# Offline Payment System Using Multi-Level Endorsement Mechanism

**Sowmiya Devi.S[1], Rajashree.G[2], Balakumar.P[3], Veera Lakshmi. P[4]**
[3,] 4associate Professor, Dept of Information Technology
[1, 2]Dept of Information Technology
[1, 2, 3, 4] Prince Shri Venkateshwara Padmavathy Engineering College , Chennai.

***Abstract-*** *In 2016 Android accounted for more than 80 percent of all smartphone sales to end-users worldwide(source-google). This can be utilised to perform a digital transaction anywhere and at anytime.This is an offline payment system using Multilevel Endorsement Mechanism(MLE) which has the potential to provide digital transaction for disaster areas. We introduce a new mobile payment system that utilizes infrastructure less mobile adhoc network (MANET), since we cannot depend on communication infrastructures at the time of disasters. specifically this paper holds a surety scheme to avail transaction whenever the user bank account has minimum balance. This system has been developed to provide an secure digital transaction by the use of QR codes to meet the challenges faced by the people at disaster times. As validated by simulation this system is a robust and secure which also prevents double spending, by the use of transaction log checking scheme, to prevent this attack before the completion of transaction.*

***Keywords***- offline payment, endorsement, MANET, double spending, surety.

## I. INTRODUCTION

In recent times ANDROID is most commonly used OS. It is a powerful Operating System supporting a large number of applications in Smart Phones. These applications make life more comfortable and advanced for the users. It enables reuse and replacement of components and it is optimized for mobile device. More than 80% of users are using android in worldwide. India is moving towards digital economy but still there is internet connection in rural areas. So we mainly focused on offline transaction. There are more offline payment system which enable transaction. But some issues are still there. We mainly focused on Network disconnection and lack of security, for that we using MANETs which is an infrastructure less network and we using multi endorser scheme to reduce the communication overhead.In general offline transaction also known as a signature debit transaction is a payment method that uses a credit card transaction .In this system,entire user bank balance will be synchronized with our application. We can efficiently use the money for a future transaction also.

## II. RELATED WORK

Several studies have been made regarding to offline payment. We refer the PAYSE application to ensure the secured payment in offline mode. It is the world's first offline cash so,ution but, we need to buy a portable device named purse which stores the offline cash. Indian government introduced the USSD system acts like a offline payment but USSD codes are not memorable as short codes.[1]using endorsement based approach to initiate the transaction in offline mode.[2] proposed a novel approach to provide a secured e-payment system using public key infrastructure. [3] introduced an offline payment transaction between a vehicle and a merchant using VANET where a constant link is required between a merchant and bank to complete a transaction and it has the limited connectivity and bad performance for long distance between the source and the destination [4] introduced an offline payment mechanism, uses debit based payment protocol to buy digital goods. This system adopts the Dai's mechanisms. Shyamasundar and patil [5] introduced an offline electronic coupon micro-payment mechanism. Their mechanism is based on credit and allows users to delegate their ability to pay for an item to another person device. The electronic coupon scheme delegation protocol is based on multiseed pay-word chains. Their scheme mainly focuses on minimizing the computational cost of mobile devices with limited resources. [6] proposed a scheme that focuses on e-payment systems with electronic cash. To reduce a merchant's burden of having an account for depositing electronic cash received from customers with multiple banks. [7]proposed a 2-Dimensional payment solution to provide a reliable transaction.[8]introduced a EMV(Europay Master Card Visa) to perform a secure offline transaction using end-to-end transaction.[9]introduced a offline communication between the two devices by using NFC technique. It is a short-range wireless communication technology without internet connection. [10] They introduce the endorsed e-cash using multiple e-coins protocol to provide the optimistic fair exchange of goods and services.

## III. MOBILE PAYMENT SYSTEM

In this previous Mobile payment system in a disaster area have the potential to provide electronic transactions for people purchasing recovery goods like foodstuffs, clothes, and medicine. Conversely, to enable transactions in a disaster area, current payment systems need communication infrastructures (such as wired networks and cellular networks). At that time the communication networks may not be available so transaction will not performed fulfilled at the users. And physically roads may be blocked no direct connection to the bank during transaction. it is impossible to get physical cash, which a customer needs to pay for the item being purchased since access to the bank is restricted due to destruction of bank infrastructure and communication. Hence, a customer cannot make a direct transaction with the merchant.

