7th International Conference
on e-Commerce in Developing Countries
with focus on e-Security

17-18 April, 2013, Kish Island, Iran

# Providing Security for E-wallet using E-cheque

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

***Dr. Assadollah Shahbahrami***
*University of Guilan,Rasht, Iran*
*shahbahrami@guilan.ac.ir*
*Computer Engineering Department*

***Dr. Mohammad Bagher Nobakht***
*Management & Economy Department*
*Ministry of Science, Research &*
*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 method shows that E-wallet in mobile is interesting for customers and they will accept it [51, 7, 34, 8, 39, 33, 45, 50, 49, 14, 9].

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 [11, 48, 33, 30]. 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 [8, 14, 32, 34, 22, 7].

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 implementation of the E-wallet system, at first initial necessary information such 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.

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

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.

## I. 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.

### A. *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 as general keys should be produced and users should open an account [4, 39, 45, 41, 11, 48, 51, 20, 14].

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 [20, 14, 41, 48, 51].

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 [33, 42, 6, 39, 2, 24, 44, 50, 39, 5, 49]. E-wallet in mobile could be equipped by functions of intelligent cards and has different paying capabilities such as different type of payment, like E-cash money, credit cards, Debit cards, paying out of the SIM cards credit, passing E-cheque through ACH [50, 49, 20, 14, 41, 48, 51].

### *B. 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 [51, 33, 1, 45]:

- 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 untraceablity of the money.

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

- Some presented security methods which are presentable in E-money are as following; utilizing blind signature, EIGamal signature, security method using in Net Cash, security method in electronic voting, security method of making confidence by mutual anonymity conversion, Alfa & Gama security method [22, 11, 51, 8,
- 48, 20, 33].
- E-commerce regulations (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

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

- the customers for offline E-money has been presented. In addition Schnorr's 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 [45, 20, 14, 32, 1, 50, 31].

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.

### C. *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 [17, 36, 28, 43, 20, 26, 37].

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 MANDATE in Europe, Safe-Cheque and E-cheque in some of the Asian countries [28, 36, 20, 17, 43, 37, 26, 21, 38, 12, 25].

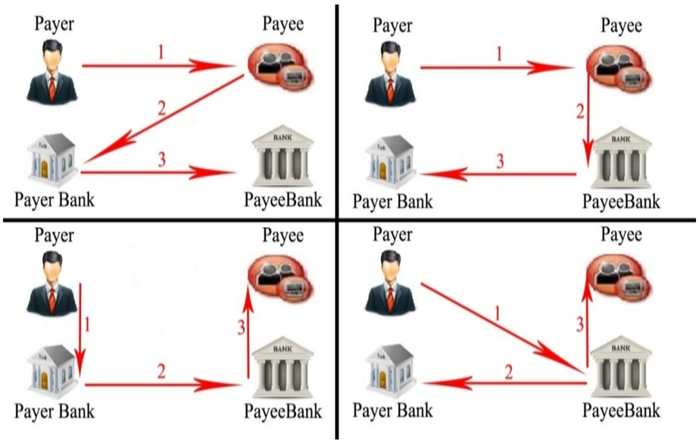


Figure 1- Four processing of FSTC for e-cheque

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 [38, 21, 26, 37, 43, 3, 16, 17].

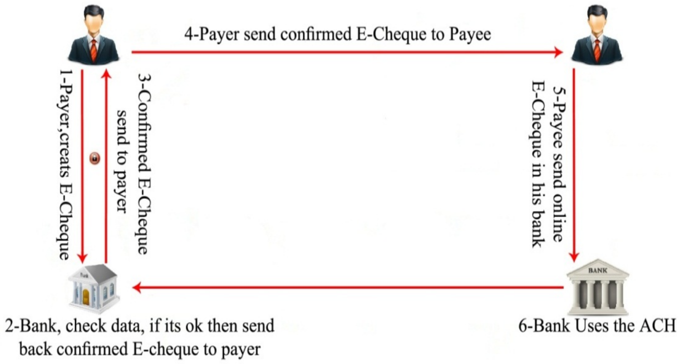

4-Payer send confirmed E-Cheque to Payee
1-Payer,creats E-Cheque
3-Confirmed E-Cheque send to payer
5-Payee send online E-Cheque in his bank
BANK
2-Bank, check data, if its ok then send back confirmed E-cheque to payer
6-Bank Uses the ACH

