ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

# SECURE OFF-LINE MICRO-PAYMENT SOLUTION USING RESILIENT DEVICE

G.Brindha[1],C.Dhanalakshmi[2],Mrs.A.Pandeeswari[3]M.E
[1][2]UG students,[3]Assistant Professor
Department of Computer Science and Engineering,
P.S.R.Rengasamy College Of Engineering For Womens
mail:brindhaganapathy12@gmail.com

***Abstract:***
Credit and debit card data robbery is one of the initial forms of cyber crime.Still it is one of the most common nowadays.Attackers over and over again aim at pinching such client statistics by targeting the point of sale(for short,PoS)system,i.e.The point at which a seller first acquires client information.ContemporaryPoS system are powerful computers equipped with a card reader and running expert software.Increasinglyoften,user devices are leveraged as input to possible.This paper describes FRoDO,a safe off-line micro-payment resolution that is flexible to PoS data breaches.Our resolution improves over up to date approaches in terms of elasticity and safety measures.To the best of our familiarity,FRoDO is the first resolution that can provide secure fully off-line payments while being flexible to all currently known PoSbreaches.Inparticular,we detail FRoDO structural design,mechanism and protocols.Further,a thorough scrutiny of FRoDO functional and safety properties is provided,showing its efficiency and feasibility.

## 1.INTRODUCTION

The exploration of e-cash schemes has one of the main snags in cryptography. Chaum introduced the online mysterious e-cash scheme using blind moniker. In this

handedly. In many current e-cash schemes, the bank is hypothetical to be dependable, and the insider spiteful by bank is not give attentiveness. But, some bank may become spiteful, for instance, because ofcorruptions and an interior private information disclosure due to the weakness in bank system. So, it is necessary to assess the security of e-cash schemes in terms of an insider spiteful by un-trusted ability when e-cash schemesaredeployed in the real world. For instance, Ferguson stated that the framing attack by the spiteful bank and to avoid such malevolent, suggested signing the in order replaced at a extraction etiquette.However, appears in the scheme that a user anbank want to remain information for the long time to put off challenges.

In this paper, we first portray the refuge of Chaumetal.Offline mysterious e-cash scheme. Then we describe the insider malevolent. Following the comments on offline e-cash

Fairness: The profits of the customer and the shop are not

the PoS.In these scenerios,malware that can pinch card data as soon as they are read by the device has flourished.Assuch,in case where client and seller are persistently or erratically disconnected from the network,no secure on-line payment is

**Keywords:**off-line,micropayment,transaction,client,vendor.

scheme, a bank wants to be built-in in the payment dealings so as to stop excessiveness of e-cash. Actually, a bank wants expense transactions between the user and the seller to be online. This can cause a confidential access to the bank system and it stops understanding ecash scheme. Chaum et al.Introduced the offline mysterious e-cash scheme where a bank is not want to be included in the expense contract between the user and the seller. In this scheme, the user withdraws e-cash from a bank and passes it to the seller without needing access to the bank system. When the user spends an ecash once, the obscurity of a user is surefire. But, when a user over-spends an e-cash spitefully, the bank can obtain *Id* of the user from an over-spending e-cash.In the Chaum et al, scheme *Id* of the user is entrenched in e-cash and also potted by the banks. Such vital *Id* wants to be locked in order to no spiteful. schemes, we will also analyze some of the e-cash schemes and In the state of the contradict agency relied on the asymmetric methods.As such, in cases where customer and vendor are persistently or intermittently disconnected from the network, no secure on-line payment is possible. This paper As such, in cases where customer and vendor are persistently or intermittently disconnected from the network, no secure on-line payment is possible. This paper describes FRoDO, a secure off-line micro-payment solution that is resilient to PoS data breaches. Our solution improves over up to date approaches in terms of flexibility and security. To the best of our knowledge, FRoDO is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches. In particular, we detail FRoDO architecture, components, and protocols. Further, a thorough analysis of FRoDO functional and security properties is provided, showing its effectiveness and viability.

sales.According to the above characteristics, weinclude the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

follows. Section 2 describes the cryptographic techniques used in our scheme. Section 3 presents our proposed protocol. The security issues are analysed and discussed in Section 4. Section 5 presents the conclusions.