## IV. MULTI-LEVEL ENDORSEMENT MECHANISM

In this proposed system will provide the infrastructure less network between user and bank during disaster to provide payment guarantees for a customer-to-merchant transaction and a multilevel endorsement (MLE) mechanism with a reduce communication overheads. Furthermore, payment systems are developed to provide electronic currency services .our secure payment system is centered on enabling offline transactions utilizing MANETs. In designing such an MANET-based payment system, we introduce a multilevel-endorser scheme to sufficiently cover transaction amount. And then we use QR code transaction with a digitally signed photograph is proposed for authentication and to restrict an attacker from carrying to avoid duplicate QR transaction. The crowd sensing road monitoring information is useful for all users.

## V. SYSTEM OVERVIEW

### 5.1 Bank account creation

In this first module user and merchant will create a bank account .And then user will deposit amount in his account. The customer submits the list of users that will serve as his/her endorsers in the system before disaster occurs. In the disaster time if user's account is under minimum balance ,then system will get the amount from the endorser’s account.we are using QR code generation algorithm where the identity of the merchant gets converted as a QR code and used for verification by the user at initiation of the product purchase.
QR Code (Quick Response Code) is developed by Denso Corporation developed a QR code in 1994 , the QR code is shown in Fig. 1. QR Code has 40 versions on that four levels are error correction, and the maximum symbol size can encoding 7089 numeric data or 4296 alphanumeric data. It allows recovery of 30% of the symbol words. The advantage of QR code is listed below

1) QR Code has high capacity encoding of data, its maximum encoding capacity is 7089 characters
2) It has High-speed reading capacity Adapted with CCD reading, it can recognize more QR Code symbol per Second.
3) QR code is a two dimensional barcode it can be read direction(360 degree)
4) Readable from any direction from 360 degree QR Code is a matrix two-dimensional barcode; it can be readable from any direction from 360 degree.

Fig. 1. Example of QR Code symbol

### 5.1.2 Encoding of QR code:

Each QR Code symbol consists of an encoding region and function patterns, as shown in Fig. 2. Finder, separator, timing patterns and alignment patterns comprised function patterns. Function patterns shall not be used for the encoding data. The finder patterns located at three corners of the symbol intended to assist in easy location of its position, size and inclination.

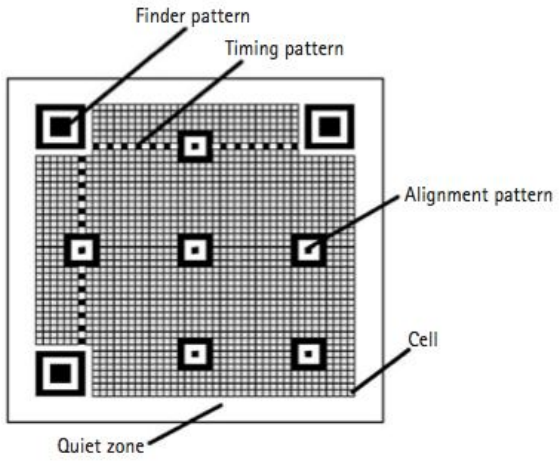


Fig.2The structure of QR Code

The encode procedure of QR Code including follows steps. Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into code words. Then code words are divided into blocks, and add error correction code words to each block. All these code words are put into a matrix and are masked with mask pattern. Finally function patterns are added into the QR symbol. A QR Code symbol is formed.

**5.1.1 Merits of QR code:**

1) Error Correction: This feature renders the QR Code scannable even if it has been damaged by up to 30%
2) Personalized Designs: You can add colours, a logo, image, or background image on a QR Code to personalize it.

**5.2 USER PURCHASE REQUEST**

In this second module user will register this application with username, and password. User scans the merchant QR code which includes merchant name, address, email, mobile number, etc to connect with the merchant. Once product purchase request have been initiated, then the request hits the bank server through mobile to mobile communication (in a secured way. ie., hash code), it will check information if valid, then the system will generate the QR code.

