Providing Security for E-Wallet using E-Cheque

B. Yahid
IT Department
University of Guilan, Rasht, Iran
behzadyahid@gmail.com

Dr. A. Shahbahrami
Postdoctoral in Computer Engineering Department,
University of Guilan, Rasht, Iran
shahbahrami@guilan.ac.ir

Dr. M. B. Nobakht
Postdoctoral in Management and Economy Department
Ministry of Science, Research and Technology, Tehran, Iran
nobakht@csr.ir

Abstract
Payment is one of the main parts in businesses. Different types of software, hardware and methods for paying electronically have been presented. Different types of banking cards, E-wallet, internet web pages for payment make it possible to pay both online and offline. However, in most payment tools, exchanging money is anonymously and untraceably. Therefore, although most security techniques within payment tools are considered to restrict abuse, if it is stolen, it makes possible to be abuse. Furthermore, anonymous characteristics of E-money make it possible for money laundering. E-cheque includes both sides name in a business, and also it is traceable. By using E-cheque techniques in payment tools instead of E-money, it is possible to increase payment tools security.

Keywords: Payment, Security, Payment Tools, E-cheque, E-commerce

Introduction
Payments are a considerable part in businesses. By increasing electronic intercourses, electronic paying tools are considered particularly. E-wallet is one of the most applicable E-payment tools. E-wallet makes it possible to pay in electronic digits both offline or online. Considering to the developing capabilities of mobile, and accessibility of it, it can be considered as a convenient tools for E-wallet, and it can lead to improving businesses. Inspecting through UTAUT\(^1\) method shows that E-wallet in mobile is interesting for customers and they will accept it (Eslami and Talebi, 2011; Basua and Muylle, 2011; Helander and Khalid, 2000; Ruiz-Martínez et al., 2012; Al-Fedaghi and Taha, 2006; Zaman Ashrafi, 2009; W. Tan and Y. Tan, 2012; Chang et al., 2009; Au and Kauffman, 2008; Shin, 2009; Gökmen, 2011).

Most people buy in offline mode. Offline E-money in mobile E-wallet is the same as bill in traditional wallet; therefore, it has many defects of traditional money. Absolute anonymity and untraceable characteristics of offline money leads to be abused or stolen. In addition, if the mobile set is naught, its including money will be naught too, and makes
sustain losses for the owner (Car bunar et al., 2011; Chen et al., 2011; Zaman Ashrafi, 2009; Van Nierop et al., 2011). Most users of mobile E-wallet are worry about security of their properties. Mobile phone is a great danger if it is naught or stolen after saving personal and financial information. Security protocols offered for E-payment do not have similar executing structure (Ruiz-Martínez et al., 2012; Shin, 2009; Narayanasamy et al., 2011; Helander and Khalid, 2000; Antoniou and Batten, 2011; Basua and Muylle, 2011).

In this paper, by considering to E-cheque, and E-coin characteristics and presenting an especial paying system, an offline E-wallet in mobile is presented to decrease or remove above mentioned problems. Presented system will offer all characteristic of traditional cheque in electronically and it leads to pale mentioned problem. Furthermore, paying will be done more safe and easy. In addition, offline money credit with comparative anonymity is included within mobile. By “comparative anonymity” it means it would be traceable, pursuit and recoverable by E-wallet owner request, if it is naught or abused. As a result, users’ confidence for using it in payment will increase.

The structure of this paper is so that in part (II), E-wallet, challenges, E-cheque, and their function and background is introduced. In the part (III), a recommended model of E-wallet by considering E-cheque in mobile is presented. In part (IV), the above mentioned E-wallet is analyzed and in (V) conclusion and result is included.

E-wallet, Challenges, and E-cheque

In this part, initial definitions and function, E-wallet and its relevant challenges are presented and E-cheque characteristics will be demonstrated.

