Smart Pay Using Distributed Gateway

Mekonen Asgele
Ethio-telecom., Addis Ababa, Ethiopia
HiLCoE, Software Engineering Programme, Ethiopia
mekonen.asgele@gmail.com

Mulugeta Libsie
HiLCoE, Ethiopia
Department of Computer Science, Addis Ababa University, Ethiopia
mlibsie@yahoo.com

Abstract

Electronic payment system is a way of making cash transactions through an electronic medium. Consumers using mobile payment today still carry the cards in their wallets to use them at least in ATM. The objective of this paper is to design a new payment system called Smart Payment System (SPS) to improve usability, efficiency, anonymity, security and interoperability of electronic payment system. The main purpose is to eliminate payment cards, gateways and payment network from the process of electronic payment systems, and to help users to withdraw cash from ATM without cards. Design science research approach is used in this work. A prototype is developed to show the improvement in security, ease of use, trust and efficiency in electronic payment systems. It is developed using Java, MySQL and Android technologies to develop core bank, ATM and mobile application to test the prototype. SPS is used to withdraw cash from ATM without card and to improve security, usability, privacy and efficiency in electronic payment systems. We believe that the results obtained are encouraging.

Keywords: E-commerce; Electronic Payment System; Smart Payment System; One Time Password

1. Introduction

E-commerce has become a dynamic force, changing all kinds of business operations world-wide. A payment is a transfer of funds from a payer to a beneficiary. A payer is the party to a payment transaction which issues the payment order or agrees to the transfer of funds to the acceptor. A beneficiary is the final recipient of funds [1]. A well-designed payment system contributes to the proper functioning of markets and helps to eliminate conflicts and distrust in trade and brings peace of mind to all genuine participants [2].

E-commerce is the transmitting of funds over the Internet for the exchange of goods and services. These business transactions occur in the form of business-to-business, business-to-consumer, consumer-to-consumer and consumer-to-business. Payment systems were not growing as expected because most people who work on payment systems have started by focusing on a business model that was centered around their self-interest instead of focusing on user experience [3].

Currently Apple Pay, Samsung pay and Google wallet are putting all kinds of cards together, so one can use all cards from a single smart phone. The drawback of using such wallets is that all the cards are of different banks so the user has to deal with all of them even though they are on the same wallet. So we need to further adapt all the wallets in one system.

This paper will first review major achievements and constraints in payment systems and their features. Based on this understanding, the main constraints will be identified. In the second stage of this paper, we will examine the existing methods, industry practices, and academic researches on electronic payment systems. Finally, once the best practices and challenges are identified, a new payment system will be designed, a prototype developed and tested. To achieve the objective, we will design mobile payment system that uses OTP (One Time Password) for cash transaction regardless of the customer and merchants accounts. To test the system, we will develop an ATM (Automated Teller

Machine) system for banks and Android mobile application for customers.

Design science research approach is used to design the system and we follow the steps in design science research approach to identify the problem, to define the objectives for a solution, to design SPS (Smart Payment System), to develop SPS and test SPS.

2. Related Work

As reported in [4] ATM as self-served machine improves the ability of bank's clients easy access to cash at any time. With all its advantages, the risk of losing money in the use of ATM is also possible. Criminals use several attack methods to steal customer's money and identity. The main objective of the paper is tightening the security of an ATM using three factor authentication methods. In addition to the traditional method of ATM authentication, present card plus knowing the pin they add OTP or finger print as the third authentication method. Although producing fingerprint is very difficult, once implemented, users cannot have a chance to change their fingerprint. ATM cards can't be shared. OTP method looks good in terms of enhancing security but still customers will be forced to carry their cards and their cell phones to access ATMs.

As reported in [5] interoperable payment systems will produce efficient markets and as a result enforce reliable and secure international transaction in the globe. Currently the world owns interconnecting networks containing Payment System Infrastructure (PSI). So we will not begin from scratch. We can use the unavoidable but important interoperable payment system. The paper also studies the effects of PSI interlinking and global interoperability for central bank oversight policy. At the moment we do everything we need to start interoperable payment system in respect to technical ability and we already started enjoying the benefit of interoperability in small size at national and regional level. The paper also concluded that central banks are not playing crucial role in shaping interoperable payment systems. An interoperable payment system with all its expected benefits to civilization will introduce more risks. The main objective of the paper was using interoperability to enable customers to perform trade in convenient, affordable, fast and secure way using single transaction from any corner of the globe with single account.