**5.3 PRODUCT PURCHASE REQUEST**

User can initiate a product purchase request by providing the product details and amount need to be paid to the merchant. On clicking the submit button the request starts to traverse through the near-by endorser and hits the bank server. Thereby it validates the request by checking the time stamp and converts the requested amount as digital currency (ie., QR Code).This is done using Base64 algorithm. Base 64 which converts the binary data into text format that represent binary data in an ASCII format by using radix-64 representation.

Table 1:ASCII code

| Value | Char | value | Char | value | char | value | char |
|---|---|---|---|---|---|---|---|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | A | 42 | q | 58 | 6 |
| 11 | L | 27 | B | 43 | r | 59 | 7 |
| 12 | M | 28 | C | 44 | s | 60 | 8 |
| 13 | N | 29 | D | 45 | t | 61 | 9 |
| 14 | O | 30 | E | 46 | u | 62 | + |
| 15 | P | 31 | F | 47 | v | 63 | / |

Steps involved in Base64 Algorithm:

1) Take the 3 bytes from the input.
2) Split into 3bits of 4 block and covert into decimal value.
3) Using base64 encoding table translate into ASCII sequence.
4) Refer the ASCII code in Table.1. Search for binary number 8 bits of the ASCII code. Combine the last 8 bits to form 24 bits. Then split a 24 bits into 6 bits.It will produce four fractions. convert each fragment into a corresponding decimal value. Make the decimal value to an index to choose a character constituent of base64 and the maximum is 63 The total bit is 48 bits i.e) 6*8=48. This 48 bits will be divided into eight parts of 6-bit characters or 64 to

the index.This section will analyze the Base64 algorithm. The plaintext will be encoded into ciphertext and then decoded into plaintext back. Assume the plaintext is "Update". It has six characters.

Table 2: BASE64 example

| Index | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Char | U | p | d | a | T | e |
| Decimal | 85 | 112 | 100 | 97 | 116 | 101 |

The illustration in Table 2 shows the explanationBase64 example.

The calculation:

Index 1 : U ASCII : 85 Binary : 01010101
Index 2 : p ASCII : 112 Binary : 01110000
Index 3 : d ASCII : 100 Binary : 01100100
Index 4 : a ASCII : 97 Binary : 01100001
Index 5 : t ASCII : 116 Binary : 01110100
Index 6 : e ASCII : 101Binary : 01100101

The concatenation of the binaries is 010101010111000001100100011000010111010001100101.T able 3 shows the final binary bit of the previous example. The amount of the plaintext is six characters.

This will be eight characters in Base64 format. The ciphertext is VXBkYXRl based on Base64 character table.

Table 3: bit binary

| INDEX | BINARY 6-BIT | CHAR |
|---|---|---|
| 1 | 010100 | 20 |
| 2 | 000111 | 7 |
| 3 | 010101 | 21 |
| 4 | 110100 | 52 |
| 5 | 011001 | 25 |
| 6 | 010111 | 23 |
| 7 | 001001 | 9 |
| 8 | 100001 | 33 |

**5.4 Road Monitoring System**

This module is used to update details related to disaster such as(flood, water stagnation, internet connectivity, food packet delivery, road condition, traffic details, accident zone, restricted area etc). Any user who owns this application can update related information. Once clicking onto the update button the user can type the information and submit it, such that it reaches all the user owning the same application in offline mode.

