected is compromised when the key is lost. Keys are also somewhat inappropriate for authentication as they can be duplicated by a locksmith thereby reducing the security it provides.
- **Physical Signature**: In a literate society, physical signatures were used to effectively authenticate an individual's identity. Physical signatures were unique to individuals and easy to compare by eye. This made them universal and common in everyday transaction. They, unfortunately, require a physical presence for creation and are restricted to paper. These limitations relegate them as inappropriate for online transactions.
- **Fingerprints**: Like the physical signature, the fingerprint uniquely identifies an individual. They are almost impossible to forge; this led to their use in investigations and passport issuance. Fingerprints are harder to compare than the physical signatures.
- **Username, Password/Pin**: Usernames and passwords have become the defacto standard for authentication and authorization of individuals in the online community ranging from email accounts to electronic banking websites. Usernames and passwords are independent of any physical medium thereby making them very suitable for online transaction. A drawback, however, is that as many sites now require these authentication details, users are required to use different passwords thereby making the process burdensome on the individual to remember.
- **Biometric, Voice Recognition and Retinal Scanning**: The newest forms of identification come in form of biological measurement. Most biological authentication methods are not practicable as a widespread authentication device as these methods require expensive hardware in order to work effectively.

The switching or move from device to device and access points to access points has posed a new challenge to the task. It is therefore important to detached an authentication process from

ISSN 1512-1232

physical devices and move this ability to the network. This approach will ensure an individual can be recognized anywhere, anytime and using any device.

For the e-wallet to be more successful, Local Area Network (LAN) and mobile devices must be used as simply an access point with partial authentication which interacts with an authentication system that is omnipresent and is located on a network. This can also be referred to as device-independent authentication.

After authentication occurs, transactions can then be carried out on user accounts. Some modes of transaction used over time include:

- **Barter**: This was a system mainly used in an agricultural based economy. This system does not allow for a precise estimate of goods being exchanged. Barter is used only in local environments.
- **Coins**: These were initially made from precious metals, ranging from copper up to gold, which captured the value of the coin. They were the first method of conveying value and they delivered a more precise means of exchange than its predecessor (bartering system). Some drawbacks of this payment method were the cumbersomeness of having to carry coins in large quantities and restrictions of purchase across borders (as coins differ depending on the region).
- **Promissory notes**: These are simply promises to pay a specific value on a specific date which are usually settled in exchange. The promissory note must carry a form of endorsement or authentication (usually a seal or stamp) from the holder, it can then be transferred without the holder being present. The promissory notes are subject to fraud as they rely on physical signatures. They serve as the predecessor to the modern day cheque.
- **Paper bills**: These are government issued bills that provide an itch free means if trading value within a particular geographical location. This payment method is currently the most commonly used form of exchange in the modern day society. The limitations of the paper bills are that they require currency conversion for them to be used across borders and they can't be used directly in the virtual world.
- **Plastic Cards**: The debit and credit cards offered the first mean of implementing electronic transaction. These cards allowed users to transact exchange across borders, leaving the currency conversion to their issuing banks in real time. Debit/credit cards are now widely accepted and its mode of authentication is done using the PIN.
- **Electronic Payment Instructions**: These are simply digital instructions that notify a financial organization to either debit or credit an account.

In the recent years, there has been a significant growth in mobile commerce and mobile payments. By means of the improvements of computer and mobile technology, consumers are now able to pay for purchases by moving their smartphone device near a point of sale terminal (Rutter, 2012).

The recurrent motivation by consumers to incorporate payment procedures and accounts management into one resolution; perhaps one that can be used on various devices, and is quick and easier to use, readily accessible in different situations and most importantly secure; has brought about the creation of several systems, one of which is the Google Wallet (Dragt, 2012).

2.1 Google Wallet

Google Wallet in figure 1 is an Android payment mobile app that transforms a phone into a wallet (Handa, Maheshwari, & Saraf, 2011). The Google Wallet application requires to be installed on a Near Field Communication (NFC) enabled Android phone, once this is done, it replaces the plastic payment cards by creating a virtual copy of the cards. The Near Field Communication technology allows consumers to use their NFC enabled Android phones to payment cards such as VISA, MasterCard, American Express and Discover (Google Wallet: How it works, 2015).

ISSN 1512-1232

Figure 1. Google Wallet

Google Wallet lets consumers pay for their purchased items by just tapping their phone with an NFC enabled point of sale if shopping at the store, or online by signing in to their Google Wallet account. This makes Google Wallet adequate for making both online and offline transactions. An online transaction is a transaction done via a website, while an offline transaction is one done in person, for example, buying items at the local supermarket.