## II.CHAUM ET AL. OFFLINE ANONYMOUS E-CASH

In this segment, we portray the Chaum et al.scheme.The bank *B* chooses the public and private keys *B Be ,d* . The moniker formed by using *B d* . This can be measured to be e-cash comparable to some quantity of money *w* . In instruct to swear obscurity of users, the bank *B* creates this cross by using the blind moniker. The user *U* and the seller *M* each have description in the bank *B* . However, Chaum et al. scheme have the following protocols.

**Withdrawal Protocol**

1. The user *U* determines the significance *U m* by using its *U Id* . The user *U* shows to the bank *B* that produced *U m* suitably without disclosing *U Id*
2. The bank *B* generates the moniker on *U m* using blind moniker and withdraws cash related to *w* from the bank account of the user *U*
3. The user *U* calculates ( ) *B U s m* as the bank *B* 's moniker on *U m*

**Payment Protocol**

1. The user *U* posts ( , ( )) *U B U m s m* to a seller *M*
2. The seller *M* checks the moniker ( ) *B U s m* and if ( ) *B U s m* is true the seller *M* posts the random confront *M c* to the user *U*
3. The user *U* calculates and passes the reply *U r* the seller *M*
4. The seller *M* checks *U r* and if true, then the seller *M* interactions goods and an e-cash with *U*

**Deposit Protocol**

1. The seller *M* passes ( , ( ), , ) *U B U M U m s m c r* to the bank *B*.
2. The bank *B* checks the bank signature ( , ( )) *U B U m s m* and the pair of the confront and reply ( , ) *M U c r* . The bank *B* saves ( , ( ), , ) *U B U M U m s m c r* in the File for prospect finding of profligacy and credits *w* to the bank account of the seller *M* .

**Over-Spender**

1.When the convinced e-cash is profligacy, the bank *B* obtains *U Id* of profligacy from the two accounts in order ( , ) *M U c r* and ( , ) ' '*M U c r* .

## III. OUR PROPOSED SCHEME

In this section, we describe an off-line payment scheme for digital content via the use of a subliminal message to verify whether a customer is legal.It is a fully off-line electronic payment systems.FRoDO customer to be free from having a bank accounts,make it also particularly a regards to privacy.Infact digital coin used in the FRoDO are just a digital version of real cash and,assuch,they are not linked to anybody else then the holder of both the identity and coin element.

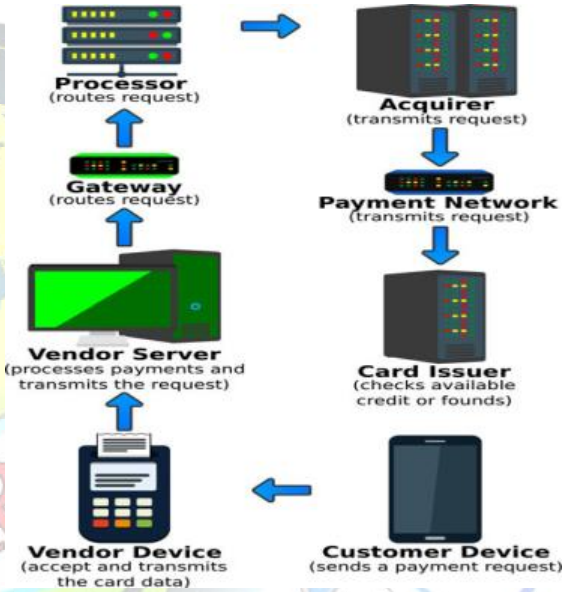
The method consists of five phases: FRoDOinitiation,the registration phase,product registration by vendor, the user transaction, the payment approval. In this paper, we assume that the transactions.

### 3.1 FRoDO Initiation:

FRoDO acts as centralized entity that connects user and vendor for their registration and payment related process.It is null key encrypted which means it can be accessed with a administrative privileges that monitors and control the activities of user and vendors.

### 3.2 Registration phase

When the customer wants to buy the digital content via the Internet, he/she should open an account in the bank. Hence the customer must go to the bank to register personal




information via secure channel as follows. The overview of the registration phase is shown in Fig. 2.

Step 1: The customer submits the actual identity himself $AC_{cid}$ to the bank.

