ADAPTATION AND USABILITY OF QR CODES FOR SUBSCRIPTION TO MOBILE NETWORK OPERATORS SERVICES

Article · March 2018

CITATION
1

READS
358

4 authors, including:

AKANDE NOAH OLUWATOBI
Landmark University
46 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Oladiran Tayo Arulogun
75 PUBLICATIONS **390** CITATIONS
SEE PROFILE

Oyediran Mayowa
Ladoke Akintola University of Technology
16 PUBLICATIONS **21** CITATIONS
SEE PROFILE

ADAPTATION AND USABILITY OF QUICK RESPONSE CODES FOR SUBSCRIPTION TO MOBILE NETWORK OPERATORS' SERVICES

[1] Akande Noah Oluwatobi, [2] Arulogun Oladiran Tayo,
[3] Adeyemo Isiaka Akinkunmi, [4] Oyediran Mayowa Oyedepo

[1] Department of Computer Science, Landmark University, Kwara State, Nigeria
[2] Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Oyo State, Nigeria
[3] Department of Computer Science, University of Nigeria, Enugu State, Nigeria
[4] Department of Electrical, Electronic and Computer Engineering, Bells University, Ota, Nigeria

Corresponding Author: akande.noah@lmu.edu.ng

ABSTRACT: Mobile Network Operators (MNOs) permit subscribers to gain access to data, voice calls or short messaging services offered by their networks. Payments for any of these services could be via online payments platforms, short codes provided by financial institutions or the acquisition of recharge vouchers. Of these payment methods, the recharge voucher acquisition option remains the most widely used. However, illegal access to the recharge codes has not been totally eradicated and this has marred the recharge vouchers payment method. Therefore, this paper examined and demonstrated the feasibility of employing Quick Response (QR) code as a more secured payment alternative to recharge vouchers. Twitter fabric's crashlytics tool was used to evaluate the performance of the developed QR code mobile payment method for a three month periods. A successful payment attempt and crash free sessions were experienced among 48 volunteers who used the application in 125 sessions.
KEYWORDS: Mobile Payment Systems, Mobile Network Operators, Quick Response codes, Recharge Vouchers.

1. INTRODUCTION

Mobile payments as an alternative to cash transactions, credit cards or cheque can be traced back to early 1990's when the first transaction was conducted on a mobile device ([DGO15]). It involves the use of mobile devices and its communication technologies (especially wireless) for payment of bills, goods and services ([D+08]). This could be done remotely or within a close distance ([UM15]). However, technical know-how, customer's trust of the transfer process ([L+11]; [Y+15]), consumer's willingness to adopt the technology ([AMA16; [KDZ16]; [O+16]), information and service quality ([CL16]), country-level institutional constraints ([Mag14]), customer's satisfaction ([XPP15]), perceived ease of use ([T+16]) and usefulness ([Soh17]), security ([KZ07]; [YKL18]) among others are some of the factors militating against mobile payment system. Nevertheless, the extensive usage of mobile devices and its continuous propinquity to consumers have made them appropriate for mobile payment services ([Mal07]).

Furthermore, the impact of mobile phone technologies in individual's daily activities and across different sectors of Nigeria cannot be underestimated. Though it has been proved that consumers tend to abandon a new technology if it has difficult usage instructions ([OPL14]), yet mobile devices have practically become the most cherished tool for communication and social interaction. Besides the provision of access to communication through voice calls, access to data services indirectly connects individuals to internet and the benefits therewith. A report released by the Nigeria Communications Commission (NCC) in June 2017 revealed that Nigeria has 241,000,790 connected lines placing it as the 5th users of mobile phone in the world ([***17c]). Of this, 236,895,278 people use mobile Global System for Mobile Communication (GSM) while 3,586,095 people use mobile Code Division Multiple Access (CDMA). 342,011 people are connected on fixed/wireless medium while the remaining 177,406 use voiceover internet facilities. In summary, Nigeria has 143,064,490 active lines which demonstrate the degree of acceptability and usage of mobile phones and its services in Nigeria. However, none of these services is free; an intending user must subscribe to a Mobile Network Operators (MNOs) of interest. As further reported by NCC in June 2017, MTN Nigeria communications remains the leading telecoms provider with 53,102,463 subscribers while Globacom limited has 37,424,154 subscribers as at June 2017. Airtel Nigeria can boast of 34,656,605 subscribers while EMTS Limited (9mobile) can boast of 18,022,674 subscribers. Other six telecommunication operators share the remaining 141,406 subscribers.

2. RELATED WORKS

Seven core actors of Mobile Payment Systems (MPS) were identified by Fun, Beng, & Razali, ([FBR13]); they are: Payment Service providers, Device Manufacturers, MNOs, Regulators, Financial Service Providers, Payer and Payee. However, Kungpisdan, Srinivasan, & Le, ([KSL03]) identified five major parties in every MPS; they are: the issuer, acquirer, the merchant, client and the payment gateway. On the contrary, Pukkasenung & Chokngamwong, ([PC16]) identified only three parties in every mobile payment transaction, they are: the seller, the payment channel and the buyer. These discrepancies are as a result of the diversities in mobile payment schemes. Nevertheless, four technologies were recognized by Chen & Li, ([CL16]) to be the backbone of every MPS; they are: QR code, Near-Field Communication (NFC), Wireless Application Protocol (WAP) and Short Message Service (SMS). The SMS option entails the exchange of short text messages containing payment requests in a specified format between the subscriber and the MNOs. A response is expected to ascertain if the request is granted or denied. If granted, deductions are expected to be made from the subscribers account. Lugo, ([Lug12]) was of the opinion that paper vouchers have been characterized with voucher fraud and misuse thereby a SMS voucher was implemented in their study as a better alternative. Similarly, SMS payment system called M-Wallet which strictly uses text messages for conducting transactions was introduced by Rai, Ashok, Chakraborty, Arolker, & Gajera, ([R+12]). For each transaction conducted, a unique one-time password is sent to subscriber's mobile number is used to prevent spoofing and replay attacks.

A SMS based mobile mini-payment scheme was introduced by ([FL16]). The scheme allows MNOs to serve as a Payment Service Provider (PSP) that charges certain consumers on behalf of an external merchant using their billing infrastructure. To guarantee security of transactions, subscribers are expected to authenticate themselves using a PIN before any transaction will be completed. A similar payment method was introduced by Gemalto - a smart card manufacturer which allows its subscribers to carry out payment using SMS. Subscribers are expected to provide their banks PIN in order to authenticate every transaction. In SMS payment method, the privacy of subscribers is not guaranteed as they are expected to reveal their identity during transaction. By default, the confidentiality and integrity of SMS content is not guaranteed, therefore transactions using SMS is not entirely secure and reliable ([Al-J16]). Furthermore, lack of transaction confirmation, reduced capacity of transmission due to 160 characters limits and several unsuccessful transaction due to mobile network failure are some of the drawbacks of SMS reported in Liébana-Cabanillas, Luna, & Montoro, ([LLM17]). To overcome some of these drawbacks, several measures have been implemented to guarantee a secured SMS payment transaction, such include peer to peer authentication ([Al-J16]), elliptic curve cryptography ([BS17]; [TS08]), Asymmetric Rivest-Shamir-Adleman (RSA) cipher algorithm encryption ([HFE08]; [LD08]) among others.

NFC uses certain set of standards to enable compatible smartphones to establish radio communication among themselves when they are within a distance of 10 centimeters. For mobile payment purposes, users are expected to hold or tap their NFC enabled smartphones that are closer to MNOs reader before account information can be transferred through an already established radio frequency link ([BB16]). Such was implemented for public transport services payment in Su, Wen, & Zou, (SWZ13]). The approach used a shared secret between the subscriber's mobile device and the transport system operator's server as the AES encryption/decryption key. Afterwards, the shared key was used to establish a mutual authenticated and secret communication path during the transaction.

Security, users' privacy, lack of NFC standardization and adoption of NFC phones, insufficient seeding of NFC-capable Subscribers Identity Modules (SIMs), acceptance infrastructure, low competitive pressure and antitrust regulation between MNOs are some of the factors militating against the acceptance and wide operability of NFC MPS ([Mad17]). However, certain security measures such as short lived certificates ([AUN14]), Transport Layer Security (TLS) ([DR17]), tiny TLS stack entrenched in secure elements ([Uri13]), tiny encryption ([O+17]), Elliptic Curve-based signature ([RZ13]), certificate and shared secret based authentication ([BB16]).

WAP is a communication protocol that sets a standard for how devices communicate over a mobile wireless medium. WAP applications employ the same transmission protocol (hypertext transport protocol) and web servers as web sites, the only major difference between them is seen in their application environment ([Bar02]). While web sites use Hypertext Markup Language (HTML), WAP applications make use of Wireless Markup Language (WML) or eXtensible Markup Language (XML). According to Chen & Li, ([CL16]), WAP based MPS can be achieved in two ways. The first approach entails the use of mobile browsers to submit payment information needed for a particular transaction while the second approach involves the

use of a mobile application that has been linked to users' bank account. To corroborate this, a secured WAP mobile payment application which uses bridge certificate authority was introduced in ([MY08]). Three levels of trust relationship were established: between the users and the bank, the payment gateway and bank likewise the device and MNOs. During every transaction, a dual signature is used to protect all parties involved. The user shares an order information with the MNOs, the MNOs in turn forwards this order as a purchase information to the bank. The bank responds by converting the purchase information into a payment instruction which is then forwarded to the MNOs. Private signature keys generated during these communications are used to secure the transaction process.

QR code is vast becoming one of the most conventional mobile payment tool in the mobile market and has drawn the attention of an increasing number of researchers in the world ([L+17]). Industrial Standard Organization in ISO/IEC18004:2006 defined QR code as a two-dimensional matrix barcode as shown in Figure 1. It is made up of several black squares organized in a specified format with a white background. It can be used to encrypt any digital information of interest such as music, video and text in vertical and horizontal directions ([DKA15]). The storage capacity of a QR code is influenced by the type and features of data stored by it. A QR code can store up to 7089 numeric numbers, 4296 alphanumeric numbers, 2953 bytes of 8-bits binary numbers and 1817 characters of kanji Chinese language. This huge storage capacity has made QR code preferable to barcode which can only store a maximum of 20 digits ([FL16]). Furthermore, QR codes can be read by any smartphone's camera and decrypted by a pre-installed application running on any mobile operating ([DKA15]). A report released by eMarketer revealed China to be the largest and fastest-growing mobile payment market having attained 247.9 million users in the first half of 2017 alone; this is attributed to the proliferation of smartphones in the country ([***17a]). Furthermore, Ozkaya, Ozkaya, Roxas, Bryant, & Whitson, ([O+15]) revealed that within a space of three months ending in October 2011, 20 million smartphone users in the US scanned a QR code at home, retail store, grocery stores, at work, restaurants, outside or on public transportation This showed that QR could be ubiquitously used to provide high accuracy, low-cost, high reading speed and high-reliability mobile transactions ([R+15]).

