International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

High Spirited Fraud Device for Payments Phase

S.K. Maha Lakshmi[1], CH. Durga Sravani[2], SK. Aminabh[3], K.G.P. Pravallika[4], V. V. Krishna Reddy[5]
[1, 2, 3, 4, 5] *Department of IT, LBRCE*

Abstract: ***Over the last years, several retail organizations have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information. Although PoS breaches are weakening, they still remain an extremely beneficial attempt for criminals .Customer data can be used by cybercriminals for fraudulent operations, and this led the payment card industry security standards council to establish data security standards for all those organizations that handle credit, debit, and ATM cardholder information. Regardless of the structure of the electronic payment system, PoS systems always handle critical information and oftentimes, they also require remote management .The system describes Frodo, a secure off-line micro-payment solution which is resilient to PoS data breaches which acts like a high spirited fraud device for finding the attackers at a payment phase. Our solution improves over up to date approaches in terms of flexibility and security. As we know that, Frodo is the first solution which provides full secure off-line micro payment in which while being strong against to all currently known PoS breaches. In particular, we point the Frodo design, components, and protocols. Further, a systematic analysis of Frodo functional and security properties is provided, showing its effectiveness and feasibility.***

Keywords: PII, security breaches, pos systems, micro payment, Frodo design

I. INTRODUCTION

Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies. The first pioneering micro-payment [2] scheme was proposed by Rivets and Shamir back in 1996. Nowadays, crypto-currencies and decentralized payment systems are increasingly popular, development a shift from physical to digital currencies. However, such payment techniques are not yet common place, due to several unresolved Issues, including a lack of widely-accepted standards, limited interoperability among systems and most importantly security. To reduce cost and simplify administration and maintenance, PoS devices may be remotely managed over these internal networks. Mobile payment solutions proposed so far can be classified as fully on-line, semi off-line, weak off-line or fully off-line. The previous work called FORCE that, similarly to FRoDO, was built using a PUF based design. FORCE provided a weak prevention strategy based on data obfuscation and did not address the most appropriate attacks. FRoDO, a secure off-line micro-payment approach using multiple physical unclonable functions. FRoDO features like identity element will authenticate the customer, and a coin element where coins are not locally stored, but are computed on-the-fly when needed. The communication protocol used for the payment transaction does not directly read customer coins. Instead, the vendor only communicates with the identity element in order to identify the user. This simplification alleviates the communication burden with the coin element that affected our previous approach. The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e. by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to frustrate malicious users.

II. RELATED WORK

R.L. Rivets: The simple paper coin method [2] may be carried out in a diffusion of approaches, to maximise ease of for the patron in a given scenario. At the same time as the primary pepper coin method requires that each consumer have digital signature functionality, you'll easily do away with this requirement by having a celebration depended on through the consumer signal payments for him as a proxy; this might be a herbal approach in an internet services environment. The pepper coin technique can also be applied in order that it feels to the client as a herbal extension of his current credit – card processing system, further growing consumer acceptance and ease of use[1].Bomgar: Restrained interfaces and location inside local networks[3] , assisting kiosks and point of sale(pos) terminals can be challenging. Regularly they're positioned on networks that aren't connected to the internet,

making direct get right of entry to impossible for most remote support equipment . and even while an worker is present on the terminal, get right of entry to restrictions and/or loss of technical knowledge makes speaking the answer to hassle difficult. to add headaches, hackers are ramping up their efforts to scouse borrow fee card information by having access to pos structures and kiosks. Reliable ospm schema for secure transaction using mobile agent in micropayment system [5]NC Kiran: This project introduces a novel offline payment system in mobile commerce using the case take a look at of micropayments. The existing assignment is an extension version of our earlier observes addressing on implication of comfortable micropayment device deploying process oriented structural design in cellular community.

The preceding gadget has wide usage of spki and hash chaining to grant reliable and at ease offline transaction in cellular commerce. however , the modern paintings has attempted to offer much greater light weight at ease offline price device in micro – payments via designing a brand new schema termed as offline comfy price in mobile trade(ospm).the empirical operation are achieved on three varieties of transaction procedure considering most state of affairs of actual time offline cases. Consequently, the modern concept introduces new parameters i.e. mobile agent and cell token that could make certain better protection and comparatively less network overhead..