Google wallet works by linking actual credit/debit cards with the electronic wallet. The card details are stored on Google's secure servers rather than on the mobile device. As soon as the credit/debit card is successfully setup within the Google wallet application, a virtual representation of the card is automatically issued. The issuing process is done by the CitiBank (one of the Google partners) (Handa, Maheshwari, & Saraf, 2011).

Technologies Involved

Some technologies that make the use of the Google Wallet Application possible are:

- The Electronic Android Application – this serves as the interface between the user and his/her account details. The application allows the user to monitor his/her account information as well as initiate payment processes.
- Service Manager – this is responsible for authenticating the account details entered by the individual. Once this is done, it enables the payment options to be used.
- The Secure Element (SE) – The SE is a smart chip typically incorporated within the NFC module or the SIM card delivered by the mobile network service operator. This integration provides a secure isolation from the phone's main memory and provides additional security layers. The core purpose of the SE is to store the virtual credit card details.

ISSN 1512-1232

Figure 2. Component used for E-wallet

- Near Field Communication (NFC) controller in figure 2 and the antenna together, are in charge of communicating securely the virtual card details from the smartphone device to the merchant's point of sale.

Problems with Google Wallet

Some problems associated with the present Google wallet system include:

- Consumers' unwillingness to switch from their current way of shopping. Some consumers see revolution as a disturbance to the lifestyle they are accustomed to.
- The unavailability of Near Field Communication (NFC) technology enabled devices (both mobile phones and POS terminals).
- Google Wallet encrypts the user's credit card information and stores it in a chip on the device. This provides hackers a possibility of reverse engineering the Google wallet app to get the key which is used to access the data.

The major problem of e-wallet generally, however, is the issue of the absence of NFC technology enabled devices and bank network failure most times on universities campuses. This current system makes payment initialization device dependent. This causes a huge drawback to the functionalities of the Google wallet and bank e-wallet system especially in this part of the world (Nigeria).

3. SYSTEM ARCHITECTURE

The proposed e-wallet system ensure access to funds kept in the virtual account at all-time via the internet and this will reduce the dependency on automated teller machines (ATM). One of the e-wallet system is hosted on the RUN server (server –side) and the second e-wallet system is the client application (client-side) on the merchant personal computer within the university campus. The new system also provides a better mode of payment for goods within the university campus. As opposed to the storing of various plastic card details on the mobile device, a single virtual card is proposed. Monetary value can be transferred to the virtual card by the university e-wallet administrator only or by the bank. This transfer can only be initiated by the card holder and completed by an authorized issuer (e-wallet administrator). The e-wallet IDs and photo IDs of the cardholder is used as a means of proper identification. On crediting the virtual card, the customer can log into his/her wallet for any internet enabled device to make purchases by entering the amount

ISSN 1512-1232

and the merchant. The merchants can also log into their wallet from any internet enabled device to confirm that the amount in question has been successfully transferred to their account.

Basically, payments are executed using the system to which the merchant and the customer have both subscribed. Consumers access the application through their mobile phones, iPads, computers, or any other internet enabled devices. Payment notification can take a number of forms (e.g., e-mail message, SMS message, or printable receipts).

The system design involves decision making focused around experience, estimation and intuition that surrounds what the software is compose and how it will be set up.

System design in figure 3 breaks down the system into logical subsystems (processes) and physical subsystems (computers and networks). The system design also decides how the machine will communicate, and it chooses the right technologies suitable for the developing the system.