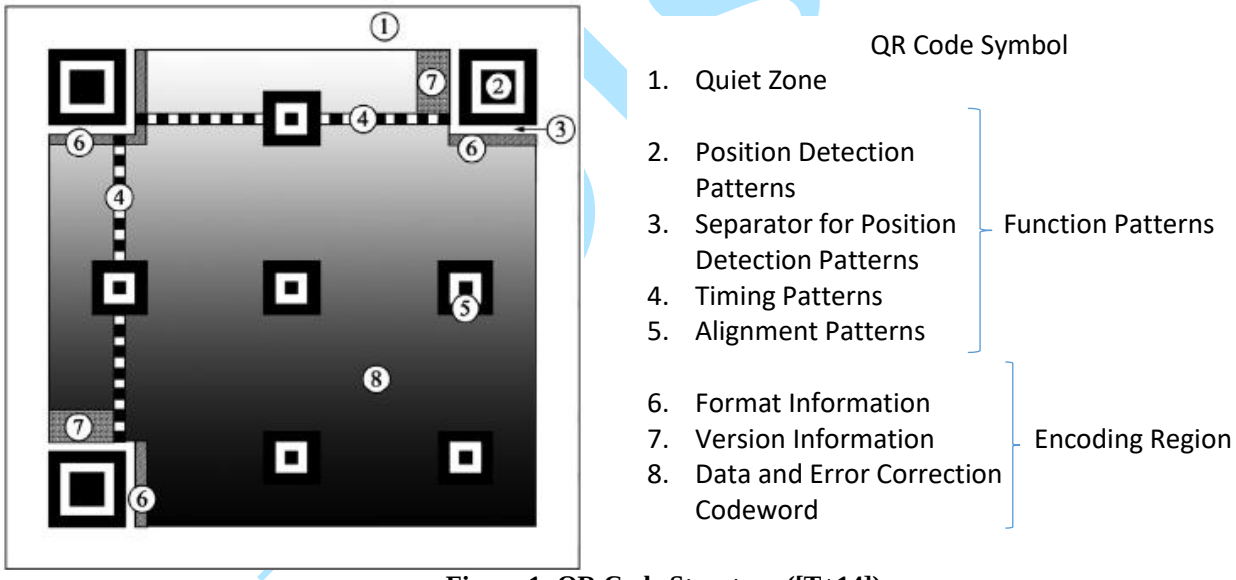

Figure 1: QR Code Structure ([T+14])

Regardless of the technology behind any MPS, security of transactions remains a paramount issue of interest. A MPS using QR code was proposed for cooperative enterprises by Suryotrisongko, Sugiharsono, & Setiawan, ([SSS12]). Using minimal infrastructure architecture, the proposed approach eliminated users' need to connect to the network. Symmetric cryptosystem was used to secure the QR code content while two factor public-private key authentication was used to secure information exchange between the user and the QR code and the web service calls. Similarly, a QR code MPS using (2, 2) Visual Cryptography (VC) scheme was implemented by Lu et al., ([L+17]). The proposed approach employs VC multiple rule to split the original QR code image into two shadows. Afterwards, the shadows were embedded into the background image. The resulting images were further fused with the carrier QR code using Reed-Solomon XOR mechanism and QR code error

correction mechanism. Anytime payment is to be made, users are expected to scan the carrier QR code and the second half will be downloaded from the cloud. Merging both shadows together produces the required payment QR code.

Similarly, QR code was integrated into an android based mobile wallet application by Ugwu & Mesigo, ([UM15]). The mobile application was majorly designed for exchanging financial value as well as encrypting transaction information between a buyer and a seller. An invoice containing details of payment to be made is generated in form of QR code and then forwarded to the mobile device of the buyer. Afterwards, buyers are expected to enter their banking information needed to authorize the payment. The feasibility of using QR code for tourist payment as a way of enhancing their satisfaction was explored in Lou, Tian, & Koh, ([LTK17]). Responses received from 247 respondents revealed that QR code payment technology could influence tourist transaction satisfaction and travel satisfaction.

MNOs Pricing Models

Several pricing models have been postulated for services provided by MNOs. These include pre-pay and post-pay pricing model ([***17d]), Smart Data Pricing (SDP) model ([S+13]), Bundling Strategy based SDP ([N+15]), Micro-billing framework ([RKT16]), Sealed-bid auction-based pricing ([MT10]), Sealed-bid reverse auction-based pricing ([LH10]), Cost-based pricing ([AYM14]), Stackelberg game-based pricing ([MLN13]), metered charging ([A+13]), Hybrid pricing model ([PGW03]), Pay-as-you-go ([And13]), Post-Paid and Pre-Paid ([PC16]). However, the most frequently used pricing model used in Nigeria are the pre-paid and post-paid pricing models. For any of these pricing models, an exchange of cash for intended services is expected.

Post-paid pricing model is an account-based model where subscribers are expected to deposit any amount into the MNOs bank account. However, with the pre-paid option, subscribers are expected to acquire the respective MNOs recharge vouchers as shown in Figure 2. After acquisition, subscribers are expected to scratch the vouchers for the recharge codes to be revealed. The revealed recharge codes are then subsequently entered into the subscribers' mobile devices. A lot of time is consumed in this process which is prone to error as the recharge code may have up to a sequence of sixteen numbers. Repeatedly entering wrong recharge codes three times may lead to the blockage of individual's mobile line. Furthermore, the scratched recharge codes must be entered in a MNOs specified format. For instance, MTN Nigeria communications expects her subscribers to use *555*recharge_code# for their payment while GLO expects a subscriber to use *123*recharge_code#. Airtel expects a subscriber to use *126*recharge_code# while EMTS expects *222*recharge_code# to be used by a subscriber. As simple as these steps seem to be, not all subscribers can accurately employ the payment method which has led to errors and subsequent forfeiture of the acquired recharge pins as the case may be.

Figure 2: Existing Recharge Vouchers

Alternatively, several proprietary websites through which subscribers can obtain recharge pins have been proposed. A novel web platform "eCard" developed for telecoms services payment was introduced by Frank, Samuel, & Emmanuel, ([FSE11]). A subscriber is expected to open an account with them in which a certain amount of cash would have been deposited for the purpose of recharging their mobile phones. After this, subscribers are expected to log into his account and supply his mobile phone number after which a chosen amount of recharge code will automatically be credited into his account. Though this method has been proved to be functional, technical know-how needed to transact on the platform and trust issues as regards cash to be initially deposited into the account remains a great concern. Besides the technical know-how required, the process is time consuming as time that would be expended in going to the bank so as to credit an account can be alternatively used to purchase a recharge voucher outside your door.

On the contrary, a multi-purpose mobile recharge code acquisition Point of Sale (POS) terminal as shown in Figure 3 can be used by recharge code acquisition. This is a small, moveable POS terminal that can permit individual to purchase recharge codes among other services for the purpose of paying their mobile telephone's services.

Figure 3: Recharge Voucher Vending POS Terminal ([*17b])**

Users of this POS are expected to purchase the POS and subsequently pay a certain amount of cash into the manufacturer's account. The cash deposited will be used to transact certain e-businesses including recharge pin vending. The POS has an inbuilt thermal printer and a slot for inserting a roll of carbonized paper for the purpose of reeling out the processed recharge codes as recharge vouchers. Besides time needed to deposit cash in the bank in order to transact business on this POS terminal, technical-know-how about the function and use of this terminal is a challenge. The cost of acquiring the POS terminal is also on a high side which has greatly reduced its acceptability among subscribers except those who intend to use it for business purposes.

Though, recharge voucher acquisition method remains the most widely accepted in the country, it is not completely safe as recharge codes can be accessed by an unauthorized middle man thereby rendering the acquired recharge code void ([MBA13]). Several instances of invalid recharge pins being acquired by subscribers have been reported and this has made the need for a more secured recharge pin acquisition a necessity. This paper presents a mobile QR based MNOs payment method is introduced in this paper.

Existing Recharge Voucher Generation Method

The present-day recharge voucher generation method in Nigeria involves the use of a standalone software. On launching the application, authorized dealers are permitted to click the "Admin Options" button to access the "Upload Inventory" form as shown in Figure 4. Clicking this button pops up a window (as shown in Figure 5) where MNOs whose recharge voucher is to be printed will be selected. Choosing the MNOs of interest will prompt the user to upload the MNOs recharge pin of choice as shown in Figure 6. A successful upload will enable the user to use the "Sell GSM Airtime" button (as in Figure 4) to print the MNOs recharge voucher displayed in Figure 7.