The method used in the paper is by examining possible technical and legal challenges and opportunities with focus group from ITU (International Telecommunication Union) and evaluating using leading experts. The study can be used as a guide to build an interoperable payment system nationally, regionally and even globally. The paper also examines every possible challenges and opportunities using an interoperable payment system. The basic weakness of the paper is that it is not detailed enough to explain how interoperability can work in the real world using a demo or real world example.

As reported in [6], it is not debatable that electronic transaction development is growing exponentially and the current authentication methods are poor and cannot solve the growing frauds. Traditional methods of authentication should be replaced with new and bullet proof methods. Despite several benefits of ATMs, they are not free from fraud. Because of fraud, despite their significance in life, they are equally sources of trouble. The main objective of the paper was to design best identification, authentication and authorization method for ATMs for Ghanaians.

After detecting and analyzing the most critical frauds in ATMs, they propose to adapt client server architecture, and the user interaction to be finger print instead of pin for authentication. They recommended descriptive conceptual approach, and they designed a cardholder interface with ATM. They developed 16-item questionnaire using interview of experts and concepts from literature review. They randomly selected customers and staff of local banks to fill the questionnaire. They analyzed the survey using descriptive statistical

methods and show the result for industry experts for certainty. They tested their instrument reliability using Cronbach alpha. The achievement of the paper was they assure that pin is near to obsolete and they focus on local solution (for Ghanaians). They have developed good methodology. The weakness of the paper is that they focus just on security. Scanning and transmitting each fingerprint, and sending it to the server for processing is expensive. Another weakness is a card should be carried to access ATM.

3. The Proposed Solution

Online payment systems are growing throughout the entire globe. We are heading to cashless and smartcard-less society if we push hard the movement of mobile payment to the next level. This paper will focus on improving mobile payment system. Nowadays if we want to tie ourselves only on mobile payment systems then we end up not getting cash if we wish from ATMs nearby. At the moment we must use cards to get cash from ATMs and this is the weakest point of mobile payment. M-Birr and Hello Cash in Ethiopia and many applications in the entire world are able to transfer money through bank retailers and agents but still unable to have money using mobile from ATM.

3.1 What is Smart Payment System (SPS)

SPS is a way of making inter-banking cash transactions through electronic medium using just mobile phones (preferably smart phones) without using cash, checks or any payment cards. The philosophy behind SPS is if anybody has single account and smart phone then it will be enough to him/her to enjoy any service available using SPS using OTP (one-time password).

3.2 Components of SPS

As we already discussed above we have mentioned smart phone and single account to use Smart Payment System but it is worth discussing all the components in more detail.

a. Smart Phones

According to Wikipedia [7] smart phone is a mobile phone (also known as cell phone or cell mobile) with an advanced mobile operating system that combines features of a personal computer operating system with other features useful for mobile or handheld use. We can use other mobile phones in order to use SPS using USSD (USSD is a menu-based service which runs as a real-time open session between the application and the end-user) but we recommend smart phones for additional usability - using NFC (Near Field Communication) to connect with POS - and security (like using fingerprint sensor).

b. One-Time Password (OTP)

A one-time password (OTP) is a password that is valid for a single transaction, on different digital systems [8].

c. Address Database

This database could be owned by the bank union or telecom union and must be distributed on country level. The address database collects all personal information to locate the customer in case of delivery of goods or services. We can use telephone number as primary key. For simplicity and convenience, we can allow customers to edit their address.

d. DLS Server

The Domain Link System (DLS) is like DNS a technology standard for managing links of banks in SPS network. DLS allows banks to automatically change ids into links and helps bank servers to automatically find the address of other banks. A DLS server is any computer registered to join the Domain Link System. A DLS server runs an application that matches the link for an id. DLS could be owned by an individual bank or by banks union.

3.3 How SPS Works

In SPS customers will always initiate the trade. Customers choose the service or goods they need then requesting to the issuing bank for OTP by sending (1) identification number of the customer, (2) identification number of the merchant, and (3) the

amount of cash needed. The issuing bank stores the id, the amount of cash and the telephone number of the customer (used as customer id) and sends the OTP to the customer. Each financial institution can have its own method to generate the OTP but must follow the standard of smart pay. For example, all OTP must be only digits and the same length. The generated OTP works only for the owner (customer) and beneficiary (merchant). The OTP generated must have a prefix of a bank id to help the acquirer bank to locate the issuing bank. Each bank and merchant registered to the SPS must have SPS id.

Online Payment and POS: Then the customer uses the OTP for purchase. The merchant sends the OTP and the amount of the service or goods to the merchant bank. The merchant bank identifies the owner of the OTP by the prefix of the OPT and sends the OTP and the amount to the customer bank. The customer replays accept or reject. The merchant bank forwards the message to the merchant.