Lightweight and secure put key[7] storage using limits of machine learning: Lightweight and at ease key garage scheme using silicon physical unclonable capabilities (pufs)[8] is defined.

To derive strong puf bits from chip production variations, a light-weight mistakes correction code(ecc) encoder/decoder is used. With a sign up rely of sixty nine, this codec centre does no longer use any traditional mistakes correction strategies and is seventy five % smaller than a previous provably secure implementation, and but achieves sturdy environmental overall performance in 65nm fpga and zero. Thirteen asic implementations.

The safety of the syndrome bits uses a new protection argument that is predicated on what can't be found out from a machine getting to know attitude. The wide variety of leaked bits is decided for every syndrome phrase, reducible using syndrome distribution shaping. The design is cozy from a min-entropy perspective towards a device –mastering-prepared adversary that, given a ceiling of leaked bits, has a type mistakes bounded with the aid of. Numerical examples are given the usages of today's machine mastering effects. Building strong m-commerce fee gadget on offline wi-fi community [8] cellular commerce is considered certainly one of the imminent research regions with attention on cell rate systems. Unluckily, the present day charge structures is without delay depending on fixed infrastructure of community (cellular network), which fails to facilitate maximum tremendous level of protection for the fee gadget.

The proposed gadget highlights a unique approach for building relaxed, scalable, and flexible e-fee structures within the allotted situation of wireless adhoc community in offline mode of communication for superior protection on transaction and rate device.

The proposed device uses easy public key infrastructure for presenting the safety in price strategies. The general overall performance evaluation of the proposed model indicates that the device is surprisingly robust and cozy ensuring anonymity, privacy, non-repudiation offline charge device over wireless adhoc network.

III. EXISTING SYSTEM

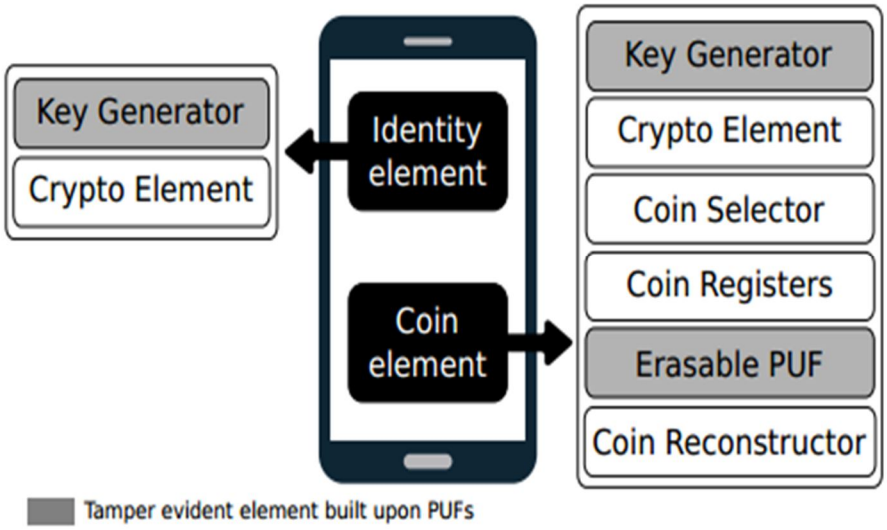
In the present system, we do online payments by means of providing our credit or debit card details or swipe our card in the vendor place where our related information like personal data can be identified by the POS vendors and might take our information. If we see the previous work Force it is for fully offline secure credits for mobile micro payments, it has some problems like it cannot find the relevant attackers, it contains some week prevention strategies. This breaches the security of our micro payments and causes a serious issue. Further this current scenario may mislead the user's potential information and can also be used to make duplicate credit or debit cards where the main information can be gathered at the POS area.