Figure 2- A sample of Security path in paying E-cheque

## II. 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,

### A. *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.

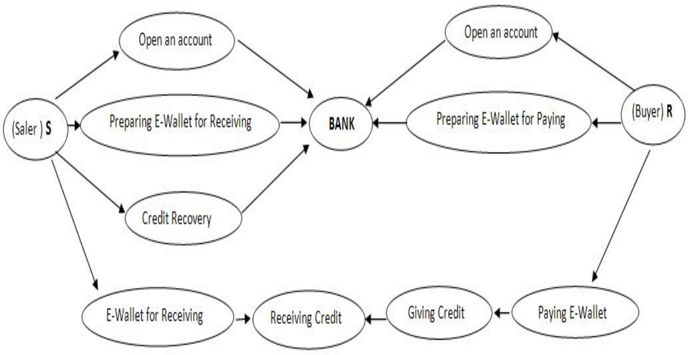


Figure 3- General process of presenting system

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

### B. *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.

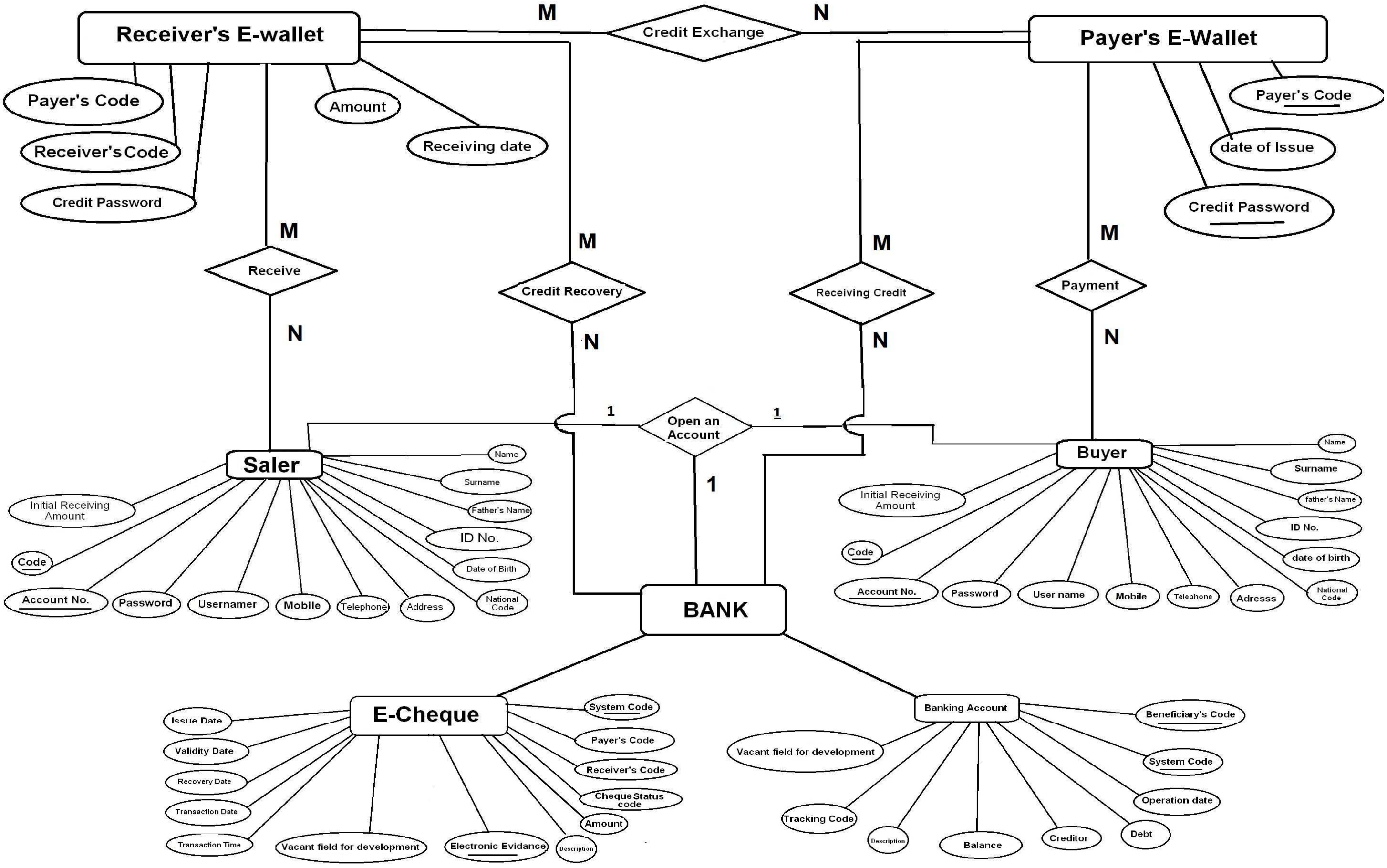
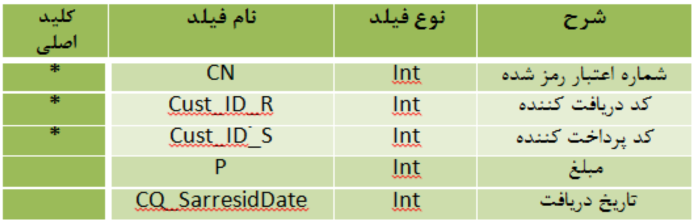