Step 2: While the bank receives the customer's request, it generates a pseudo identity $PID_C$ and uses the arbiter's public key $e_A$ to encrypt $PID_C$ as follows

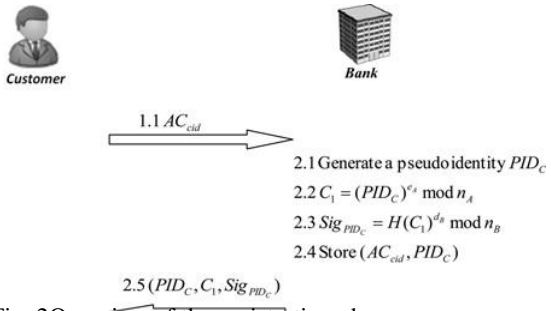



Fig. 2Overview of the registration phase

3.1 $H(C_1) \stackrel{?}{=} Sig_{PID_C}^{e_B} \bmod n_B$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

Fig. 3 Overview of the withdrawal phase computes $C_2$.

Using thepublic key $e_A$ of the arbiter and a hash value $r_1$ of $C_2$.Then, the customer continuously computes the blinded message *a* and submits *a* to the bank as follows

$$a = u_2^{eB}\, u_3\, H(r_1\ \ (u_3^{eB}\, y)) \bmod n_B$$

Step 4: Upon receiving the message *a*, the bank uses its private key $d_B$ to compute the blind signature

$$t = ((au_1)^{dBt(v)})^{-1} \bmod n_B$$

Then the bank sends (t, $u_1$) to the customer.
Step 5: Upon receiving the message, the customer computes

$$r_2 = u_1\, u_3 \bmod n_B$$

$$s = u_2^{t(v)} t \bmod n_B$$

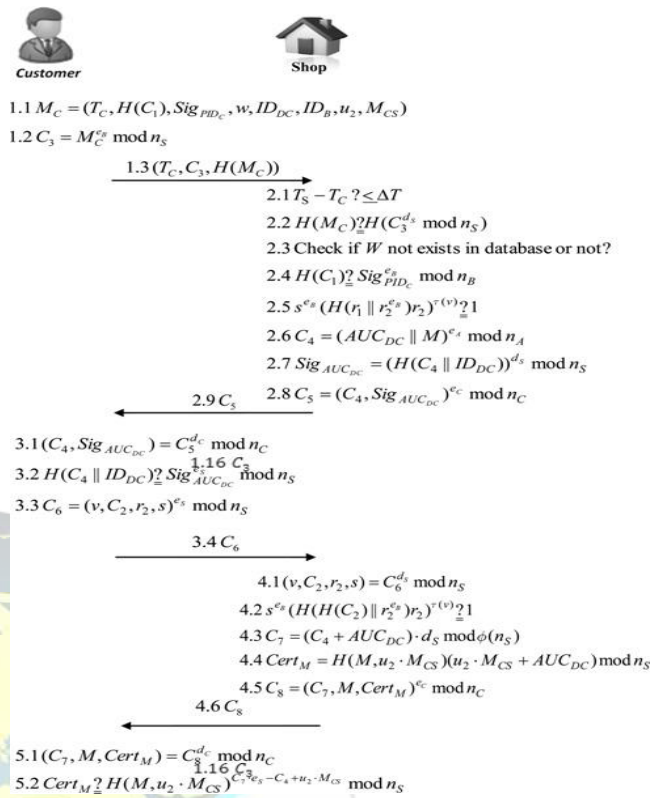
Finally, the customer stores ($u_2$,$C_1$,$C_2$,W ¼ (v, $r_1$, $r_2$, s)).

### 3.3 Product registration by vendor

Inside of vendor,products have to be added by the vendor with the specification details and the details will be updated in the vendor base which will be viewed in the user at the time of the purchase. [3] proposed a system about Efficient Sensor Network for Vehicle Security. Today vehicle theft rate is very high, greater challenges are coming from thieves thus tracking/ alarming systems are being deployed with an increasingly popularity .As per as security is concerned today most of the vehicles are running on the LPG so it is necessary to monitor any leakage or level of LPG in order to provide safety to passenger. Also in this fast running world everybody is in hurry so it is required to provide fully automated maintenance system to make the journey of the passenger safe, comfortable and economical. To make the system more intelligent and advanced it is required to introduce some important developments that can help to promote not only the luxurious but also safety drive to the owner. The system "Efficient Sensor Network for Vehicle Security", introduces a new trend in automobile industry.

### 3.4 Transaction phase

When the customer wants to purchase digital content, he/she sends a purchase message and a subliminal message to the shop. The shop signs a signature of the authorised code for digital content and uses the subliminal message to embed into the digital content. Finally, the shop sends the above messages to the customer. The overview of the transaction phase is described in.