ATM: The OTP will be generated using ATM id instead of customer id. Customers can use the OTP to collect the cash without ATM card. Using this method, we can even go further and use the OTP to transfer cash from person to person using SPS.

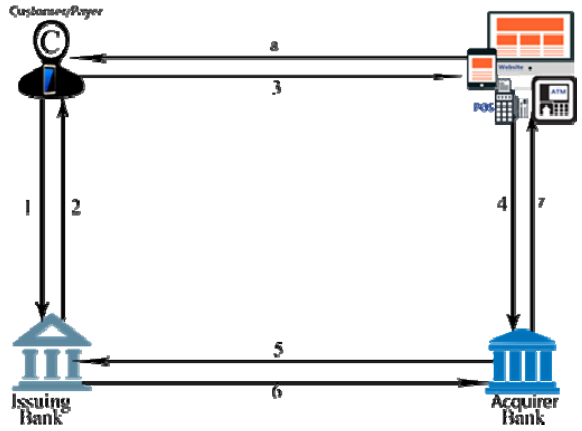

Figure 1: General Overview of SPS for multi bank

As shown in Figure 1, SPS (ATM specific) can be summarized in the following steps.

Step 1: The payer sends a request for OTP to the issuing bank along with id of the ATM, amount and phone number (phone number is automatic using app or USSD).

Step 2: The issuing bank sends OTP for the amount requested and temporarily deducts from the account for the amount requested. Temporary deduction could be permanent if the OTP is used or adjust the account by increasing amount deducted otherwise.

Step 3: The customer will enter the OTP to the ATM.

Step 4: The ATM sends the OTP to the bank (ATM's bank).

Step 5: The ATM's bank sends the OTP to the issuing bank.

Step 6: The issuing bank sends the amount and the id of the ATM to the ATM's bank.

Step 7: The ATM's bank orders the ATM to withdraw cash to the customer.

Step 8: The customer collects the cash.

To elaborate it using a real world scenario let us say a customer whose name is Abebe wants to buy hundred Birr airtime from ethio-telecom. Abebe is a customer of Dashen bank and his telephone number is 0911000000. Abebe opens his smartphone and uses an app called Smart Pay and fills the form id of ethio-telecom which is 11001100, hundred Birr and presses generate OTP using USSD. Then Dashen bank receives the phone number 0911000000 and id of the merchant in this case ethio-telecom whose id is 11001100 and hundred Birr. Dashen bank stores all the three attributes and the current time and then sends OTP to Abebe, let us say 9999 prefixed by the Dashen bank id, let us say 22. Now Abebe has the OTP, he opens the webpage of ethiotelecom to buy airtime. He fills the amount in this case 100 Birr and the OTP 229999. Ethio-telecom sends the 229999 and the 100 Birr to Commercial Bank of Ethiopia (CBE) and ethio telecom which is 11001100 are also received by CBE. CBE sends the id of ethio telecom 11001100; amount 100 Birr and OTP 229999, CBE sends the credentials received from ethio telecom to Dashen bank. Dashen bank checks if the OTP was

initially generated with the received attributes. If it is OK, then sends phone number of the owner of OTP 0911000000 to CBE. Then CBE sends OK along with 0911000000. Then ethio telecom sends the airtime to 0911000000.

If Abebe wants to buy a product let us say shoe, then when the shoe shop receives the phone number then the shoe shop should use the phone number for shipment.

If Abebe wants to buy software, then the company should send the license key using the phone number received from the bank.

SPS also works the same way if both acquiring and issuing banks are the same, when both merchant and customer from the same bank (we call it single bank SPS). Single bank SPS is a very simplified form of SPS when the customer and merchant/PAW (POS, ATM and Website) accounts are from same bank. The same bank will generate the OTP, process the OTP and did clearing and settlement process. The advantage of single bank SPS is that banks that do not trust other banks or banks that do not want to work with other banks can use the system with limited benefit.

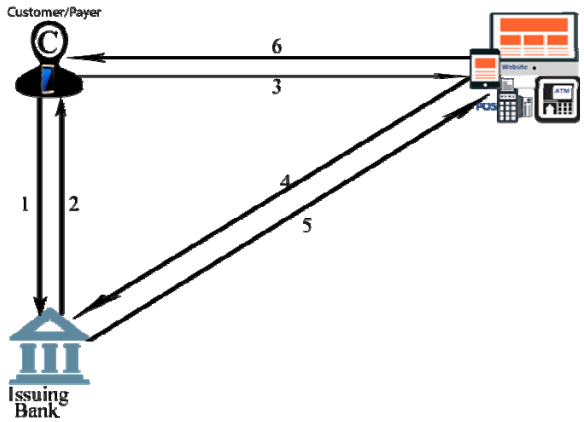

Figure 2: General Overview of SPS for Single Bank

As shown in Figure 2, in Single Bank SPS the OTP generator and verifier is a single bank. We can get every advantage of the SPS for multi bank but without interoperability.