Figure 4- Complete ER diagram for E-wallet through E-cheque

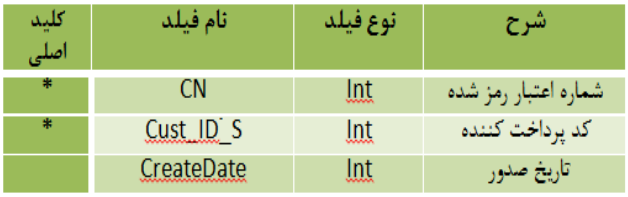
Following, designing of the feature tables for the entities are considered, and tables are created. Some examples of the tables are showed in figure 5 and 6.

Figure 5- Field Description of payer's E-wallet



| کلید اصلی | نام فیلد | نوع فیلد | شرح |
|---|---|---|---|
| * | CN | Int | شماره اعتبار رمز شده |
| * | Cust_ID_R | Int | کد دریافت کننده |
| * | Cust_ID_S | Int | کد پرداخت کننده |
| | P | Int | مبلغ |
| | CQ_SarresidDate | Int | تاریخ دریافت |

Figure 6- Field Description of Receiver's E-wallet



| کلید اصلی | نام فیلد | نوع فیلد | شرح |
|---|---|---|---|
| * | CN | Int | شماره اعتبار رمز شده |
| * | Cust_ID_S | Int | کد پرداخت کننده |
| | CreateDate | Int | تاریخ صدور |

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.

### *C. 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 ($PCS = X_2$)
- In the payer's mobile E-wallet, HCS 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 $KS_i$
- number of $X_3$ credit number randomly $CN_i$
- 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 $_i$ = $CN_i$, $\{H(CN_i)\}KS_i$). 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 CAFÉ studying project in Europe).
- Then, as shown in figure 7, number of $X_3$ records is included within the payer's mobile E-wallet.

| **Credit No.** | **Date of Issue** | **Payer's Code** |
|---|---|---|
| $CN_1$, $\{H(CN_1)\}KS_1$ | DS | $S \oplus HCS$ |
| … | … | … |
| $CN_{X3}$, $\{H(CN_{X3})\}KS_{X3}$ | DS | $S \oplus HCS$ |

Figure 7- a record of payer's Mobile E-wallet

### D. *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 $KR_i$.
- An scratched card with $X_4$ digit pin is given to the Receiver ($PCR = X_4$)
- In the receiver's mobile E-wallet, HCR is registered to start correlation with payer's mobile E-wallet.
- For securing the receiver's identity from deception, R with HCR is under ⊕.
- Then, as shown in figure 8, records are included within the receiver's mobile E-wallet.

| **Receiver's Code** | **Credit No.** | **Receiving Date** | **$P_i$ Amount** | **Payer's Code** |
|---|---|---|---|---|
| R⊕ HCR | Empty | Empty | Empty | Empty |
| … | … | … | … | … |
| R⊕ HCR | Empty | Empty | Empty | Empty |