### 3.5 Payment Approval

After entering the payment information,theFRoDO have to view the pending transcationmade by the user.Byrefering the user,The payment will be approved after refreing the coin value generated from the payment information in recorder in the base for further processing.

## IV.SECURITY ANALYSES AND DISCUSSIONS

### 4.1Security analyses

In this section, we demonstrate that the proposed protocol provides a fair and secure transaction system. Our scheme can resist known attacks.

#### 4.1.1 Replay attack issue:

If a malicious customer wantsto replay messages ($T_C$, $C_3$, $H(M_C)$) in step 1 of the transaction phase to the shop, the shop or the bank is able to detect this attempt. Suppose a malicious customer has two ways to replay messages as follows:

Case 1: If a malicious customer replays messages ($T_C'$, $C_3$, $H(M_C)$), it cannot pass the verification $T_S$ 2 $T_C$ ? ≤ DT. Case 2: If the replaying message ($T_C'$, $C_3$, $H(M_C)$) can pass the shop's verification: $T_S$ 2 $T_C$ ? ≤ DT, the shop continues to check whether W is in its database. The verification cannot

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

That is, our scheme can prevent the replay attack and can prevent double spending, when the customer uses the same withdrawal message W again in the same shop.

### 4.1.2 Conspiracy attack issue:

The most effectivesolution for the conspiracy problem is to eliminate the demand for a TTP in the protocol. TTP is not involved in each transaction; it only participates in the arbitration phase. Hence, our scheme can prevent the conspiracy attack.

### 4.1.3 DoS attack issue:

Assume that a malicious customerwants to perform the denial-of-service attack on the shop. He/ she will fail. In the transaction phase, the customer sends ($T_C$, $C_3$, $H(M_C)$) to the shop. The shop receives and decrypts the message. Then the shop verifies all the
verifications via (13) – (16). If the verifications do not hold, the shop terminates the transaction. Hence it can prevent the DoS attack.

**4.1.4 Man-in-the-middle attack issue:**In our scheme,all transferred messages between the customer and the shop are encrypted or generate signatures. The bank communicates with the customer and the shop is under a secure channel. Suppose there is an attacker who wants to modify the communication messages during the transaction, it is impossible. Hence, the main

### 4.2Unforgeability

In our scheme, the shop and the customer forge withdrawal messages (v, $r_1$, $r_2$, s) to cheat the bank for illegal benefit. The signature s of E-cash is signed by the bank. The shop and the customer cannot forgesbecause they do not know the bank's private key $d_B$.

For the authorised code of digital content $AUC_{DC}$, signing $AUC_{DC}$ should use the shop's private key $d_S$. However getting the shop's private key $d_S$ is difficult. So a counterfeit customer uses imitative $AUC'_{DC}$ to forge the authorised code $AUC_{DC}$ of digital content to pass the arbiter's verification; success is impossible. If a counterfeit customer generates a fake parameter $Sig'_{AUCDC}$ with plausible the shop's private key $d'_S$, and uses the arbiter's public key to compute $C'_4 = (AUC'_{DC} M)^{e_A} \bmod n_A$ andsends ($ID_{DC}$, $C'_4$,

$Sig'_{AUCDC}$ ) to the arbiter, the arbiter will confirm that the signature of the authorised code of digital
content$Sig'_{AUCDC}$ is not valid. The malicious behaviour will be detected as follows

$$Sig_{AUC_{DC}}^{e_S} \bmod n_S = (H(C'_4 \; ID_{DC}))^{d'_S} \bmod n_S$$

$$= H(C'_4 \; ID_{DC}) \qquad (35)$$

Hence, our protocol scheme can avoid the forgery attack for the withdrawal message and the authorised code $AUC_{DC}$ of the digital content.

### 4.3 Anonymity

In the withdrawal phase, the customer obtains a certification of the withdrawal t from the bank, and the customer transforms t into s (s

$=u_2^{t(v)}t$) with a random number $u_2$. When the customer sends the message W to the bank via the shop in the deposit phase, the bank only knows (v, $C_2$, $r_2$, s) and verifies whether the withdrawal message is valid through (23). The bank cannot know who bought the digital content unless the customer is detected to have engaged in double spending with the same withdrawal message during the transaction phase.

In the transaction phase, the customer does not send any messages related to identity. Hence, the shop also does not know who bought the digital content. Our scheme achieves the anonymous requirement.