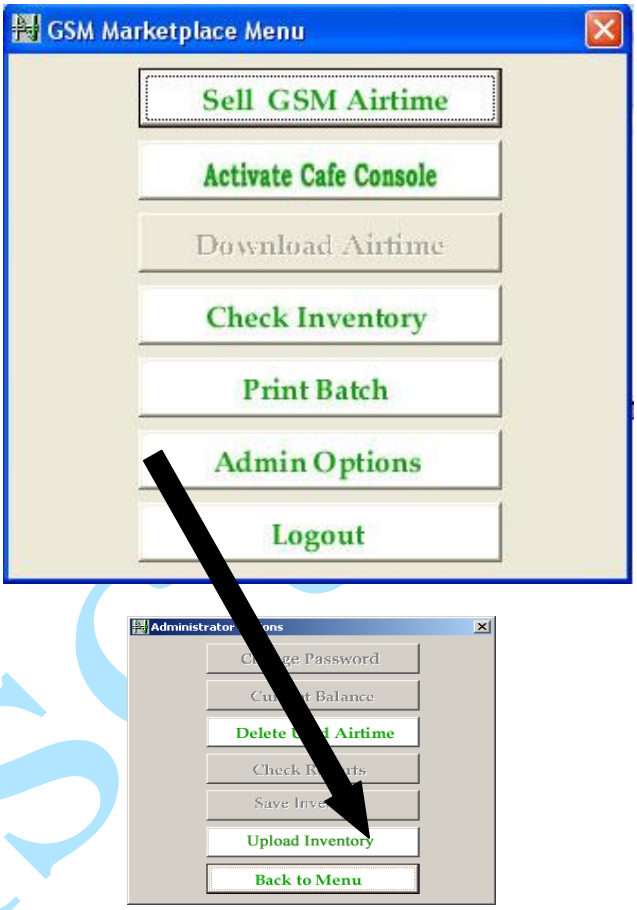

Figure 4: Existing Recharge Voucher Printing Stand-alone User Interface

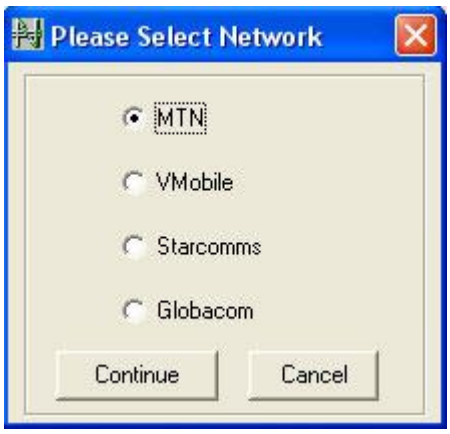

Figure 5: MNOs Menu

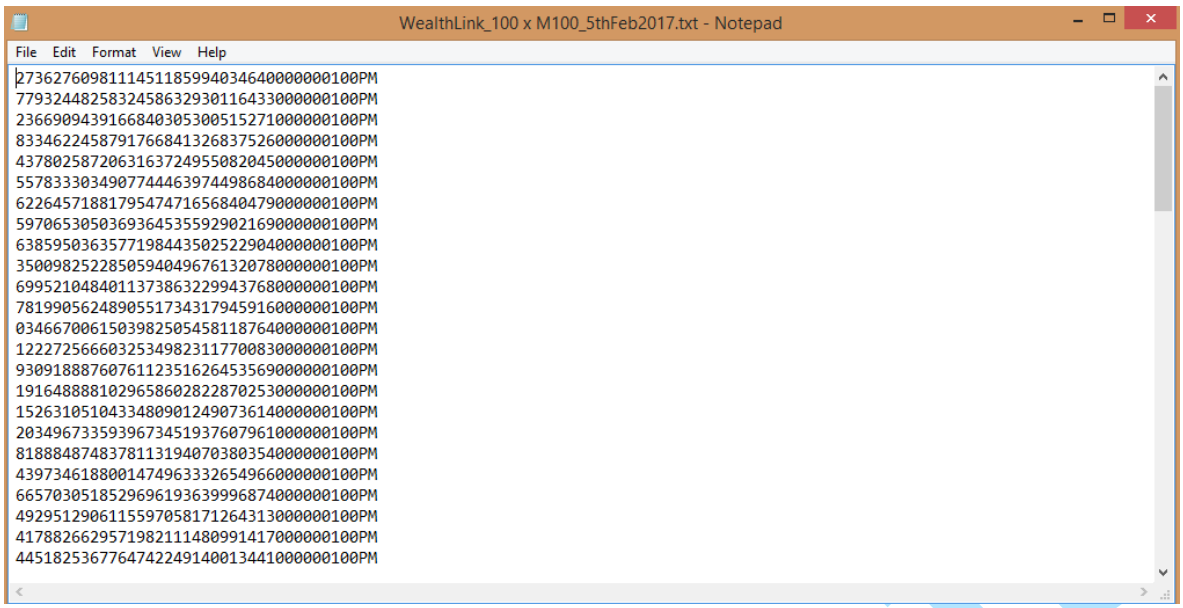

Figure 6: A Typical Recharge Code

Figure 7: A printed Recharge Voucher

3. RESEARCH METHODOLOGY

A mobile application was developed to implement the proposed QR based mobile telecoms services payment system. The entire process was divided into three phases as discussed below:

Phase I: Generating the QR Code

The QR Code generation process entails the following steps:

Step 1: Data Analysis:

Usually, QR code can be of four data types: numeric, alphanumeric, byte, and Kanji. These data types can be encoded into string of bits 1's and 0's in different ways. Hence, this stage analyzed the data to be encoded so as to determine its data type and the appropriate encoding mode to be adopted. The recharge PIN being considered here is of numeric data type hence; numeric encoding mode was adopted.

Step 2: Data Encoding:

The data encoding process includes the following:

i. Choosing the error correction level: the extracted character could be damaged or defaced during extraction attempt, therefore, QR Code uses its error correction capability to restore the extracted characters. To achieve this, the appropriate error correction level must be selected. There are four levels of error correction depending on their error correction capabilities. Error correction level L has the capability to recover 7% of damaged data while error correction level M could recover 15% of damaged data. Similarly, 25% and 30% of impaired data could be restored by error correction level H and Q respectively. With these conditions, anyone would have preferred error correction level Q, however, higher the higher the correction level, the larger the bytes to be required as well as the size of the QR code. The appropriate QR code for recharge voucher purposes shouldn't be large hence, error correction level L was adopted.

ii. Determining the appropriate data version: QR code could be in different sizes called versions. Version 1 is of 21 × 21 pixel dimension while the next version is 4 levels higher than the previous version. Furthermore, each version has different character capacities which also depend on the encoding mode. The numeric mode and version 1 adopted has 41-character capacity which is sufficient for the proposed task.

iii. Determining the mode indicator: a sequence of 0's and 1's in four-bit are used to indicate the chosen encoding mode. This precedes the encoded data. For numeric encoding mode, 0001 is the mode indicator that will be used.

iv. Determining the character count indicator: character count indicator specifies the number of characters to be encoded. For instance, if recharge PIN 1234 5678 1234 is to be encoded using version 1 QR code in numeric mode, its character count indicator as documented in QR code specification will be 10 bits. The length of the PIN to be encoded will be counted and converted into binary. In this case, the length is 14 and in binary is 1110. Since it's not up to the required 10 bits for version 1 QR code in numeric mode, 0's will be added to it to make it 10 bits yielding 0000001110. Adding the numeric encoding mode 0001 makes it 00010000001110 which is the final character count indicator.

v. Encoding the input data: the chosen encoding mode will be used to encode the input data. This entails:

a) Splitting the code into groups of three, however, if the bit is not a multiple of three then the last bit could be one or two bits. With this in mind, the recharge PIN becomes 123 456 781 234
b) Converting each group into binary: each group of codes generated above will be converted into binary such that 123 456 781 234 becomes 1111011 111001000 1100001101 11101010
c) Merge the mode indicator, character count indicator and the converted binary bits to yield the intermediary bits, i.e. mode indicator (0001), character count indicator (00010000001110) and the converted binary bits (1111011 111001000 1100001101 11101010. Therefore, the intermediary bits are: 000100010000011001111011 111001000 110000110111101010

vi. Breaking up the intermediary bits into 8-bit code words: Since, version 1 QR code in numeric mode is being used, 19 total data code words will be needed. The total number of bits needed for the QR code generation now becomes 19 * 8 i.e. 152 bits. Since, the intermediary bits is 54 length which is not up to the required 154 bits, 0000 will be added to the right side of the string. Then the intermediary bits become 000100010000001100111101111100100011000011 01111010100000. These code words are now divided into a group of 8 bits to generate the final string of data bits:

00010001 00000011 00111101 11110010 00110000 11011110 10100000

Step 3: Error Correction Coding:

Errors as a result of improper handling of the QR code may undermine the credibility of the data encoded in the QR code; therefore, when encoding the data, code words needed to correct the errors are also generated. Hence, both the encoded data and these code words will be read by the QR scanner and

compared in order to ascertain if the correct data are decoded. As specified in the QR error correction table, a version 1 QR code with error correction level L can have up to 19 data code words in a single block, and only 7 error correction code words would need to be generated.

The most popular algorithm for the error correction code words is the Reed-Solomon error correction. It uses polynomial long division as well as Galois field arithmetic in computing the error correction code words. In general terms, polynomial long division entails dividing a polynomial (message polynomial) by another polynomial (generator polynomial) but in this instance the exponents of the polynomial terms will be discarded. The Galois field arithmetic generates a restricted set of numbers (child set) using certain mathematical operations, however, the child set generated still belongs to the original set (parent set).

Generating the error correction code words entail the following steps:

i. Convert the data bits generated in the previous step to decimal such that 00010001 00000011 00111101 11110010 00110000 11011110 10100000 becomes 17, 3, 61, 242, 48, 222, 160.

ii. Use the decimal as coefficients needed to generate the message polynomial such that 17, 3, 61, 242, 48, 222, 160 becomes

$$17x^6 + 3x^5 + 61x^4 + 242x^3 + 48x^2 + 222x + 160 \quad (1)$$

iii. Compute the generator polynomial using $(x - \propto^0) \ldots (x - \propto^{n-1})$ where $\propto$=2 and n is the number of error correction code words to be generated; in this instance n=7. This yields

$$x^7 + \propto^{87} x^6 + \propto^{229} x^5 + \propto^{146} x^4 + \propto^{149} x^3 + \propto^{238} x^2 + \propto^{102} x + \propto^{21} \quad (2)$$

iv. Divide the message polynomial by the generator polynomial using Galois field arithmetic. This entails the following:

Iteration 1

a) Ensuring that the exponent of the message polynomial's first term will not become too small when computing the division by multiplying the message polynomial by x^n where n is the number of error correction code words that are needed i.e. 7. Hence, multiplying equation 1 by x^7 results to:

$$17x^{13} + 3x^{12} + 61x^{11} + 242x^{10} + 48x^9 + 222x^8 + 160x^7 \quad (3)$$

b) Ensuring that the first term in the generator polynomial is similar to that of the message polynomial. Hence, equation 2 will be multiplied by x^6 to give:

$$x^{13} + \propto^{87} x^{12} + \propto^{229} x^{11} + \propto^{146} x^{10} + \propto^{149} x^9 + \propto^{238} x^8 + \propto^{102} x^7 + \propto^{21} x^6 \quad (4)$$

c) Convert the message polynomial's first term to alpha notation using log antilog table such that 17 becomes α^{100}

d) Multiply the generator polynomial by the alpha notation α^{100}, however, if any exponent is greater than 255, modulo 255 will be performed on it; hence, the generator polynomial becomes

$$\alpha^{100}x^{13} + \propto^{187} x^{12} + \propto^{26} x^{11} + \propto^{246} x^{10} + \propto^{249} x^9 + \propto^{17} x^8 + \propto^{202} x^7 + \propto^{121} x^6 \quad (5)$$

e) Convert equation 5 to integer notation to give:

$$17x^{13} + 83x^{12} + 6x^{11} + 173x^{10} + 214x^9 + 152x^8 + 73x^7 + 118x^6 \quad (6)$$

f) XORing equation (6) with the message polynomial to have:

$$(17 \oplus 17)x^{13} + (3 \oplus 83)x^{12} + (61 \oplus 6x11+242 \oplus 173x10+48 \oplus 214x9+222 \oplus 152x8+160 \oplus 73x7+(0 \oplus 118)x6 \quad (7)$$

$$0x^{13} + 80x^{12} + 59x^{11} + 95x^{10} + 230x^9 + 70x^8 + 233x^7 + 118x^6 \quad (8)$$

Neglecting the first term yields:

$$80x^{12} + 59x^{11} + 95x^{10} + 230x^9 + 70x^8 + 233x^7 + 118x^6 \quad (9)$$

g) Repeat steps a) to f) in n-1 times, where n will be determined by the number of data code words, here n=7.