IV. PROPOSED WORK

Our proposed work Force which is a powerful device against the pos breaches which Contains the multiple and erasable Strong physical unclonable functions may perform any recomputed challenge response pair. Physical Unclonable every transistor in an integrated circuit has slightly different physical properties that lead to assessable differences in electronic properties. Process variations are not controllable during manufacturing; the physical properties of a device cannot be copied or cloned. As such, they are unique to that device and can be used for authentication purposes. The first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide strong against to frauds based on data breaches in fully off-line electronic payment systems. By allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to confidentiality.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

V. ZSYSTEM DESIGN



In this design, we develop the Identity Element module functionalities. FRoDO does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device. Similarly to secure elements, both the identity and the coin element can be considered tamperproof devices with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e., APIs) are not central to the security of our solution and can be easily and constantly updated. This renders infrastructure maintenance easier. we develop Coin Element. In this coin Element we develop Key Generator and Cryptographic Element. The Key Generator is used to compute on-the-fly the private key of the coin element. The Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element. The Coin Selector is responsible for the selection of the right registers used together with the output value computed by the coin element PUF in order to obtain the final coin value. The Coin Registers used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data. Coin seeds are used as input to the PUF whilst coin helpers are used in order to reconstruct stable coin values when the PUF is challenged. Attack Mitigation, in this module we develop the Attack Mitigation process. The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors. The private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/ public key pair. However, identity/coin element public keys are valiantly if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately rejected .Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins

VI. IMPLEMENTATION

In this system, in order to get the fruitful results we use two algorithms and the modules involves in this system are stated below.

A. Vendor module (bank authority):

In this module, there are n numbers of Vendors are present. Vendor should register by selecting bank before performing any operations. Once Vendor registers, their details will be stored to the database. After registration successful, he has to login by using authorized Bank Name, user name and password. Once Login is successful Vendor can perform some operations like viewing their profile details, Viewing Their Corresponding Bank Users and Authorizing them for login and for account creation, Viewing Users Requests to generate Account Numbers, Viewing all their user's bank details and mini statements and viewing all user deposit, withdraw, transfer requests.

Fig.6.1.1 Represents Vendor module

B. User Module

In this module, there are n numbers of users are present. User should register by selecting bank name and finger print image before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using bank name, finger print image, user name and password. Once Login is successful user can perform some operations like viewing their profile details with Finger print, sending request for private key, sending request to generate account number, depositing amount, transferring amount, withdrawing amount, checking Mini Statements, and Viewing all account details from particular date to date.

C. Frodo Module

In this module, the FRoDO has to login by using valid user name and password. After login successful he can perform some operations such as Viewing all Users with Private Key and their Finger Prints, Verifying Finger Prints and Private Keys and Sending Transaction Requests to Corresponding (Vendor) Bank Authority.
Generating the private keys for the allowed users

Fig 6.2.1 Represents FRoDO Module

D. Puf Module

In this module, the PUF has to login by using valid user name and password. After login successful he can perform some operations such as Viewing all Users with Finger Prints and giving permissions for their Money Transactions and Listing, Encrypting All User Account Numbers.

Fig 6.3 Represents Puf Module

E. AES Algorithm

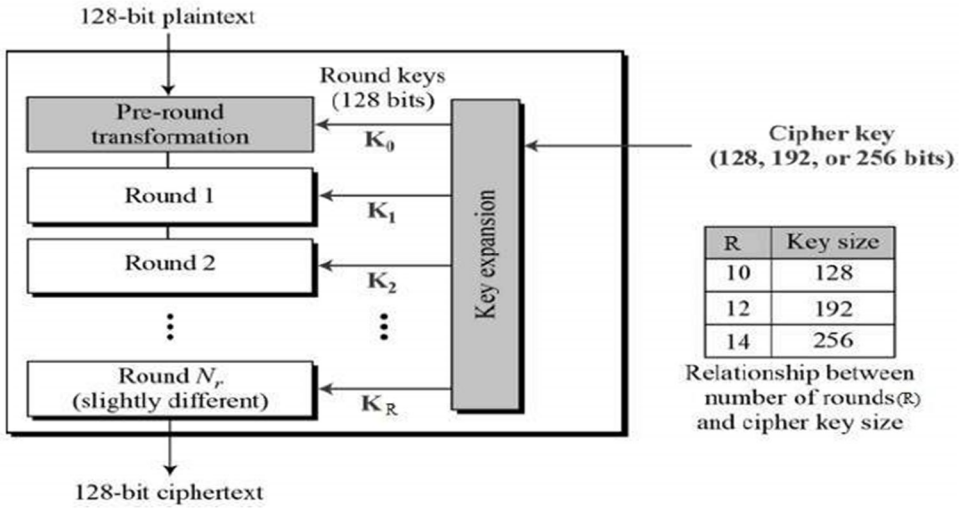
The main objective of this algorithm is to encrypt as well as decrypt the input given to it.

F. Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.The schematic of AES structure is –



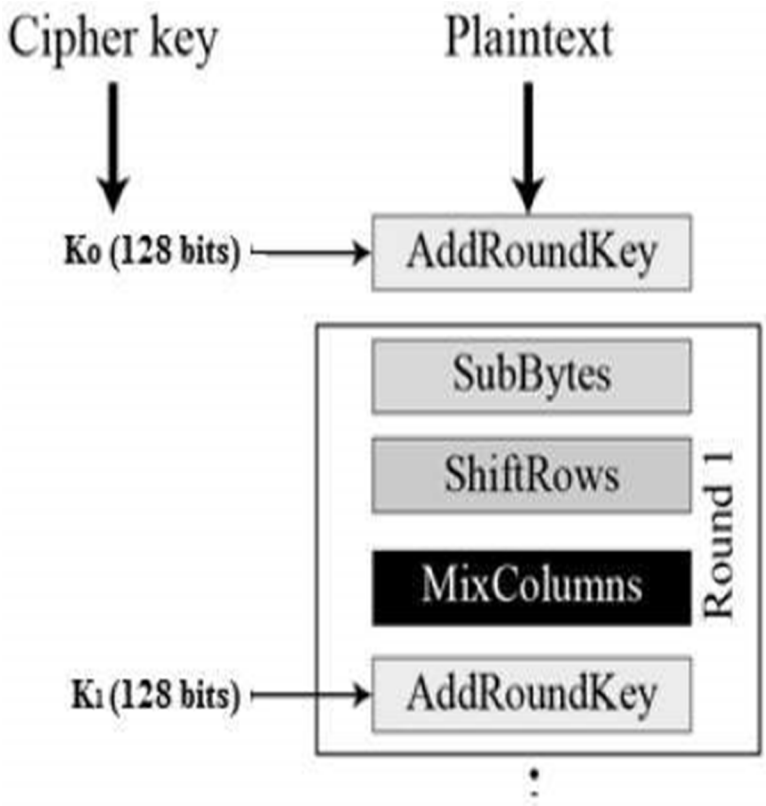
R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

G. Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com



H. Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

I. Shift Rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

First row is not shifted.

Second row is shifted one (byte) position to the left.

Third row is shifted two positions to the left.

Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

J. Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

K. Add Round key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

L. Decryption Process

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

Add round key

Mix columns
Shift rows
Byte substitution
Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

M. RSA Algorithm

The main objective of this algorithm is to generate digital signature key and secret key which play a major role in uploading the data to server and downloading the data from the server i.e. when a file is uploaded to server it generates digital signature and secret key to that image or file.

N. Operation of RSA algorithm:

Choose public exponent e to be co-prime to $(p-1)(q-1)$, with $1 < e < (p-1)(q-1)$. The pair (n, e) is the public key

The private key is the unique integer $1 < d < (p-1)(q-1)$ such that $ed = 1 \bmod (p-1)(q-1)$. Encryption: Split a message M into a sequence of blocks M1, M2, . . . , Mt where each Mi satisfies $0 \leq Mi < n$. Then encrypt these blocks as

$$C = E(M) = Me \pmod{n}; \quad (1)$$

Decryption: Given the private key d and the cipher text C, the decryption function is:

$$D(C) = Cd \pmod{n}; \quad (2)$$

Note that encryption does not increase the size of a message. Both the message and the cipher text are integers in the range 0 to n - 1.

The encryption key is thus the pair of positive integers (e; n). Similarly, the decryption key is the pair of positive integers (d; n). Each user makes his encryption key public, and keeps the corresponding decryption key private.