Figure 8- A record of Receiver's E-wallet

### E. *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.

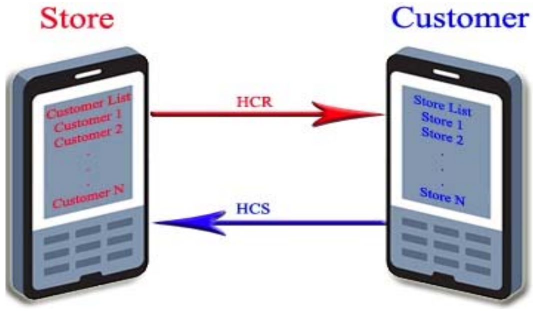


Figure 9- E-wallet connection and identification

- Payer confirms the amount of paying operation. Then payer's E-wallet software sends $\{H(CN_i)\}KS_i$, $S\oplus HCS$, $Pi\oplus PCS$ 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.

| **Receiver's Code** | **Credit No.** | **Date of Cheque** | **$P_i$ Amount** | **Payer's Code** |
|---|---|---|---|---|
| $R\oplus HCR$ | $\{H(CN_i)\}KS_i$ | $DR_i$ | $\{P_i\oplus PCS\}\oplus PCR$ | $S\oplus HCS$ |

Figure 10- A record of Receiver's E-wallet

- Receiver's E-wallet coded that the complete record again by $KR_i$ key
- Payer's E-wallet clear that record after confirmation and the amount is deducted out of "P".
- Payer's E-wallet clears all recorded of E-wallet if "P=0"

### F. *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

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

- 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.

## III. ANALYZING THE SPECIFICATIONS OF THE PROPOSED MODEL

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

### A. *Payer & 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.

### B. *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.

### C. *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 ($3/36^x$). Furthermore, by referring to the bank, payers can inform them and cancel credits.

### D. *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.

### E. *Legal Prosecution Capabilities as the same as Cheque:*

In recommended model, indeed paper cheques are presented electronically. Therefore, all documents are presentable and prosecutable.

### F. *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.

## IV. CONCLUSION

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

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

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.

## References

[1] Aashish Srivastava, Resistance to change: six reasons why businesses don’t use e-signatures, Electron Commer Res (2011) 11:357–382

[2] Adam Finn, Luming Wang & Tema Frank, Attribute Perceptions, Customer Satisfaction and Intention to Recommend E-Services, Journal of Interactive Marketing 23 (2009) 209–220

[3] A.Fakoor, “E-banking, theory & practice” Taraneh publisher, 2009

[4] Ali Sanayei, Electronic brand with attitude of management, World Science Citation Database Islam, 2011

[5] Arnd Weber, MichaelHaas, DanielScuka, Mobile serviceinnovation:AEuropeanfailure, Telecommunications Policy35(2011)469–480

[6] Arnd Weber, The convergence of mobile data phones consumer electronics and wallets: Lessons from Japan, Telematics and Informatics 24 (2007) 180–191

[7] Amit Basu a, Steve Muylle, Assessing and enhancing e-business processes, Electronic Commerce Research and Applications 10 (2011) 437–499

[8] Antonio Ruiz-Martínez, Óscar Cánovas Reverte, Antonio F. Gómez-Skarmeta, Payment frameworks for the purchase of electronic products and services, Computer Standards & Interfaces 34 (2012) 80–92

[9] Aytaç Gökmen, Virtual business operations, e-commerce & its significance and the case of Turkey: current situation and its potential, Electron Commer Res, Springer Science+Business Media, LLC 2011

[10] Barzegar, “Business guideline models & solutions in internet”, Behineh Publisher, 2001

[11] Bogdan Carbunar, Weidong (Larry) Shi, Radu Sion, Conditional e-payments with transferability, J. Parallel Distrib. Comput. 71 (2011) 16–26

[12] Business Intelligence, 2009 John Wiley

[13] Commercial Ministry http://www.moc.gov.ir

[14] Dong-Hee Shin, Towards an understanding of the consumer acceptance of mobile wallet, Computers in Human Behavior 25 (2009) 1343–1354

[15] Deputy of Planning & Economic Affairshttp://prd.moc.gov.ir

[16] Domestic websites referring to banks

[17] ECheck 2005 world wide

[18] Electronic commerce 2010, Turban, Efraim

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

[19] Electronic Commerce Expanding office http://www.ecommerce.gov.ir

[20] Electronic Payment Systems for E-Commerce Second Edition Donal O'Mahony

[21] Farya Nasiri Mofakham, "Designing and Appling E-cheque in Iran", JahadDaneshgahi Publisher, 2005