Iteration 2

a) Using the log antilog table, the coefficient of the first term in the XOR result will be converted to alpha notation, i.e. 80 now becomes $\propto^{54}$

b) The generator polynomial (equation 4) will be multiplied by the alpha notation $\propto^{54}$ performing modulo 255 on exponents above 255 to have:

$$\propto^{54} x^{12} + \propto^{141} x^{11} + \propto^{28} x^{10} + \propto^{200} x^9 + \propto^{203} x^8 + \propto^{37} x^7 + \propto^{156} x^6 + \propto^{75} x^5 \quad (10)$$

c) Convert equation (10) to integer notation to give:

$$80x^{12} + 21x^{11} + 24x^{10} + 28x^9 + 224x^8 + 74x^7 + 228x^6 + 15x^5 \quad (11)$$

d) XOR equation (11) with equation (9) to give:

$$(80 \oplus 80)x^{12} + (59 \oplus 21)x^{11} + (95 \oplus 24)x^{10} + (230 \oplus 28)x^9 + (70 \oplus 224)x^8 + (233 \oplus 74)x^7 + (118 \oplus 228)x^6 + (0 \oplus 15)x^5 \quad (12)$$

Simplifying equation (12) gives:

$$(0x^{12} + 46x^{11} + 71x^{10} + 250x^9 + 166x^8 + 163x^7 + 146x^6 + 15x^5 \quad (13)$$

Discarding the first term gives:

$$46x^{11} + 71x^{10} + 250x^9 + 166x^8 + 163x^7 + 146x^6 + 15x^5 \quad (14)$$

Iteration 3

a) Using the log antilog table, the coefficient of the first term in the XOR result will be converted to alpha notation, i.e. 46 now becomes $\propto^{130}$

b) The generator polynomial (equation 4) will be multiplied by the alpha notation $\propto^{130}$ performing modulo 255 on exponents above 255 to have:

$$\propto^{130} x^{11} + \propto^{217} x^{10} + \propto^{26} x^9 + \propto^{9} x^8 + \propto^{6} x^7 + \propto^{17} x^6 + \propto^{232} x^5 + \propto^{151} x^4 \quad (15)$$

c) Convert equation (15) to integer notation to give:

$$46x^{11} + 155x^{10} + 6x^9 + 58x^8 + 64x^7 + 152x^6 + 247x^5 + 170x^4 \quad (16)$$

e) XOR equation (16) with equation (14) to give:

$$(46 \oplus 46)x^{11} + (71 \oplus 155)x^{10} + (250 \oplus 6)x^9 + (166 \oplus 58)x^8 + (163 \oplus 64x7+ (146 \oplus 152)x^6 + (15 \oplus 247)x^5 + (0 \oplus 170)x^4 \quad (17)$$

Simplifying equation (17) gives:

$$0x^{11} + 220x^{10} + 252x^9 + 156x^8 + 227x^7 + 10x^6 + 248x^5 + 170x^4 \quad (18)$$

Discarding the first term gives:

$$220x^{10} + 252x^9 + 156x^8 + 227x^7 + 10x^6 + 248x^5 + 170x^4 \quad (19)$$

Repeating these steps till the 7th iteration gives:

$$239x^6 + 206x^5 + 57x^4 + 255x^3 + 67x^2 + 61x^1 + 251x^0 \quad (20)$$

The seven error correction code words needed are the coefficients of equation (20) i.e.

239 206 57 255 67 61 251

Step 4: Module Placement in QR code matrix

The next step is to place the generated data and error correction code words into QR code matrix alongside the function patterns as required by the QR code specification. Every version 1 QR code always has 21 pixels by 21 pixels. These pixels are made up of three finder patterns, separators, alignment patterns, timing patterns and dark module. The finder patterns are not data element of the QR code but guides QR code scanners to correctly recognize and position the data code and error correction code words for easy decoding. Regardless of the QR code versions, finder patterns are usually positioned at the top right, top left and bottom left corners of the QR code pixels. They are connected together by timing patterns. The finder patterns are encapsulated by whitespaces called separators. Alignment patterns are smaller but similar to finder patterns but are mostly found in higher QR code versions. Their locations varies depending on the QR code version been used. A single black module called the dark module is also placed on the QR code pixel. The following steps was used to generate the QR code matrix

a) Adding the finder patterns:

As documented in the QR code specification, finder patterns as shown in Figure 8 consists of a 7 by 7 pixels outer black square, 4 by 4 pixels inner white square and a 3 by 3 pixels solid black square in the center.

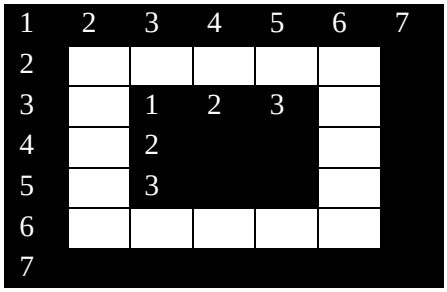

Figure 8: Finder Pattern

The finder pattern when placed on the 21 by 21 QR code pixels is as shown in Figure 9:

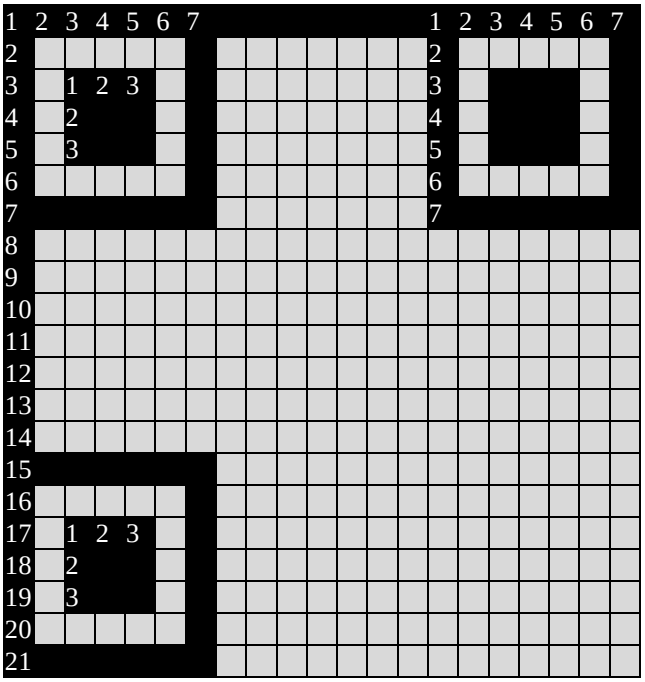

Figure 9: Finder Patterns placed on the QR Code Pixel

b) Adding the Separators: these are one pixel wide white lines that are used to separate the QR code from other elements in the pixel. They are located at the edges of the finder pattern as shown in Figure 10:

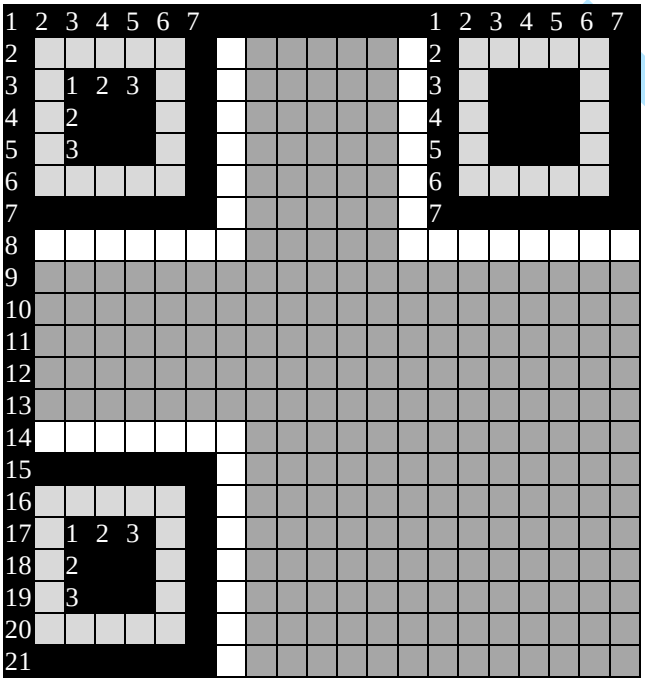

Figure 10 QR Code Pixels showing Finder Patterns and Separators

c) Adding the Timing Patterns: these are two horizontal and vertical lines with interchanging black and white pixels. The horizontal timing pattern which starts and ends with the black pixel is always positioned on the QR code's sixth row between the separators while the vertical timing pattern which also starts and ends with the black pixel is positioned on the 6th column of the QR code between the separators. Figure 11 illustrates how the timing patterns are located on the QR code pixels.