Mobile E-wallet

E-wallet similar to its electronic version of physical wallet makes possible to do financial exchanging and to increase speed of payment. E-wallet is implemented and secured in different hardware. UTAUT as a format of Technology Acceptance Model (TAM) shows that the E-wallet is technology-centered and user-centered. For implementation of the E-wallet system, at first initial necessary information such as general keys should be produced and users should open an account (Sanayei, 2011; Al-Fedaghi and Taha, 2006; Juang, 2010; Car bunar et al., 2011; Chen et al., 2011; Eslami and Talebi, 2011; O’Mahony, 1997; Shin, 2009).

Different electronic paying could be included three different parts; Banks, Payers, and Sellers. Payers emit money from the bank, and pay it to the seller in returns of goods or services and at last businessman will deposit money in the bank. There are three distinct phases in this cycle- take, pay, and deposit. There is usually a bank as the supporter of a model of E-wallet in the field of software and hardware to define working function and offline financial exchanges. Like as intelligent cards, and POS set that are presented as E-wallet in offline mode by the banks (O’Mahony, 1997; Shin, 2009; Chen et al., 2011; Eslami and Talebi, 2011).

Hardware such as PC, different types of banking cards, and mobile are used as E-wallet. E-wallet in mobile could be used more easily in business, and it is economical in time, expense, and energy (Zaman Ashrafi, 2009; Panniello and Gorgoglione, 2012; Weber,
Challenges and Stimulie

Considering to surveying and studying done in the field of E-wallet, that some of them are mentioned in the previous pages, mobile E-wallet has a lot of challenges that some of them are as following (Eslami and Talebi, 2011; Zaman Ashrafi, 2009; Juang, 2010):

- If its bearing hardware destroyed, the money of the E-wallet would be naught.
- Security and transaction cost is high.
- There are risks for misusing of the E-wallet by two parts of a business or hackers due to anonymity and untraceability of the money.

However, a lot of efforts have been made by the researchers to remove some of the mentioned challenges. For example:

- E-Trading Laws (ETLs), support E-signature, and it has legal reliability as the same as traditional signature.

- For decreasing security cost, mobile digital alias technique with blind signature in to some extent, through private key of the customers for offline E-money has been presented. In addition Schnorr’s⁴ scheme proposes a better solution to produce digital signature and to decrease intelligent cards security processing. This efficiency is very important for some hardware, because for example there are many limitations in intelligent cards with 8-bit processors using in CAFÉ right now (Juang, 2010; O’Mahony, 1997; Shin, 2009; Narayanasamy et al., 2011; Aashish, 2011; Chang et al., 2009).

Considering to different types of present challenges, and by investigating offered solutions, it make us to decrease some mentioned limitations through a new algorithm, uses combination of E-check in the mobile E-wallet. In general, the advantages of the proposed idea in comparison with other methods are following:

- Money will not be included in the E-wallet, whereas financial credit will be transmitted by using E-cheque characteristics.
- If it is necessary, payment will be traceable.

If its hardware is stolen or naught, its credit will be recoverable.
E-Cheque

E-cheque is the electronic version of the cheque, and it has all the features of the paper cheque. E-cheque could be used in different conditions such as payment without cash, installments, conditional, warranty for business, and official payments. E-cheque has important fields such as Cheque Number, which is a random big and unique number to identify E-cheque, payer’s account number, beneficiary name, cheque amount, and date of payment. However, E-cheque fields depend on cheque regulations in each country, and could be variable (Heffernan, 2005; Tan and Y. Tan, 2012; O’Mahony, 1997; Liaw and et al., 2007; Sunitha et al., 2007).