Algorithms we use in this project are

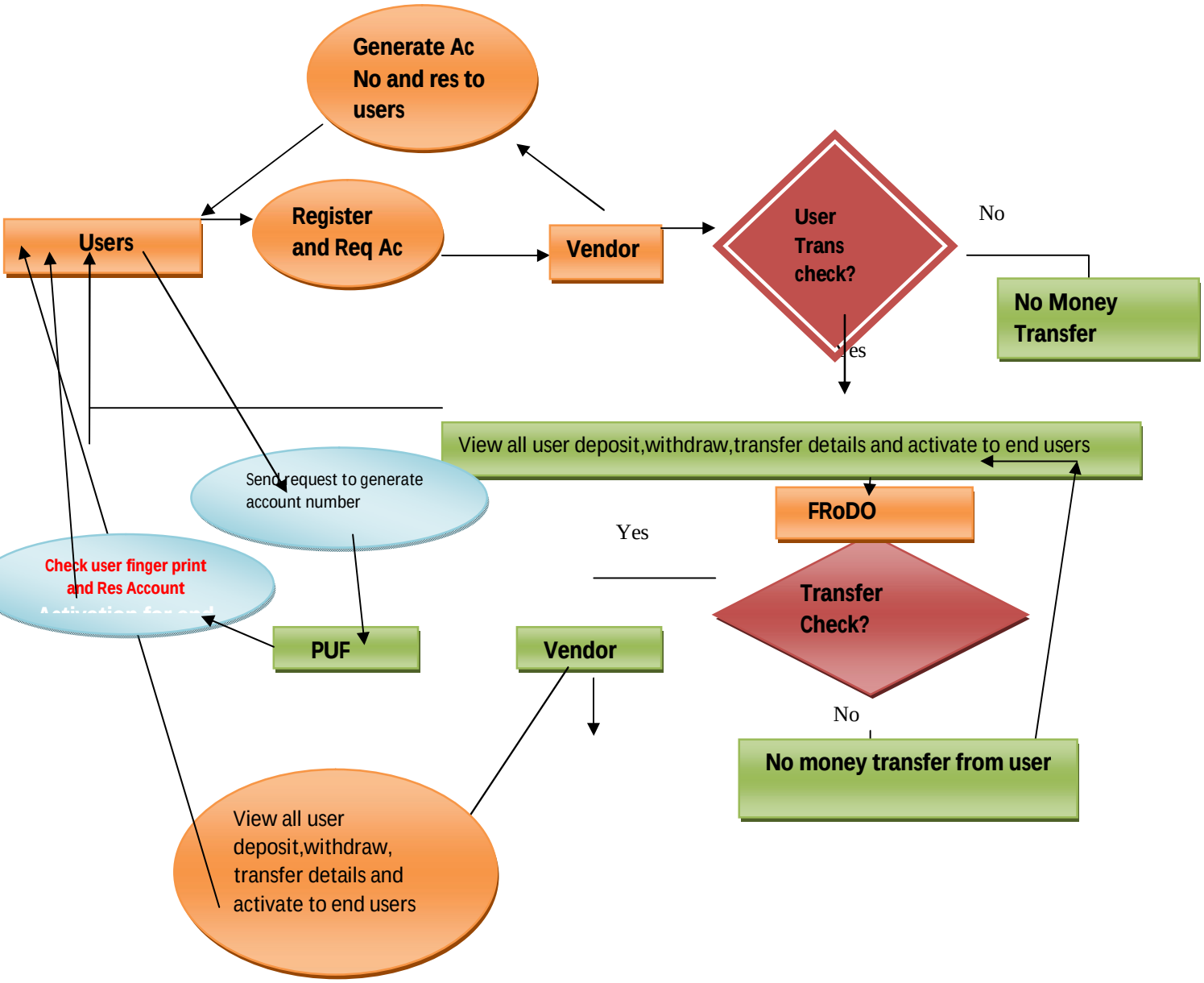
1) *Bit Exchanging Method:*encryption taken on the name of the game message documents the usage of easy bit shifting and xor operation. the bit trade approach is introduced for encrypting any document.

Algorithm
step 1: examine the all content and locate the all individual to covert the ascii value
step 2: that ascii price transformed in binary fee
step 3: encryption taken on the secret message document the use of simple shifting and xor operation. like a 1001110.
step 4: the bit alternate method is added for encryption any document
step 5: examine one at a time byte from the secret information and convert every byte to 8 bits. then practice one bit proper shift operation. like this 0100 1110.
step 6: divide the eight bits into to dam after which carry out xor operation with four bit on the left and four bits at the proper side(1010).
step 7: the same element repeated for all bytes within the file.