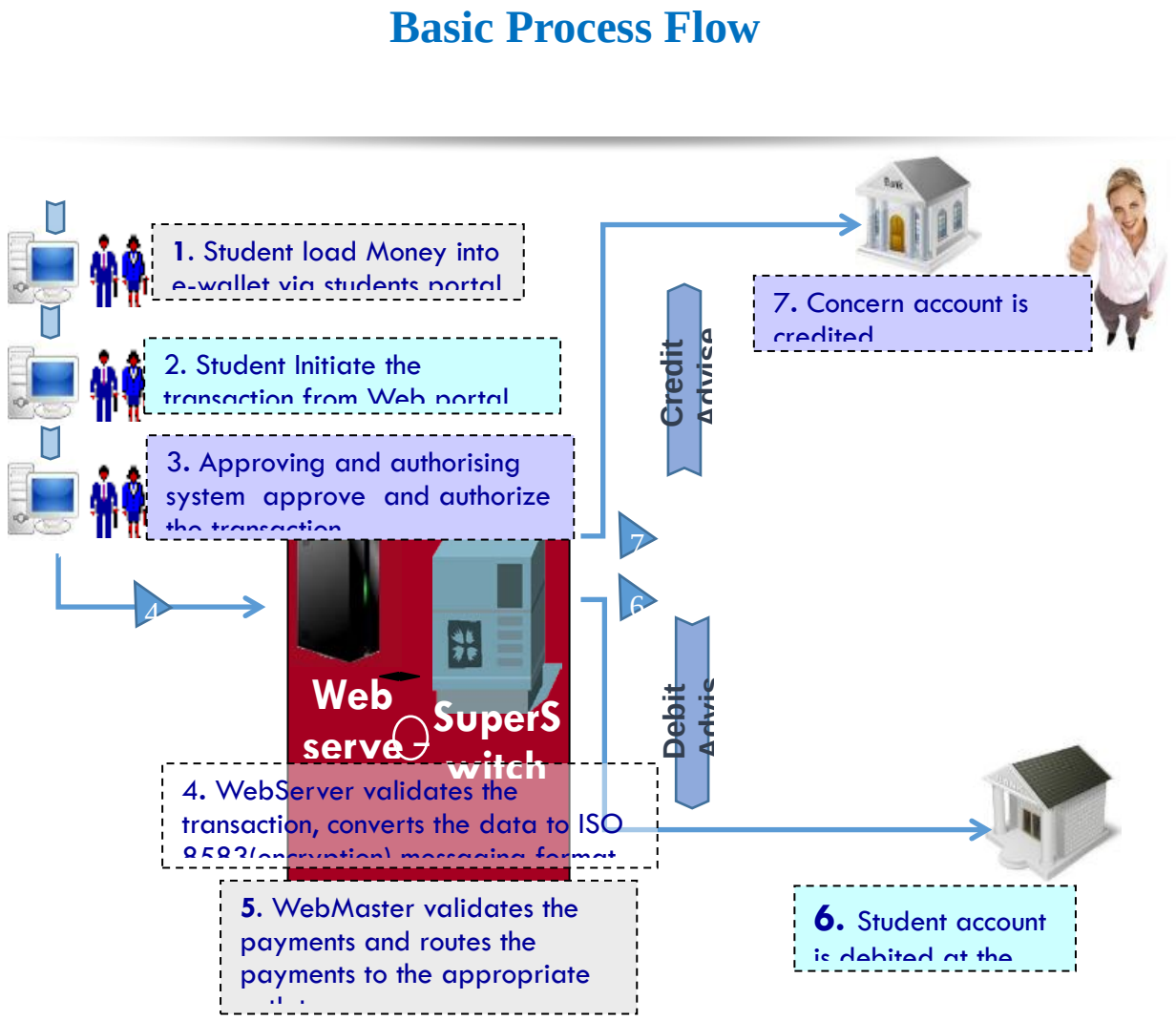

Figure 3. Basic Process Flow

This payment system is such that deposit can be made into an e-wallet account and payment for goods and services can be made with such. A case study as illustrated in figure 3 is such that a student trying to make payment of schools fees made a deposit into his e-wallet account, initiate a payment transaction through a web portal.

The transaction request is passed through the webserver and webmaster for necessary validation. The transaction request from the webserver is converted into an encrypted format for processes and validation by webmaster.

ISSN 1512-1232

webmaster validation is routed to e-wallet account of the student for necessary verification and availability of funds while payment is made into the querying bank after which the student e-wallet account is debited while the account which the transaction is being made to is credited.

Redeemer's University e-wallet system is where you can load the payment you have made into your account within the university. You do this by entering the Transaction Number collected from the webmaster and the equivalent amount paid. Having loaded fund in the e-wallet card, the card can be used on web portal for payment of school fees and payment for goods on Point of sale machines within the campus only.

The e-wallet architecture in figure 4 is the instrument that hides the complexity: once a user decides to make a purchase or show his credentials to get access to some kind of good or service, the wallet drives the protocol to transport information from the keeper to the service. The e-wallet terminal should be a mobile phone, a personal digital assistant (PDA) or a dedicated hardware module. When a user needs his credentials, for example when paying for or getting access to a service, the e-wallet terminal is responsible for retrieving the credentials required by the service. Instead of having the credentials stored in the e-wallet terminal, the e-wallet retrieves the credentials from its corresponding credential keeper and presents them for the service application. This way the user can keep all his credentials physically safe, but still have access to them anywhere and anytime, as long as the e-wallet can get connected to its credential keeper. The operations are performed according to a protocol interacting with the user through a graphical user interface (GUI).