As E-cheque is a complete digital document for e-payment, its security implementation is very close to mathematical algorithm and coding system implementation as well as E-money. Many protocols in international level for E-cheque implementation have been applied. US Financial Service Technology Consortium (FSTC) is the first sample of it in coding format. Four types of processing have been demonstrated in FSTC, in which the payer could submit E-cheque to the payee, or Payee bank, or payer bank directly. In addition, payee would be able to cash the cheque through his/her bank, or payer bank. Figure 1 demonstrates processing methods in FSTC. Further most famous processing are MANDATE5 in Europe, Safe-Cheque and E-cheque in some of the Asian countries (Heffernan, 2005; O’Mahony, 1997; Pasupathinathan et al., 2005; Sunitha et al., 2007; Liaw et al., 2007; Nasiri Mofakham, 2005; Ebrahimi and Yahid, 2011; Vercellis, 2009; Abbasnejad, 2010).

Security of E-cheque is secured by digital signatures and different attacks toward it are restricted through the most confident methods such as Anonymity, Confidentiality, Generality, Non-repudiation, and Non-repetition. Signatures could be saved within intelligent cards in coding keys, and the card would be activated through ID number. Figure 2 represent a security path in E-cheque payment (Ebrahimi and Yahid, 2011; Nasiri Mofakham, 2005; Liaw et al., 2007; Sunitha et al., 2007; Pasupathinathan et al., 2005; Fakoor, 2009).
Resenting a New Model of E-Wallet in Mobile

In this section, by characteristics combination of E-cheque, E-money, and mobile phone, a new paying method for E-wallet in mobile is presented. At first, the possibility is evaluated by investigating necessities, Bank charts and Use Case. Then UML charts are implemented for designing. Then, databases and program algorithm are considered through ER charts, and tables.

General Use Case Process of the system

In this process, the relationship between major parts and the internal operation among them are evaluated generally. Seller and Receiver already open an account by the bank, registration process; necessary identification and presenting document have been done. Payer would be able just to pay. Receiver would be able just to receive. Produced credit in payer E-wallet is through E-cheque that has expiry date. Receiving credit also has expiry date. Figure 3 present this process.
ER Complete Diagram

In this section, entities, adjectives, and main keys are introduced and at last the relation between entities and ER complete diagram is presented. Seller and buyer are considered as independent entities, and account number and code are considered as main keys. Current account and E-cheque are considered as sub-entity out of the bank entity. System code and electronic evidence are presented as main keys. Payer’s and Receiver’s E-wallet play are as independent entity Figure 4 represents a complete ER diagram.

Following, designing of the feature tables for the entities are considered, and tables are created. Some examples of the tables are showed in figure 5 and 6.

<table>
<thead>
<tr>
<th>Main Key</th>
<th>Field name</th>
<th>Type of Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>CN</td>
<td>Int</td>
<td>loaded credit no.</td>
</tr>
<tr>
<td>*</td>
<td>Cust_ID_S</td>
<td>Int</td>
<td>Payer’s Code</td>
</tr>
<tr>
<td></td>
<td>CreateDate</td>
<td>Int</td>
<td>Date of issue</td>
</tr>
</tbody>
</table>
Now, it is necessary to apply banking regulations and to implement an algorithm for preparing the E-wallet. Therefore, considering to the regulations of issuing chequebook, E-cheque, and different security methods mentioned in previous pages for E-money, by a combination of them we present some algorithms.

### The algorithm for preparing the E-wallet through E-cheque for payer

Considering to banking regulations and necessity in each country, number of the variable of the algorithm is different; therefore natural variables such as $X_i$ are used for implementation to have more flexibility to save algorithm conformity. For creating credit by the bank and including it within the payer's mobile E-wallet, following steps are taken:

- Considering to the bank criteria, amount $X_1$ is included within the payer E-wallet ($P=X_1$). This amount is equal to the total payable credit through payer's mobile E-wallet.
  - An scratched card with $X_2$ digit pin is given to the payer ($PCS^9 = X_2$)
  - In the payer's mobile E-wallet, $HCS^{10}$ is registered to start correlation with receiver's mobile E-wallet.
  - For securing the payer's identity from deception, $S$ with $HCS$ is under $\oplus$.
  - Number of $X_3$ keys for coding payer's E-cheque are created $KS_i^{11}$
  - number of $X_3$ credit number randomly $CN_i^{12}$
  - For restricting of unfeigned credit creation, credit serial number is put in a HASH function, and then it would be coded through RAS method ($Credit = CN_i \cdot H(CN_i)KS_i$). Thereupon if RAS coding is reverse engineering, as HASH function is one way, it could not be fraud, and counter cheque could not be created. (Similar to CAFÊ studying project in Europe).