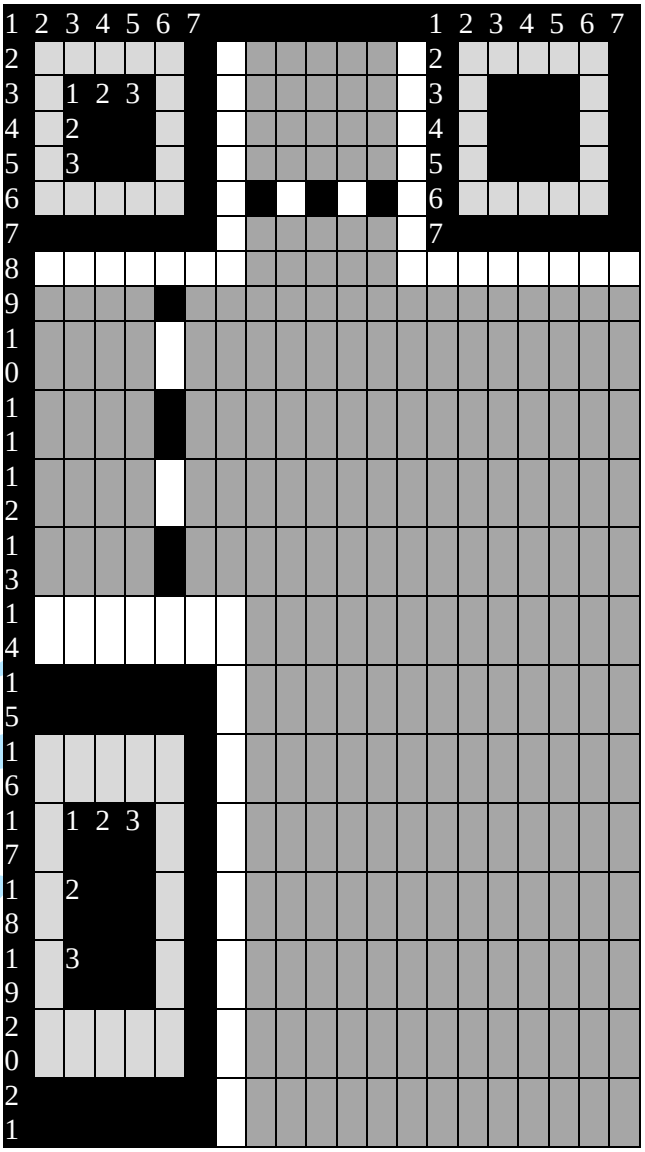

Figure 11: QR Code Pixels showing Finder Patterns, Separators and Timing Patterns

d) Adding the Dark Modules and Reserved Areas: these are used to store format and version information respectively. As documented in the QR code specification, for version 1 QR code, the dark module is placed after the separators while the pixel after the dark module of the bottom-left finder pattern and top-right finder pattern is used for as the reserved area. This is illustrated with blue and red lines in Figure 12:

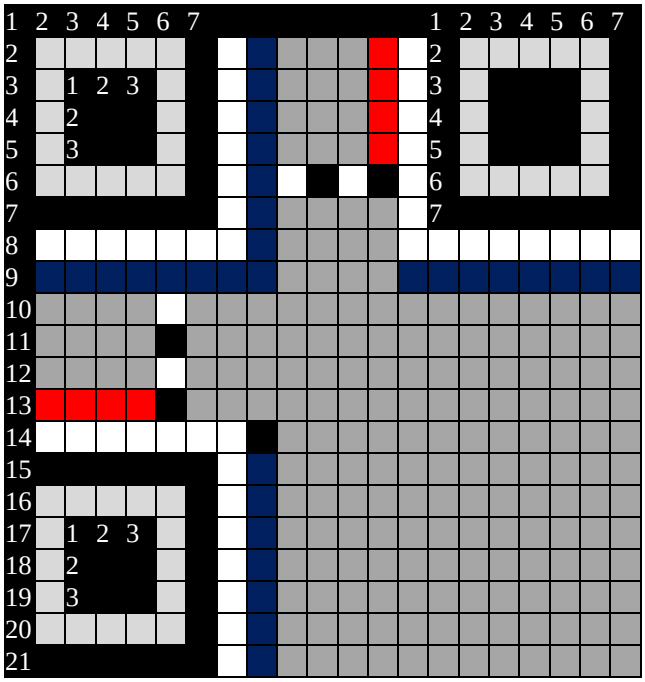

Figure 12: QR Code Pixels showing Finder Patterns, Separators, Timing Patterns, Dark Modules and Reserved Areas

e) Placing the Data Bits

This entails arranging the data bits on the QR code pixels as presented in Figure 13. The bottom-right corner of the matrix is dedicated for this. Data bits can be arranged in a zig-zag manner either upward or downward. Any time the end of a column is reached, the data are arranged on the next two columns. While arranging the data, whenever finder patterns, separators, horizontal timing pattern, dark modules and reserved areas are reached, their pixels will be exempted except vertical timing patterns.

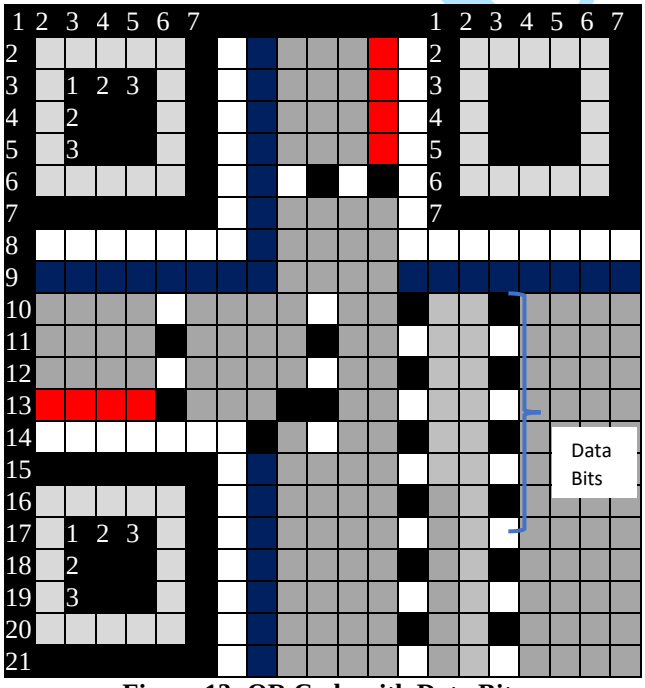

Figure 13: QR Code with Data Bits

Step 5: Adding Format Information

An insight into the error correction level used and mask pattern employed are needed in order to read the data embedded in the QR code. Bits carrying this fact will be added to the QR code using the following steps:

a) Generating the Format String
   As detailed in the QR code specification; these are five bits where the first two bits in this sequence represent the error correction level (L in this instance) and the remaining three bits represents the mask pattern to be used (pattern 3 in this instance). The resulting five bits are 00011

b) Generating the Ten Error Correction Bits for the Format String: Reed-Solomon Error Correction will be used. The steps entail using the generator polynomial in equation 21:

$$x^{10} + x^8 + x^6 + x^4 + x^2 + x^1 + 1 \qquad (21)$$

   Converting the generator polynomial to binary strings produces string 10100110111 which represents the coefficients of the generator polynomial including the missing exponents.

c) Generating the Error Correction Bits: this entails dividing the coefficients of the generator polynomial by the Format String. This produces bits 1101111

d) Combine the format string and error correction bits together; this gives 000111101111

e) XOR the result in (d) with mask string 101010000010010 to obtain the final format string 101010111111101

f) The format string is inserted into the QR code as shown in Figure placed below the topmost finder patterns and to the right of the leftmost finder patterns, as shown in Figure 14.

Should a QR code with versions ranging from 7 to 40 be used, information about this version information will also be added.

Step 6: Data Masking:

The QR code needs to be modified in a way that its content will be more secured and also easier for QR code scanner to read; the process of doing this is called data masking. This entails using a specified rule to determine the pixels that will be white (of bit 0) or black (of bit 1). There are eight mask bit patterns; pattern 3 will be generated using equation (21) as detailed in the QR code specification:

(row + column) mod 3 == 0 (22)

Besides the finder patterns and separators, for any other chosen coordinate, if the result obtained is 0, the opposite bit at that coordinate will be used.

Applying these to Figure 10 yields the QR code in Figure 15.

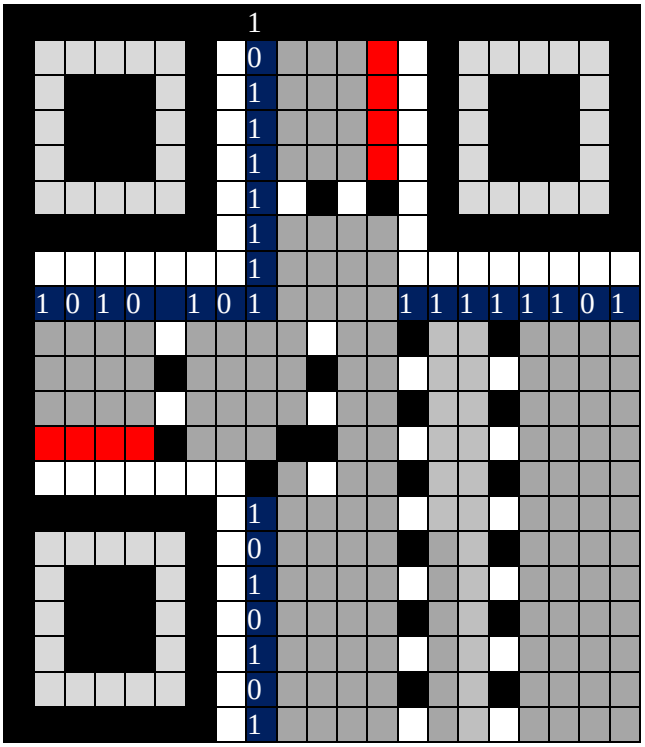

Figure 14: QR Code with Format Information

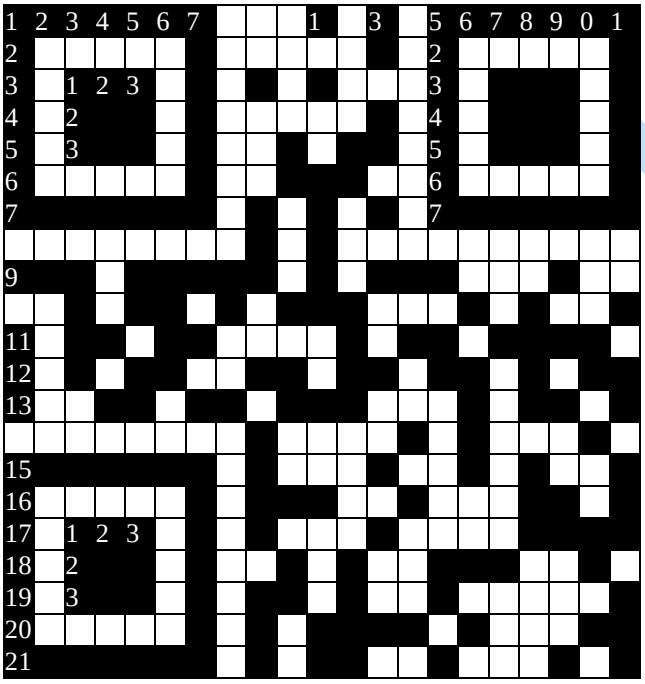

Figure 15: The Intermediary QR Code

Removing the grids produces the final QR code shown in Figure 16:

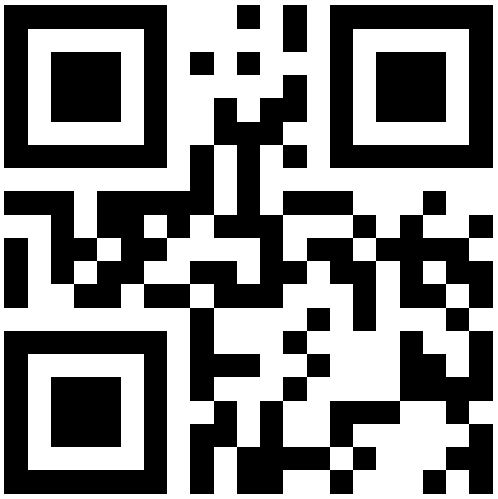

Figure 16: The Complete QR Code

Phase II: Developing a Standalone Application to Implement the QR Code

A standalone desktop application was developed to implement the QR code generation steps enumerated in Phase I. Visual Basic 2012 programming language was used for the implementation.

Phase III: Developing the QR Code Mobile Payment System

A mobile application was developed to read, decode and translate the MNOs recharge code payment information embedded in the QR code. Java software Development Kit version 6 (JDK6) containing eclipse Integrated Development Environment (IDE) and Android Development Tools (ADT) eclipse plugin were used for the mobile application development.

4. RESULTS AND DISCUSSION

QR Code Generation

The developed standalone desktop application can be used by MNOs to convert recharge codes shown in Figure 5 into QR codes. Authorized dealers are required to use the "upload button" of the interface shown in Figure 17 to upload the recharge codes into the QR code generation engine. Afterwards, the "Generate QR Code" button will be used to generate the corresponding QR code. A maximum of ten (10) QR codes can be printed on an A4 paper at once as illustrated in Figure 18. The generated QR code can be further customized as shown in Figure 19.

Reading the QR Code Recharge Voucher

As displayed in Figure 20, users are expected to employ the developed QR Code payment application to scan the obtained QR code recharge voucher. The QR code region is expected to be placed inside the

red square so as to ensure correct positioning and accurate capturing of the QR code. Afterwards, a splash screen which contains the extracted recharge codes with MNOs USSD information as shown in Figure 21 is displayed. This splash screen is optional as it can be hidden in the settings options of the mobile application. The extracted information is further forwarded to the dialer application of the mobile phone before the subscriber will be credited with the value of the services paid for.

System Testing

Prior to the system testing, unit testing of the developed mobile payment application was carried out using Roboelectric. Roboelectric is a unit testing framework that provides a Java Virtual Machine (JVM) compliant version of the Android SDK jar. This permits developers to write codes to test each units of their android application and run them on desktop JVM while still using the Android Application Program Interface (API). After a successful unit testing, a user acceptance testing (beta testing) of the mobile application was carried out using Twitter fabric's crashlytics tool. This was conducted among 48 volunteers who used the application for three months. Initial crashes were reported when lower android versions were used, when there was low memory space in volunteers' mobile devices or as a result of programming bugs. Information about these crashes were gathered and reported by the Twitter fabric's crashlytics tool. Initial crash reports as shown in Figure 22 revealed that 33 crashes were experienced among 19 volunteers; these occur between 11th and 18th of June, 2017. When these bugs were fixed, the crashlytics report obtained as shown in Figure 23 revealed that out of 125 sessions among the 48 monthly users the mobile application was 100% crash free. This showed an improvement over the initial crash report obtained.