The service. The service is presented as a remote entity that may be an end-user, vendor that requires a proof or identity from the user.

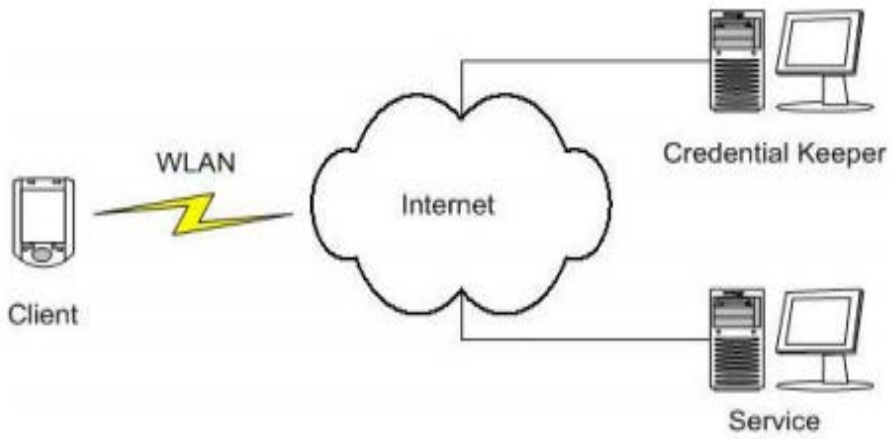

Figure 4. The Architecture of the e-wallet system

These three elements are supposed to be physically distributed and communicated using a wireless network (for this experiment a WLAN was chosen but the results are easily extrapolated to Bluetooth or cellular packet switching like GPRS).

ISSN 1512-1232

Use Case Diagram

Figure 5 shows the users of the system, the major components and the interaction between components and users.

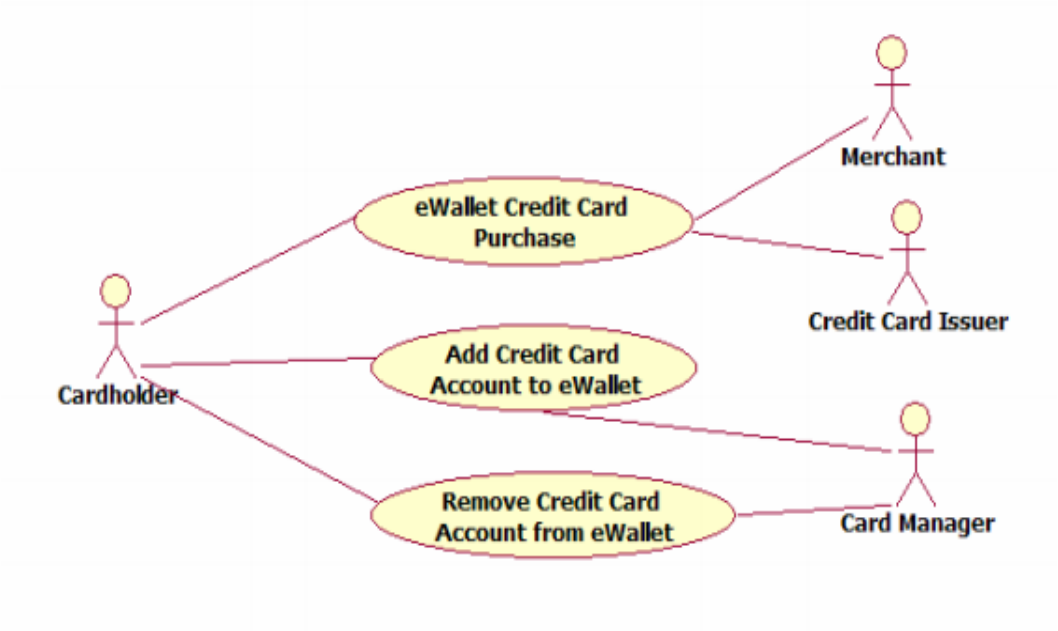

Figure 5. Use Case Diagram

Point of sales (POS) Component: The POS Component of the system is responsible for the merchant transaction piece of the process. The POS component interacts with the Card component to obtain necessary credit card information to complete a sale. It is essentially a set screens that drive the user and cashier through the checkout process. Along with retrieving necessary credit card account information from the card, the POS component interacts with the Security component to make sure each access to the card is authenticated via a fingerprint captured from the user.