Then, as shown in figure 7, number of $X_3$ records is included within the payer's mobile E-wallet.

### Figure 6. Field Description of Receiver’s E-wallet

<table>
<thead>
<tr>
<th>Mani Key</th>
<th>Field Name</th>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>CN</td>
<td>Int</td>
<td>Coded Credit No.</td>
</tr>
<tr>
<td>*</td>
<td>Cust_ID_R</td>
<td>Int</td>
<td>Receiver's Code</td>
</tr>
<tr>
<td>*</td>
<td>Cust_ID_S</td>
<td>Int</td>
<td>Payer's Code</td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>Int</td>
<td>Amount</td>
</tr>
<tr>
<td></td>
<td>CQ_SarresidDate</td>
<td>Int</td>
<td>Date of Receiving</td>
</tr>
</tbody>
</table>

### Figure 7. A Record of Payer’s Mobile E-Wallet

<table>
<thead>
<tr>
<th>Credit No.</th>
<th>Date of Issue</th>
<th>Payer’s Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CN_1 \cdot H(CN_1)KS_1$</td>
<td>DS</td>
<td>$S \oplus HCS$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$CN_{X_3} \cdot H(CN_{X_3})KS_{X_3}$</td>
<td>DS</td>
<td>$S \oplus HCS$</td>
</tr>
</tbody>
</table>
The algorithm for preparing the E-wallet through E-cheque for receiver

For receiving an offline credit, the Receiver's E-wallet should be prepared by the bank as following:

- Receiving key coding from the bank KR\textsubscript{13}.
- An scratched card with X\textsubscript{4} digit pin is given to the Receiver (PCR\textsubscript{14} = X\textsubscript{4})
- In the receiver's mobile E-wallet, HCR\textsubscript{15} is registered to start correlation with payer's mobile E-wallet.
- For securing the receiver's identity from deception, R with HCR is under $\oplus$.
- Then, as shown in figure 8, records are included within the receiver's mobile E-wallet.

\begin{table}[h]
\begin{tabular}{|c|c|c|c|c|}
\hline
Receiver’s Code & Credit No. & Receiving Date & P\textsubscript{i} Amount & Payer’s Code \\
\hline
R $\oplus$ HCR & Empty & Empty & Empty & Empty \\
\hline
\ldots & \ldots & \ldots & \ldots & \ldots \\
\hline
R $\oplus$ HCR & Empty & Empty & Empty & Empty \\
\hline
\end{tabular}
\caption{A record of Receiver’s E-wallet}
\end{table}

Paying Process

Following steps are recommended to do paying operations from payer's mobile E-wallet.

- Physical relation between E-wallet software is through Blue Tooth, and all messages are coded under commitment encryption and then they would be sent.
- For payer's E-wallet activation, PCS is necessary. (by 3 times wrong entrance, or credit expiring, the E-wallet remove the credit automatically.)
- Customer inserts PCS to activate his/her E-wallet, and receives HCR. Then list of salesroom appears, HCS is sent for them. Two E-wallets recognize each other, and are ready to exchange. Figure 9 demonstrates recognition process of wallets. Receiver transmits amount of the invoice to the payer as a request.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure9.png}
\caption{E-wallet connection and identification}
\end{figure}

- Payer confirms the amount of paying operation. Then payer’s E-wallet software sends $\{H(CN_{i})\}KS_{i}, S\oplus HCS, P_{i}\oplus PCS$ to the receiver, and waits for confirmation.