2) *Payment section:* The force price section is depicted and it's far composed by using the following steps the consumer sends a purchase request to thevd inquiring for some goods.the vendor computes the entire amount and sends it returned to the consumer. encsalt(req)=creq
3) the patron exams for the quantity and either confirms or denies the transaction. if the transaction is showed, the cd creates a reply for the vd with the indexes of all of the credits which are still to be had in the card. if the ith index quantity is present within the respond, it means that the ith credit score check in can be examine with the intention to retrieve the ith digital credit inside the card.

credit price is correct, a brand new entry is saved inside the storage tool of the vendor after having being encrypted with the non-public key.

Data flow diagram



VII. SECURITY ANALYSIS

A. *Authenticity*

It is assured in FRODO by the on-the-fly computation of private keys. Literally, both the identity and the coin component utilize the Key generator to figure their private key needed to encode and decode every one of the messages exchanged in the convention. Furthermore, every open key Used by both the merchant and the identity/coin component is signed by the bank. As such, its authenticity can always be verified by the merchant.

B. *Availability*

The availability of the proposed arrangement is guaranteed predominantly by the fully off-line Scenario that totally get rid of any form of external correspondence requirement and makes it desirable to use off-line digital coins likewise in extreme situations with no organize scope. Furthermore, the lack of any enlistment or withdrawal phase, makes FRODO ready to be used by numerous devices.

C. Confidentiality

Both the interchanges among the purchaser and the merchant and people between The individual component and the coin thing use awry encryption primitives to perform message privacy.

VIII. CONCLUSION

In this paper we have introduced FRODO that is, to the best of our knowledge, It is the first solution which is strong against the attackers at time of transaction. The security study shows that FRODO does not impress consistency assumptions. Further, FRODO is also the first solution in the literature where no customer device data attacks can be broken to compromise the system. This has been done because of mainly by leveraging a novel erasable PUF design and a novel protocol design. in addition, our application has been systematically discussed and compared beside the state of the ability. Our study shows that FRODO is the only proposal that enjoys all the properties required to a secure micro- payment solution, while also introducing flexibility when allowing for the payment standard. Our investigation describes that FRODO is the main proposal that appreciates every one of the properties required to a confined smaller scale instalment preparation, while likewise presenting flexibility while allowing for the instalment medium.

REFERENCES

[1] VanesaDaza, Roberto Di Pietro, Flavio Lombardi, And Matteo Signorini “Off-Line micro-Payments”, Dependable And Secure Computing, IEEE Transactions On (Volume:PP , Issue: 99), 12 June 201
[2] R. L. Rivest, “Payword and micromint: two simple micropayment schemes,” in CryptoBytes, 1996, pp. 69–87
[3] W. Chen,G. Hancke,K. Mayes,Y. Lien, and J.-H. Chiu,“Using 3G network components to enable NFC mobile transactions and authentication,” in IEEE PIC ’10, vol. 1, Dec 2010, pp. 441 –448
[4] T. Nishide and K. Sakurai, “Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited,”ser. INCOS’11.Washington, DC, USA: IEEE Comp. Soc., 2011, pp.656–661
[5] M. A. Salama, N. El-Bendary, and A. E. Hassanien, “Towards secure mobile agent based e-cash system,” in Intl. Workshop on Security and Privacy Preserving in e-Societies. New York, NY, USA: ACM, 2011, pp. 1–6
[6] B. Kori, P. Tuyls, and W. Ophey, “Robust key extraction from physical uncloneable functions,” in Applied Cryptography and Network Security,ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 407–422
[7] M.-D. Yu, D. MRaihi, R. Sowell, and S. Devadas, “Lightweight and Secure PUF Key Storage Using Limits of Machine Learning,” in CHES 2011, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373
[8] U. Rhrmair, C. Jaeger, and M. Algasinger, “An attack on PUF-Based session key exchange and a hardware-based countermeasure: Erasable PUFs,” in Financial Cryptography and Data Security, ser. LNCS. Springer, 2012, vol. 7035, pp. 190–204.