## VI. SYSTEM ARCITECTURE

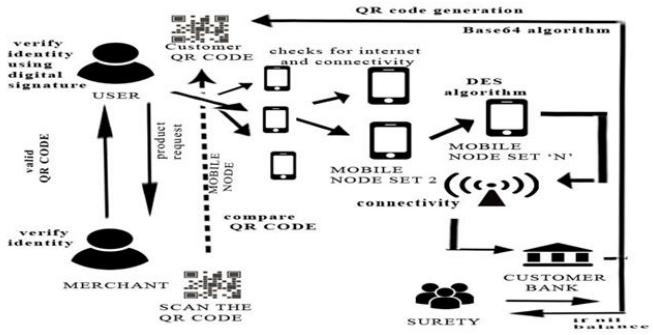


Fig.3 System Architecture

At first the user verifies the merchant's details by scanning the QR code given by the bank. once the verification is valid ,user initiates the product purchase request by providing the amount payable to the merchant. This request hits the bank server in a secured way using DES algorithm through the multiple endorsement based mechanism where the mobile nodes acts as the endorsers. This request checks for the internet connectivity in the endorsers mobile, if available it reaches the bank server thereby gets converted into digital currency(ie.,QR code)using QR code generation algorithm and sent to requested user's mobile. This QR code has to be scanned by the merchant and on updating the product name and price .this again reaches the bank server through the same mechanism in which the request will be cross checked using the timestamp that has been generated at initial stage to avoid double spending. once it is verified the amount gets credited into merchant's bank account. this application allows the user as well as the merchant to verify their bank account balance and additionally the merchant can view a mini statement of the purchase that has taken place.

## VII. CONCLUSION

In this paper, we proposed a new mobile payment system which provides a secured payment for every transaction between the customer and merchant using mobile adhoc networks.It ensures security by adopting various

schemes like the Bloom filter, the blind signature, the event chain, plus location information-based Monitoring and also prevents fraudulent transaction, collusion, reset and recovery attacks, impersonation of users and double spending. The system also reduces merchant overhead and transaction completion time.

In future, to achieve more coverage implement "LOON FOR ALL". It is a google product provides internet for everyone. Project Loon balloons approximately travel in the stratosphere and 20 km above the Earth's surface in the stratosphere. Based on the stratosphere atmosphere and the wind's speed , balloon direction varies. Project Loon uses software algorithms to determine where its balloons need to go.

## REFERENCES

[1] B. Ojetunde, N. Shibata, J. Gao, and M. Ito, "An endorsement-based mobile payment system for a disaster area," in Proc. 29th IEEE International Conference Advanced Inf. Netw. Appl. (AINA), Gwangju, South Korea, Mar. 2015, pp. 482–489.

[2] N.C. Kiran and G.N. Kumar, "Building roust m-commerce payment system on offline wireless network," in IEEE International Conference on Advanced Telecommunication Systems and Networks(ANTS),Bangalore,2011, pp.1-3.

[3] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," Comput Commun., vol. 35, no. 2, pp. 188–195, 2012.

[4] X. Dai, O. Ayoade, and J. Grundy, "Off-line micro-payment protocol for multiple vendors in mobile commerce," in Proc. 7th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT), Taipei, Taiwan, 2006, pp. 197–202.

[5] V. Patil and R. K. Shyamasundar, "An efficient, secure and delegable micro-payment system," in Proc. IEEE Int. Conf. e-Technol. e-Commerce e-Service (EEE), Taipei, Taiwan, Mar. 2004, pp. 394–404.

[6] Y.-Y. Chen, J.-K. Jan, and C.-L. Chen, "A novel proxy deposit protocol for e-cash systems," Appl. Math. Comput., vol. 163, no. 2, pp. 869–877,2005.

[7] J. Gao, V. Kulkarni, H. Ranavat, L. chang and H. Mei," A 2D Barcode-Based Mobile Payment System," in 2009 Third International Conference on Multimedia and Ubiquitous Engineering Qingdao,2009,pp. 320-329.

[8] D. Jayasinghe, K. Markantonakis, I. Gurulian,R.N. Akram and K. Maye,"Extending EMv Tokenised Payments to Offline-Environments," 2016 IEEE Trustcom/BigDataSE/ISPA,Tianjin,2016,pp. 443-450.

[9] Aye Mi San and Chnaboon Sathitwiriyawong, "Privacy-preserving offline mobile payment protocol based on NFC" in computer science and engineering conference(ICSEC),2016,pp.1-5.

[10] J.Camenisch, A.Lysyanskaya and M.Meyeovich, "Endorsed E-cash", in IEEE symposium on security and privacy(sp '07),Berkeley, CA, 2007, pp.101-115.