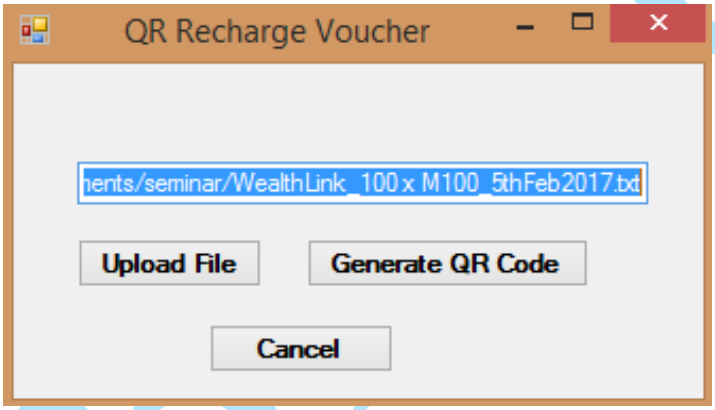

Figure 17: QR Recharge Voucher Interface

Figure 18: The Proposed QR Code Recharge Voucher

Figure 19: The Customized QR Code Recharge Voucher

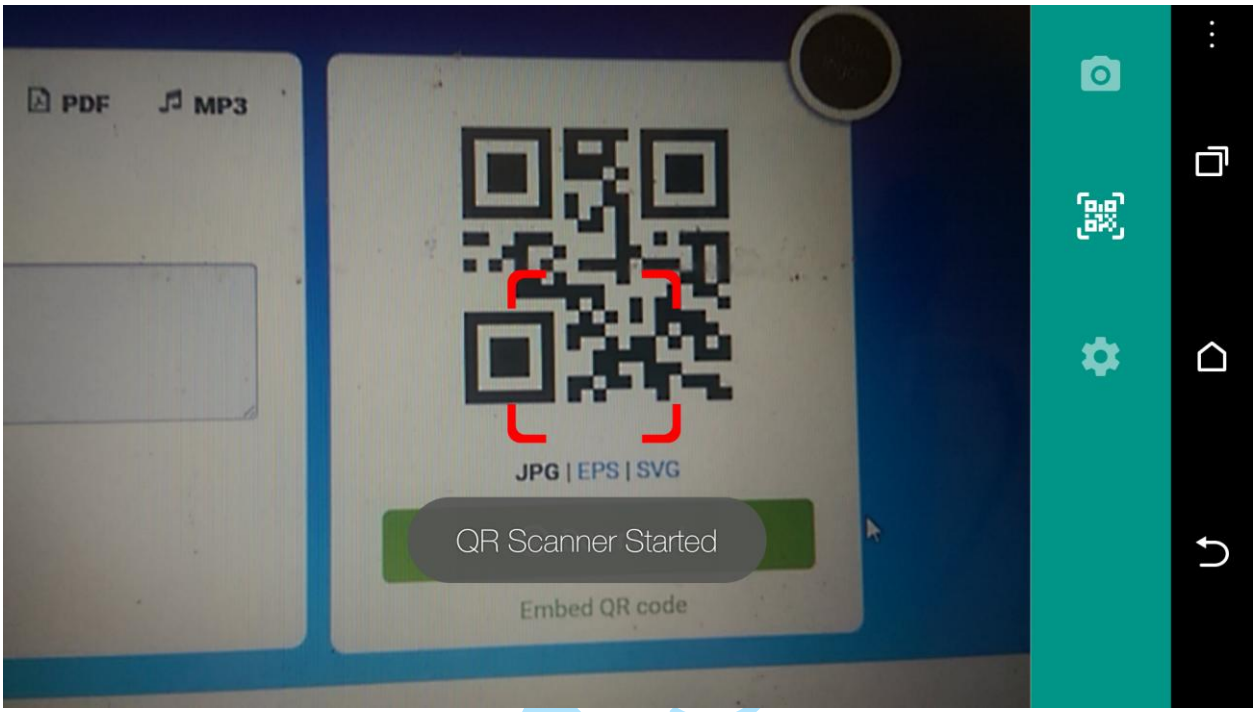

Figure 20. QR Code Recharge Scanning Process

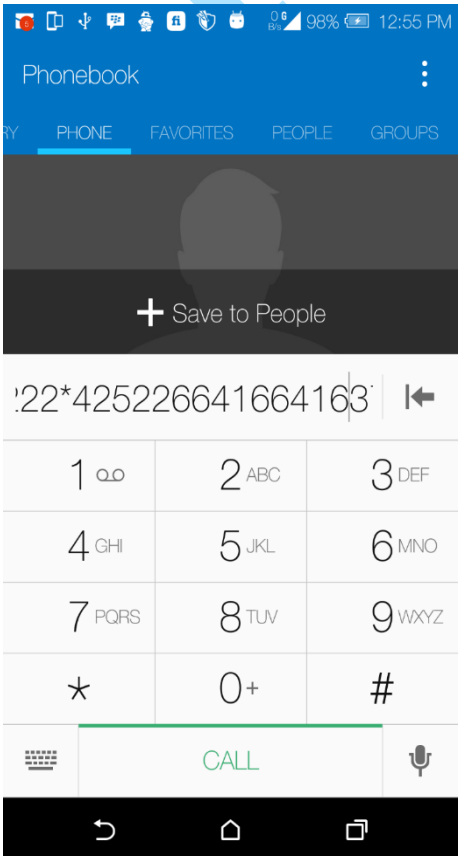

Figure 21: USSD Code being Affixed to the Extracted Recharge Code

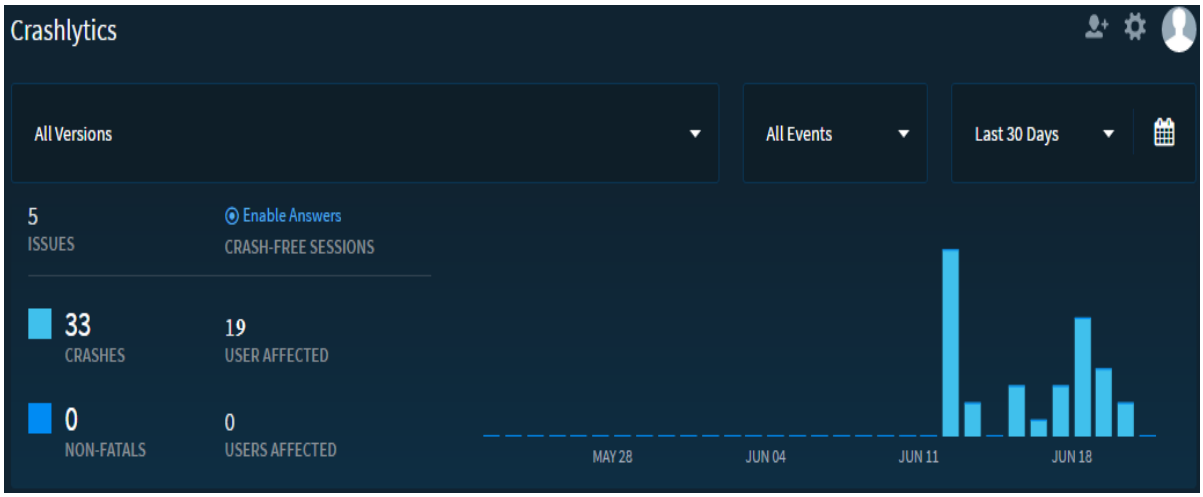

Figure 22: Initial Crash Summary

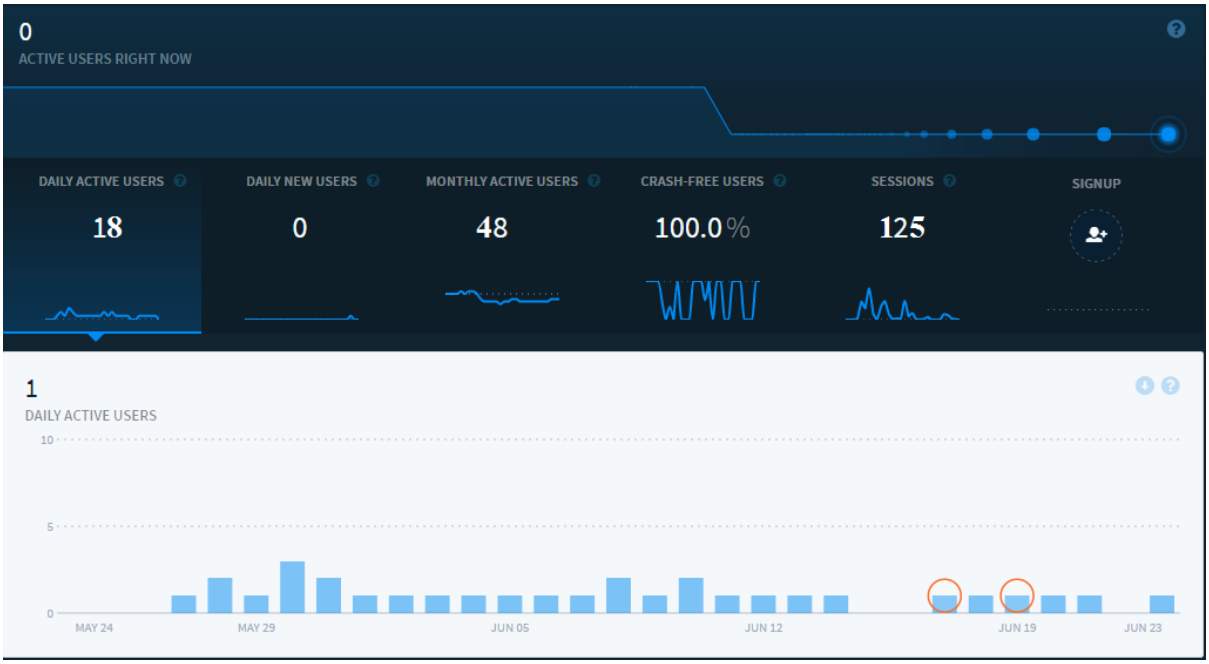

Figure 23: Final Crash Summary

CONCLUSION

This paper has introduced a novel MNOs services payment method using QR codes. It has successfully demonstrated how QR codes can be used to secure MNOs payment information with a view to prevent unauthorized access to recharge codes that has characterized the existing recharge voucher payment option. The standalone desktop application developed was used to generate the QR code while the mobile application introduced was used to read the recharge code information embedded into the QR code. The advent of smartphones with powerful features like mega pixel camera has also made the QR code scanning process easier contributing to its wide usage and acceptability. Twitter fabric's crashlytics tool was used to monitor the performance of the developed QR mobile payment application among its users. Initial reports obtained among the first 19 volunteers revealed that 33 crashes were experienced; these were as a result of program bugs which were later fixed. Subsequent reports obtained over a period of 3 months among 48 volunteers reveled that no crashes were experienced for a total of 125 sessions evaluated and the payment attempts were successful throughout these sessions. This has shown that QR code can find practical applications in MNOs services payment.

REFERENCES

[Al-J16] **Al-juaifari M. K. R.** - *Secure SMS Mobile Transaction with Peer to Peer Authentication Design for Mobile Government*. American Journal of Engineering Research (AJER), 4(11), 143–149, 2016.

[And13] **Andra R. S.** - *Investigating Pricing and Negotiation Models for Cloud Computing*. M.Sc. Thesis, University of Edinburgh, 2013.

[AMA16] **Abrahão R. de S., Moriguchi S. N., Andrade D. F.** - *Intention of adoption of mobile payment: An analysis in the light of the Unified Theory of Acceptance and Use of Technology (UTAUT)*. RAI Revista de Administração E Inovação, 13(3), 221–230. 2016. https://doi.org/10.1016/j.rai.2016.06.003

[AUN14] **Ahamad S. S., Udgata S. K., Nair M.** - *A Secure Lightweight and Scalable Mobile Payment Framework* (pp. 545–553). 2014, Springer, Cham. https://doi.org/10.1007/978-3-319-02931-3_62

[AYM14] **Adeel U., Yang S., McCann, J. A.** - *Self-Optimizing Citizen-centric Mobile Urban Sensing Systems*. Proceedings of the 11th International Conference on Autonomic Computing (pp. 161–167). 2014. Retrieved from http://blogs.usenix.org/conference/icac14/technical-sessions/presentation/adeel

[A+13] **Al-Roomi M., Al-Ebrahim S., Buqrais S., Ahmad I.** - *Cloud Computing Pricing Models: A Survey*. International Journal of Grid and Distributed Computing, 6(5), 93–106. https://doi.org/10.14257/ijgdc.2013.6.5.09, 2013.

[Bar02] **Barnes S. J.** - *Provision of Services Via the Wireless Application Protocol: A Strategic Perspective*. Electronic Markets, 12(1), 14–21. https://doi.org/10.1080/10196780275343 3227, 2002.

[BB16] **Badra M., Badra R. B.** - *A Lightweight Security Protocol for NFC-based Mobile Payments*. Procedia Computer Science, 83(Ant), 705–711. https://doi.org/10.1016/j.procs.2016.04.156, 2016.

[BS17] **Bojjagani S., Sastry V. N.** - *A secure end-to-end SMS-based mobile banking protocol*. International Journal of Communication Systems, (January), 1–19. https://doi.org/10.1002/dac.3302, 2017.

[CL16] **Chen X., Li S.** - *Understanding Continuance Intention of Mobile Payment Services: An Empirical Study*. Journal of Computer Information Systems, 0(0), 1–12. https://doi.org/10.1080/08874417.2016.1180649, 2016.

[DR17] **Dierks T., Rescorla E.** - *The Transport Layer Security (TLS) Protocol Version 1.2*. Retrieved October 27, 2017, from https://www.bibsonomy.org/person/198ca7937ba442fa30e172eed395c3a55/author/0

[DGO15] **Dahlberg T., Guo J., Ondrus J.** - *A critical review of mobile payment research*. Electronic Commerce Research and Applications, 14(5), 265–284, 2015. https://doi.org/10.1016/j.elerap.2015.07.006

[DKA15] **Demir S., Kaynak R., Alpaslan K.** - *Usage level and future intent of use of quick response (QR) codes for mobile marketing among college students in Turkey*. Procedia - Social and Behavioral Sciences, 181, 405–413, 2015. https://doi.org/10.1016/j.sbspro.2015.04.903

[D+08] **Dahlberg T., Mallat N., Ondrus J., Zmijewska A.** - *Past, present and future of mobile payments research: A literature review*. Electronic Commerce Research and Applications, 7(2), 165–181. 2008. https://doi.org/10.1016/j.elerap.2007.02.001

[FL05] **Fong S., Lai E.** - *Mobile Mini-payment Scheme Using SMS-Credit*. Computational Science and Its Applications – ICCSA 2005. ICCSA 2005. Lecture Notes in Computer Science, 3481, 1106–1114.

[FL16] **Fei J., Liu R.** - *Drug-laden 3D biodegradable label using QR code for anti-counterfeiting of drugs*. Materials Science & Engineering C, 63, 657–662. https://doi.org/10.1016/j.msec.2016.03.004

[FBR13] **Fun T. S., Beng L. Y., Razali M. N.** - *Review of Mobile Macro-Payments Schemes*. Journal of Advances in

Computer Networks, 1.(4). https://doi.org/10.7763/JACN.2013.V1.65, 2013.

[FSE11] **Frank I., Samuel J., Emmanuel A.** - *Online Mobile Phone Recharge System in Nigeria*. European Journal of Scientific Research, 60(2), 295–304, 2011.

[HFE08] **Harb H., Farahat H., Ezz M.** - *SecureSMSPay: Secure SMS mobile payment model*. 2nd International Conference on Anti-Counterfeiting, Security and Identification, ASID 2008, 11–17. https://doi.org/10.1109/IWASID.2008.4688346, 2008.

[KZ07] **Kadhiwal S., Zulfiquar M.** - *Analysis of mobile payment security measures and different standards*. Computer Fraud and Security, 2007(6), 12–16. https://doi.org/10.1016/S1361-3723(07)70077-5, 2007.