4. IMPLEMENTATION

The following programming tools were used in the development of the web-based university e-wallet system:

The Hypertext Mark-up Language (HTML) is a fundamental set of instructions that makes it possible for a browser to render web pages. HTML is the language that serves as the communication between the web server and client browser. Although the server side functions such as the database processing may be performed in another language, but they must be output back to the user in HTML.

NetBeans is a software development application written in Java. The NetBeans Platform permits applications to be produced from an arrangement of measured programming parts called modules. Applications in light of the NetBeans Platform, including the NetBeans integrated development environment (IDE), can be reached out by third party designers.

The NetBeans IDE is basically intended for developing programs in Java programming language, it, in addition, also works with other languages like C/C++, HTML5 and PHP. NetBeans is cross-platform and runs on Microsoft Windows, Mac OS X, Linux, Solaris and other platforms supporting a compatible JVM.

ISSN 1512-1232

System Module

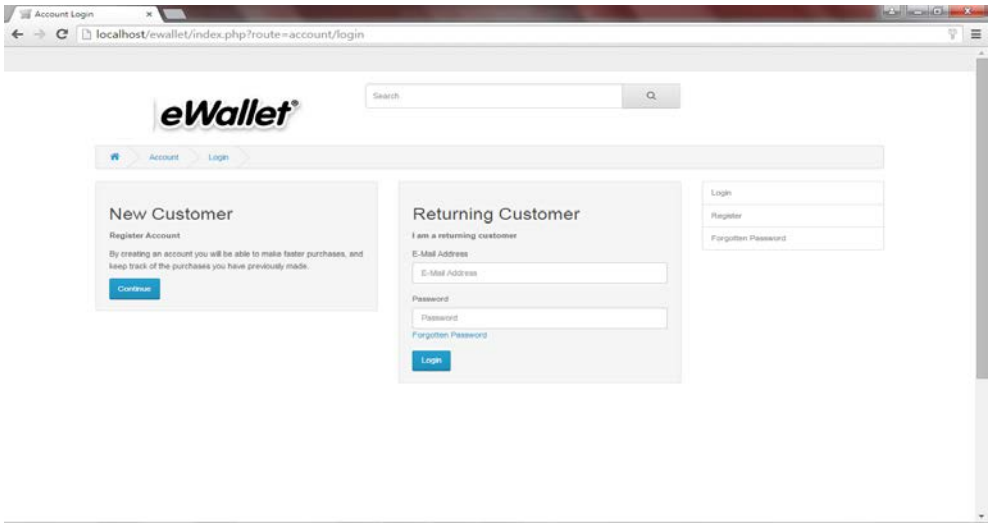

Figure 6. User login & register page

Purchase window in figure 6 is the page that can only be accessed by register users of the system to make purchase only.