Receiver’s E-wallet software will $\oplus$ the receiving amount by PCR, and fill out one of its records as following and declare receiving confirmation. Figure 10 shows a record of the Receiver's wallet.
Recovering Procedure

For using received offline credits, receiver should transmit them to his/her online account, and following steps are recommended:

- By PCR code, Receiver’s E-wallet is activated. (By 3 times wrong inserting, the E-wallet would be locked and bank would be able to activate it again).
- Receiver’s E-wallet declares a report of expiry of received credit when it turns on.
- In each period, Receivers’ should refer to the bank at least once to recover the E-wallet before expiring date.

Receivers refer to the bank, and the bank clears all receiving credits out of the E-wallet and transmits these records to the bank software for processing. Then initial and raw records are prepared through encoding and reverse processing, and all fields are inspected to see if there is any difference with mentioned regulations in the proposed model for mobile E-wallet. At last, mentioned records are canceled and relevant amount is transferred to the Receiver’s account.

Analyzing the Specifications of the Proposed Model

Our proposed model for mobile E-wallet in this article has the following specifications;

Payer and Receiver comparative Anonymity

Payers and receivers have financial transactions through special codes, which are definable just for banks, and are included in E-wallets in coding format. This function also is processed anonymously. It is comparative anonymous, because banks have access to these data if it is necessary.

Not Double Spending and Coping

As cheque is included within payer’s wallet without amount, double spending concept is dismissed, and by every payment, one credit is used. In addition, when a credit amount is confirmed, transacting to receiver’s wallet and deleting from payer’s wallet is done, therefore that record does not exist anymore to be copied.

High Security if Hardware or Software Has Been Lost

A X_2 digit PIN code activates the mobile E-wallet, and through three wrong inserts, it would be locked. Therefore, there is very low chance for a robber (3/36^3). Furthermore, by
referring to the bank, payers can inform them and cancel credits.

Revealing Forgery and Restricting
As the paying cycle is limited and it is not continues, therefore any discrepancies or forgeries will be revealed maximum within two months, and it can be followed legally based on document.

Legal Prosecution Capabilities as the same as Cheque
In recommended model, indeed paper cheques are presented electronically. Therefore, all documents are presentable and prosecutable.

High Risks for Hackers, and Low Risks for Users:
In this recommended model, as paying is done in a short paying cycle with distinct entrance and exit and with initial registrations, there are high risks for revealing hackers. In addition, due to low amount available in the E-wallet and suitable security precautions, there are low risks for payers.

Results and discussion
Offline mobile E-wallet has different challenges and limitations such as security issues, loosing amount, limitation in buying, etc. To decrease these limitations, using E-cheque in the mobile E-wallet is proposed in this article. Proposed mobile E-wallet based on E-cheque has been analyzed. Using process of this model for payer and receiver has been analyzed. For example, after opening an account, payer would receive credit from the bank and would save it in the mobile. Mentioned algorithm has been implemented and proposed model has the following premiums:

Banking sources are not excluded from the bank, but digital credit exchanges, due to stolen or naught, E-wallet owner’s profits are protected, any money laundering or misuse is traceable, and most specifications of E-money are existing. As result, this proposed algorithm could be considered as a new method for paying electronically.

Notes
1. Unified Theory of Acceptance and Use of Technology (UTAUT)
2. Blind Signiture was used for designing E-money by Chaum in 1983
3. The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. It was described by Taher ElGamal in 1984.
4. In cryptography, a Schnorr signature is a digital signature produced by the Schnorr signature algorithm.
5. Managing and Adminisrating Negotiable Documents and Trading them Electronically (MANDATE)
6. Though “Use Case”, system behavior could be defined.
7. Unified Modeling Language (UML): This language analyzes and interprets Object orientation systems.
8. Entity Relationship (ER): this chart is used to represent relationship between entities.
9. Pin Code Sender (PCS)
10. Hello Code Sender (HCS)
11. Key Sender (KSi)
12. Cheque Number (CNi)
13. Key Receiver (KRi)
14. Pin Code Receiver (PCR)
15. Hello Code Receiver (HCR)

References