[22] Giannakis Antoniou, Lynn Batten, E-commerce: protecting purchaser privacy to enforce trust, Electron Commer Res (2011) 11:421–456

[23] Governmental Roots Certification Authority, http://www.rca.gov.ir

[24] Gregory E. Trumana, Kent Sandoeb, Tasha Rifkinc, An empirical study of smart card technology, Information & Management 40 (2003) 591–606

[25] H. Abbasnejad, "E-banking", Samt Publisher, 2010

[26] Horng-Twu Liaw, Jiann-Fu Lin, Wei-Chen Wu, A new electronic traveler's check scheme based on one-way hash function, Electronic Commerce Research and Applications 6 (2007) 499–508

[27] How to make a million, 2001, Morgan Rowland

[28] Internet Banking Comptroller's Handbook October 1999

[29] Issuing center of Public intermediate Electronic Certificate, http://www.mocca.ir

[30] J.E.M. van Nierop, P.S.H. Leeflang, M.L. Teerling, K.R.E. Huizingh, The impact of the introduction and use of an informational website on offline customer buying behavior, Intern. J. of Research in Marketing 28 (2011) 155–165

[31] Jesús Téllez Isaac, Sherali Zeadally, José Sierra Cámara, A lightweight secure mobile Payment protocol for vehicular ad-hoc networks (VANETs), Springer Science+Business Media, LLC 2011

[32] Kogilah Narayanasamy, Devinaga Rasiah, Teck Ming Tan, The adoption and concerns of e-finance in Malaysia, Electron Commer Res (2011) 11:383–400

[33] Mafruz Zaman Ashrafi, See Kiong Ng, Privacy-preserving e-payments using one-time payment details, Computer Standards & Interfaces 31 (2009) 321–328

[34] Martin G. Helander, Halimahtun M. Khalid, Modeling the customer in electronic commerce, Applied Ergonomics 31 (2000) 609}619

[35] M. Fathiyan, "E-Commerce", Atinegar Publisher, 2010

[36] Modern Banking, Heffernan, Shelagh, City University, London

[37] N.R.Sunitha, B.B.Amberker, Prashant Koulgi, Siddharth P., Secure e-Cheque Clearance between Financial Institutions, Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services(CEC-EEE 2007)

[38] RezaEbrahimi, Behzad Yahid, "applying E-cheque in E-banking system", Tabriz IT conference, 2011

[39] Sabah S. Al-Fedaghi, and Mahmoud M. Taha, Personal Informnation eWallet, 2006 IEEE International Conference on Systems, Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

[40] Sh. Bakhtiyari, “Computer, Networks & system security principals”, Sharif University, 2011

[41] Song-Zan Chiou-Wei, J. Jeffrey Inman, Do Shoppers Like Electronic Coupons? A Panel Data Analysis, Journal of Retailing 84 (3, 2008) 297–307

[42] Umberto Panniello, Michele Gorgoglione, Incorporating context into recommender systems: an empirical comparison of context-based approaches, Springer Science+Business Media, LLC 2012

[43] Vijayakrishnan Pasupathinathan, Josef Pieprzyk, Huaxiong Wang, Privacy Enhanced Electronic Cheque System, Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC’05)2005

[44] Wee-Kheng Tan, Yu-Jie Tan, Transformation of smart-card-based single-purpose e-micropayment scheme to multi-purpose scheme: A case study, Expert Systems with Applications 39 (2012) 2306–2313

[45] Wen-Shenq Juang, RO-cash: An efficient and practical recoverable pre-paid offline e-cash scheme using bilinear pairings, The Journal of Systems and Software 83 (2010) 638–645

[46] www.wikipedia.com

[47] www.usaepay.com/echeck.htm

[48] Yalin Chen, Jue-Sam Chou, Hung-Min Sun, Ming-Hsun Cho, A novel electronic cash system with trustee-based anonymity revocation from pairing, Electronic Commerce Research and Applications 10 (2011) 673–682

[49] Yoris A. Au, Robert J. Kauffman, The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application, Electronic Commerce Research and Applications 7 (2008) 141–164

[50] Yung Fu Chang, C.S. Chen, Hao Zhou, Smart phone for mobile commerce, Computer Standards & Interfaces 31 (2009) 740–747

[51] Ziba Eslami, Mehdi Talebi, A new untraceable off-line electronic cash system, Electronic Commerce Research and Applications 10 (2011) 59–66