4. Discussion

The reason why cash still exists is mostly because there is no cost of transaction, suitability, anonymity and acceptance. So any new electronic payment system should keep the most important features of cash in mind. Whatever the next development in online payment, electronic payment system will remain a key factor in e-commerce. Currently online businesses are growing regardless of the growing attacks in online systems. So the need of cost effective and convenient electronic payment system are quite significant. SPS applies Java's concept of "write once run everywhere". In SPS we can have a single account and make business with everybody. SPS eliminates integrators, network owners and leaves all finical institutions at the same stage. SPS helps customers to buy products or services regardless of the accounts of both the customers and merchants.

SPS solves ATM and POS frauds such as skimming attack (unauthorized capture of payment data to commit fraud) and card trapping attack (to trap the ATM card in cash dispenser and steal pin) by simply avoiding using cards. The target of criminals is the card and we avoid using them. So criminals have nothing to skim or trap. For attacks like phishing and malware we introduce OTP, use and throw approach. In case of criminals successfully getting access to the OTP before the user uses them, we use mapping concept, every OTP maps to a single machine id. So criminals should know the machine id to know which ATM or POS is referred. Even though it is impractical to know all these in ten minutes because the OTP expires in ten minutes, we make machine id to be randomized periodically to strengthen the security of SPS.

Customers with traditional type of payment system must find a merchant that accepts the payment system they have in order to purchase the product or service. Customers are forced to have many payment cards which basically did the same as a result of luck of interoperability between the

payment systems. SPS solves this problem by developing an open standard for financial institutions to make transaction without sharing sensitive information of the customer or the merchant. Not sharing sensitive information helps one financial institution to trust any registered financial institution without knowing their record of security compliance.

When users access ATM using SPS to withdraw cash or POS to purchase goods or services or purchasing goods or services online, SPS uses the same technique, i.e., request OTP and use them. As a result, users have short learning curve. Accessing ATM without card also improves the way we transfer money. Using SPS users can transfer the OTP at any time so beneficiaries can collect their cash from nearby ATMs regardless of place or time.

SPS is also highly likely to improve efficiency since the cost of transaction is a result of competition among payment systems and secured transactions. Competition is achieved by interoperability of the system and helps the cost of transaction to decrease. Cost of transaction falls when cash lost due to fraud drops.

Finally, we show SPS improves security in transactions, is able to trade without cards, eliminates third-party switches and networks that cost money for participants, privacy of users and trust among financial institutions due to not sharing sensitive information among them.

5. Conclusion and Future Work

SPS is open standard electronic payment system. The central philosophy behind SPS is a user needs just a single account to purchase a product or service regardless of the account of the merchant. Using SPS one will request an OTP for any amount and use the OTP at ATM, POS or online using the same concept. Even though the main purpose of SPS is to conduct inter-banking transaction, it is also possible to be used by a single bank. Since a merchant and user have single account, every transaction will be lodged using the respective banks. Since no user data is transferred to the merchant, privacy will not be compromised. In SPS, OTP is generated using merchant id, so there is no possible loss of cash in the transaction. We believe the standard of the SPS will be accepted and transforms the payment system.

The results of this paper show that there is a need to refine SPS by including currency converter module in the design of the prototype and improve the privacy issue by avoiding to use phone number as primary key.

References

[1] Dennis Abrazhevich, “Electronic Payment Systems: A User-Centered Perspective and Interaction Design”, Eindhoven, Netherlands, 2004.

[2] “The Evolution of Payments”, http://www.paymentsleader.com/the-evolution-of-payments/, June 22, 2016.

[3] “History of e-commerce”, http://searchcio.techtarget.com/definition/e-commerce/, June 24, 2016.

[4] Mohammed Hamid Khan, “Securing ATM with OTP and Biometric”, IJRITCC, 2015.

[5] Biagio Bossone and Bruce Schneier, “Payment System Interoperability and Oversight: The International Dimension”, ITU, 2015.

[6] Nana Kwame Gyamfi, “Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective”, Kumasi, Ghana, 2014.

[7] Wikipedia, the free encyclopedia, “Smartphone”, March 10, 2017.

[8] Fumiko Hayashi, “Mobile Payments: What’s in it for Consumers”, Federal Reserve Bank of Kansas City, 2016.