### 4.4 Non-repudiation

1. The bank's withdrawal response message in the withdrawal phase is non-repudiation through (16) and (23).
2. The shop provides the signatures of the authorised code of digital content and certification of digital content, which are non-repudiation through (21) and (29).

### 4.5 Fairness issue

In the section, we discuss two cases for the transaction fairness via an arbitration flow chart of fairness.

Case 1: Suppose the customer receives the encrypted messages $C_5$ of the authorised code from the shop in step 2 of the transaction phase, but he/she does not send the legal payment message $C_6$ to the shop. He/she still cannot obtain the digital content and legal certification because the shop does not send the encrypted message $C_8$ of digital content.the customer, and the customer also cannot obtain any information on digital content through the fair arbitration phase. As the arbiter sends $W'$ to the bank to check whether $W'$ has been used in his database and transferred v value to the shop's account, it cannot hold; hence, the shop's profits are not harmed.

Case 2: Suppose an attacker intercepts or tampers with encrypted message $C_8$ such that the customer could not receive these messages or (29) verification fails. The customer can prove that he/she did not lie and obtain the right certification message of digital content through the fair arbitration phase. Hence, the customer's profits are not harmed.

**Discussion:**

In this section, we present the computation costs of participants.In our scheme, the customer provides the subliminal message to let the shop embed it into the digital content such that the customer can prove that he/she is the owner of the digital content in the arbitration phase. Our scheme ensures that the customer is unaware of the authorised code for digital content in the transaction phase
and the arbiter can make correct judgements without the customer and the shop's private key in the arbitration phase. That is, our scheme focuses on proposing a complete and practical fair transaction despite requiring more

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

We have provided a comparison of computation cost of a normal transaction between ours and Lin and Liu's scheme.The registration phase is regarded as anoffline model. Therefore we omit the comparison. In we can see that the proposed scheme may cost alittle in terms of computation than Lin andLiu's scheme on the client's side (customer or shop), but our scheme is to the customer, and the customer also cannot obtain any information on digital content through the fair arbitration phase. As the arbiter sends to the to the customer, and the customer also cannot obtain any information on digital content through the fair arbitration phase. As the arbiter sends to the bank to check whether $W'$ has been used in his database and transferred v value to the shop's account, it cannot hold; hence, the shop's profits are not harmed.

Case 2: Suppose an attacker intercepts or tampers with encrypted message $C_8$ such that the customer could not receive these messages or (29) verification fails. The customer can prove that he/she did not lie and obtain the right certification message of

digital content through the fair arbitration phase. Hence, the customer's profits are not harmed.

**VCONCLUSION:**

In this paper, we proposed a fair digital content transaction system based on RSA. The customer not only can transfer the subliminal

message to prove the legitimacy himself through owner arbitration when he/she is mistakenly regarded as being in illegal possession of digital content, but he/she can also protect his/her own interests through the fair arbitration. Briefly, our protocol has the following properties:

The customer proves himself as the legitimate consumer by the shop having embedded the customer's subliminal message in the digital content.

The customer can communicate with the shop securely via an insecure channel.

Does not have a TTP involved in the each transaction process; the ariter only participates in the arbitration phase.

Resists known attacks.

Achieves the common characteristics such as unforgeability, anonymity, non-repudiation, fairness and owner tracing of E-coin.

The customer and shop do not need to participate in the arbitration phase at the same time.

**VI.REFERENCES**

[1] Xuan, H.: 'A fair off-line electronic cash scheme based on RSA partially blind signature'. Proc. First Int. Symp. on Pervasive Computing and Applications, 2006, pp. 508 – 512

[2] Wang, Z.G., Wan, Z.K.: 'A secure off-line electronic cash scheme basedon ECDLP'. First Int. Workshop on Education Technology and Computer Science, Wuhan, Hubei, China, 7 – 8 March 2009, pp. 30 – 33

[3] Christo Ananth, I.Uma Sankari, A.Vidhya, M.Vickneshwari, P.Karthiga, "Efficient Sensor Network for Vehicle Security", International Journal of Advanced Scientific and Technical Research (IJST), Volume 2, Issue 4, March-April 2014,pp – 871-877

[4] Lin W.D., Jan J.K. "Security personal learning tools using a proxy blind signature scheme," *Proccedings ofInternational Conference on Chinese LanguageComputing*. Illinois, [S.l.]: KSI, 2000, pp. 273-277.