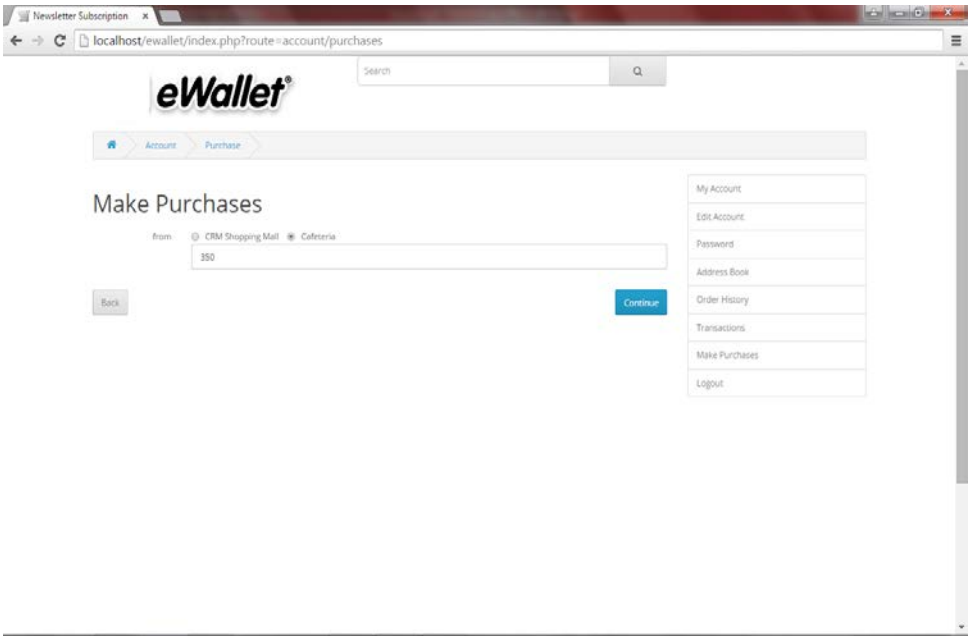

Figure 7. Purchase Window

Past transactions in figure 7 is the page that can only be accessed by the administrator of the system to check users past transactions.

5.0 CONCLUSION

This study shows how to manage data which entails the process of acquiring, validating, storing and authorizing exchange of information, making it readily accessible and dependable to

ISSN 1512-1232

authorized users. The electronic wallet system creates the platform for storing and accessing of monetary fund without the need of plastic cards, otherwise known as ATM cards.

The universe is gradually becoming more digitized in numerous areas. The electronic wallet system is a vital tool in the tertiary education institutions. It is of benefit to students, staff and merchants within the campus and thus should be properly managed.

The electronic wallet incorporates a payment system that allows for purchase without the physical exchange of cash. The said funds are transferred directly from the customer's e-wallet account to merchant's e-Wallet account.

The following are the recommendations for further studies that will enable others take additional step towards a more effectual electronic wallet system in a tertiary institution:

- There should be option of wireless transfer from third-party bank accounts to the electronic wallet account.
- There should be an interfacing with the interswitch payment portal for additional security and reliability.
- There should be an avenue for communication between the administrator and users (both customers and merchants). This will enable users to adequately lodge complaints or request assistance at any point in time.

Limitations of the proposed system

- The proposed electronic wallet cannot function in the absence of internet.
- The wallet is limited to a closed system i.e. in this case, it cannot be used outside the Redeemer' University.
- The wallet is restricted to only accredited merchants i.e. only merchant outlets which are signed up to the system can benefit from the system.
- Transactions may be slow depending on the internet connection speed.

REFERENCES

1. Bentogoa. (2014). *Electronic Money: Wikipedia*. Retrieved from Wikipedia website: http://www.en.wikipedia.org
2. Clarke R. (2001) Authentication: A Sufficiently Rich Model to Enable e-Business. Xamax Consultancy Pty Ltd, 26 December 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html
3. *Digital Wallet: Wikipedia*. (2008). Retrieved from Wikipedia website: http://www.en.wikipedia.org
4. Dragt, B., 2012. *Universal Commerce: A Seamless, Personalized, Purchase Experience for Today's Connected Consumers,* s.l.: First Data Corporation.
5. Google, 2015. *Google Wallet: How it works.* [Online] Available at: http://www.google.com/wallet/how-it-works/index.html.
6. Gutman, J., Beach, B., Wright, J., Springs, C., & Puhl, L. (2000). *Electronic Wallet.* Chicago.
7. Handa, R., Maheshwari, K. & Saraf, M., 2011. *Google Wallet - A Glimpse into the future of mobile payments,* s.l.: GRIN Publish & Find Knowledge.
8. Hun, P. P. (2008). Design and Implementation of Secure Electronic Payment System (Client). *World Academy of Science, Engineering and Technology,* Vol. 48, pp. 60-67.
9. ISIS Project (2012). *Available at http://www.paywithisis.com.*
10. Izhar, A. (2011). Designing and Implementation of Electronic Payment Gateway for Developing Countries. *Journal of Theoretical and Applied Information Technology,* Vol. 26, no. 2.
11. Lahiri, S. (2003). *System And Method For Electronic Wallet Transaction.* Austin, US.

ISSN 1512-1232

12. Law, E. C., & Yam, L. M. (Jun. 7, 2007). *EXTENDED ELECTRONIC WALLET*. United States.
13. Lee, I. (2011). *Electronic Commerce Systems*, available at http://www.cis.upenn.edu/~lee/01emtm553/.
14. Rutter, J., 2012. *What is Universal Commerce?* [Interview] (26 October 2012).
15. Tang, B. (2009). *Innovations in China's e-Payment Market*, available at http://iisdb.stanford.edu/docs/189/epayment_bin_tang.pdf.
16. Xu, W. (2000). E-commerce online payment security issues. *Joint Hefei University Journal*, vol 3.

Article received: 2016-07-06