[KDZ16] **de Kerviler G., Demoulin N. T. M., Zidda P.** - *Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?* Journal of Retailing and Consumer Services, 31, 334–344. 2016. https://doi.org/10.1016/j.jretconser.2016.04.011

[KML13] **Kim C., Mirusmonov M., Lee I.** - *An empirical examination of factors influencing the intention to use mobile payment*. Computers in Human Behavior, 26(3), 310–322. https://doi.org/10.1016/j.chb.2009.10.013, 2013.

[KSL03] **Kungpisdan S., Srinivasan B., Le P. D.** - *Lightweight Mobile Credit-Card Payment Protocol*. In International Conference on Cryptology in India INDOCRYPT 2003 (pp. 295–308). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24582-7_22, 2003.

[Lug12] **Lugo K.** - Enhancing public-private partnerships through SMS Vouchers, 10, 666–671. https://doi.org/10.1016/j.procs.2012.06.085, 2012.

[LD08] **Lisoněk D., Drahanský M.** - *SMS Encryption for mobile communication*. Proceedings - 2008 International Conference on Security Technology, SecTech 2008, 198–201. https://doi.org/10.1109/SecTech.2008.48.

[LH10] **Lee J.-S., Hoh B.** - *Sell your experiences: a market mechanism based incentive for participatory sensing*. In IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 60–68). https://doi.org/10.1109/PERCOM.2010.5466993, 2010.

[LLM17] **Liébana-Cabanillas F., de Luna I. R., Montoro F.** - *Intention to use new mobile payment systems : a comparative analysis of SMS and NFC payments*. Economic Research-Ekonomska Istraživanja, 30(1), 724–742. https://doi.org/10.1080/1331677X.2017.1305784, 2017.

[LTK17] **Lou L., Tian Z., Koh J.** - *Tourist Satisfaction Enhancement Using Mobile QR Code Payment : An Empirical Investigation*, 9(1186), 1–14. https://doi.org/10.3390/su9071186, 2017.

[L+11] **Lu Y., Yang S., Chau P. Y. K., Cao Y.** - *Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective*. Information and Management, 48(8), 393–403. https://doi.org/10.1016/j.im.2011.09.006, 2011.

[L+17] **Lu J., Yang Z., Yuan W., Li L., Chang C. C., Li L.** - *Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography*. Mobile Information Systems, 2017, 1–13. https://doi.org/10.1155/2017/4356038, 2017.

[Mad17] **Madureira A.** - *Factors that hinder the success of SIM-based mobile NFC service deployments*. Telematics and Informatics, 34(1), 133–150. https://doi.org/10.1016/j.tele.2016.05.003, 2017.

[Mag14] **Magnier-Watanabe R.** - *An institutional perspective of mobile payment adoption: The case of Japan*. Proceedings of the Annual Hawaii International Conference on System Sciences, 1043–1052. https://doi.org/10.1109/HICSS.2014.136, 2014.

[Mal07] **Mallat N.** - *Exploring consumer adoption of mobile payments - A qualitative study*. Journal of Strategic Information Systems, 16(4), 413–432. https://doi.org/10.1016/j.jsis.2007.08.001, 2007.

[MT08] **Meng J. M. J., Ye L. Y. L.** - *Secure Mobile Payment Model Based on WAP*. 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, 1–4. https://doi.org/10.1109/WiCom.2008.2121, 2008.

[MY10] **Mihailescu M., Teo Y. M.** - *Dynamic resource pricing on federated clouds*. CCGrid 2010 - 10th IEEE/ACM International Conference on Cluster, Cloud, and Grid Computing, 513–517. https://doi.org/10.1109/CCGRID.2010.123, 2010.

[MBA13] **Mohammad N., Barua A., Arafat M. A.** - *A smart prepaid energy metering system to control electricity theft*. In Proceedings of 2013 International Conference on Power, Energy and Control, ICPEC 2013 (pp. 562–565). https://doi.org/10.1109/ICPEC.2013.6527721, 2013.

[MLN13] **Mei L., Li W., Nie K.** - *Pricing Decision Analysis for Information Services of the Internet of Things Based on Stackelberg Game*. In Proceedings of 2nd International Conference on Logistics, Informatics and Service Science (pp. 1097–1104). https://doi.org/10.1007/978-3-642-32054-5, 2013.

[N+15] **Niyato D., Hoang D. T., Luong N. C., Wang P., Kim D. I., Han Z.** - *Smart Data Pricing Models for Internet-of-Things (IoT): A Bundling Strategy Approach*. IEEE Network Magazine, 1–16. Retrieved from http://arxiv.org/abs/1512.05075, 2015.

[OPL14] **Oh J., Park C.-U., Lee S.** - *NFC-based Mobile Payment Service Adoption and Diffusion*. Journal of Convergence, 5(2), 8–14, 2014.

[O+15] **Ozkaya E., Ozkaya H. E., Roxas J., Bryant F., Whitson D.** - *Factors affecting consumer usage of QR codes*. Journal of Direct, Data and Digital Marketing Practice, 16(3), 209–224. https://doi.org/10.1057/dddmp.2015.18, 2015.

[O+16] **Oliveira T., Thomas M., Baptista G., Campos F.** - *Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology*. Computers in Human Behavior, 61(2016), 404–414. https://doi.org/10.1016/j.chb.2016.03.030, 2016.

[O+17] **Olaniyi O. M., Arulogun O. T., Omotosho A., Onuh V. O.** - *Securing clinic tele-diagnostic system using enhanced tiny encrypted radio frequency identification and image steganographic technique*. International Journal of Telemedicine and Clinical Practices, 2(3), 242. https://doi.org/10.1504/IJTMCP.2017.087878, 2017.

[PC16] **Pukkasenung P., Chokngamwong R.** - Review and Comparison of Mobile Payment Protocol. Advances in Parallel and Distributed Computing and Ubiquitous Services, 368. https://doi.org/10.1007/978-981-10-0068-3, 2016.

[PGW03] **Piro R. M., Guarise A., Werbrouck A.** - *An economy-based accounting infrastructure for the datagrid*. In Proceedings - IEEE/ACM International Workshop on Grid Computing (Vol. 2003–Janua, pp. 202–204). https://doi.org/10.1109/GRID.2003.1261716, 2003.

[RZ13] **Rosati T., Zaverucha G.** - *Elliptic curve certificates and signatures for NFC signature records*. Research In Motion Certicom Research, Rosati, T., 1–17. Retrieved from http://members.nfc-forum.org/resources/white_papers/Using

_ECQV_ECPVS_on_NFC_Tags.pdf, 2013.

[RKT16] **Robert J., Kubler S., Traon Y. Le** - *Micro-billing framework for IoT: Research & technological foundations*. In Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016 (pp. 301–308). https://doi.org/10.1109/FiCloud.2016.50, 2016.

[R+12] **Rai N., Ashok A., Chakraborty J., Arolker P., Gajera S.** - *M-Wallet : An SMS based payment system*. International Journal of Engineering Research and Applications, special is(48), 258–263, 2012.

[R+15] **Rongsheng X., Chaoqun H., Shunzhi Z., Dapeng T.** - *Anti-counterfeiting Digital Watermarking Algorithm for Printed QR Barcode*. Neurocomputing, 167(15), 625–635. https://doi.org/10.1016/j.neucom.2015.04.026, 2015.

[Soh17] **Sohn S.** - *A contextual perspective on consumers' perceived usefulness: The case of mobile online shopping*. Journal of Retailing and Consumer Services, 38(January), 22–33. https://doi.org/10.1016/j.jretconser.2017.05.002, 2017.

[SSS12] **Suryotrisongko H., Sugiharsono, Setiawan B.** - *A Novel Mobile Payment Scheme based on Secure Quick Response Payment with Minimal Infrastructure for Cooperative Enterprise in Developing Countries*. Procedia - Social and Behavioral Sciences, 65(ICIBSoS), 906–912. https://doi.org/10.1016/j.sbspro.2012.11.218, 2012.

[SWZ13] **Su H., Wen X., Zou D.** - *A Secure Credit Recharge Scheme for Mobile Payment System in Public Transport*. IERI Procedia, 4, 303–308. https://doi.org/10.1016/j.ieri.2013.11.043, 2013.

[S+13] **Sen S., Joe-Wong C., Ha S., Chiang M.** - *Smart Data Pricing (SDP): Economic Solutions to Network Congestion*. Recent Advances in Networking, 221–274. Retrieved from http://www.cl.cam.ac.uk/teaching/1314/R02/sigcomm/sigcomm-ebook-2013paper3.pdf, 2013.

[TS08] **Toorani M., Shirazi A. A. B.** - *SSMS - A secure SMS messaging protocol for the m-payment systems*. Proceedings - IEEE Symposium on Computers and Communications, 700–705. https://doi.org/10.1109/ISCC.2008.4625610, 2008.

[T+14] **Tarjan L., Šenk I., Tegeltija S., Stankovski S., Ostojic G.** - *A readability analysis for QR code application in a traceability system*. Computers and Electronics in Agriculture, 109, 1–11. https://doi.org/10.1016/j.compag.2014.08.015, 2014.

[T+16] **Ting H., Yacob Y., Liew L., Lau W. M.** - *Intention to Use Mobile Payment System: A Case of Developing Market by Ethnicity*. Procedia - Social and Behavioral Sciences, 224(August 2015), 368–375. https://doi.org/10.1016/j.sbspro.2016.05.390, 2016.

[Uri13] **Urien P.** - *LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things*. 2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013, 845–846. https://doi.org/10.1109/CCNC.2013.6488560, 2013.

[UM15] **Ugwu C., Mesigo T.** - *A Novel Mobile Wallet Based on Android OS and Quick Response Code Technology*. International Journal of Advanced Research in Computer Science & Technology, 3(1), 85–89, 2015.

[XPP15] **Xu C., Peak D., Prybutok V.** - *A customer value, satisfaction, and loyalty perspective of mobile application recommendations*. Decision Support Systems, 79, 171–183. https://doi.org/10.1016/j.dss.2015.08.008, 2015.

[YKL18] **Yu X., Kywe S. M., Li Y.** - *Security*

Issues of In-Store Mobile Payment. Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2 (1st ed., Vol. 2). Elsevier Inc. https://doi.org/10.1016/B978-0-12-812282-2.00006-1, 2018.

[Y+15] **Yang Q., Pang C., Liu L., Yen D. C., Michael Tarn J.** - *Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation*. Computers in Human Behavior, 50, 9–24. https://doi.org/10.1016/j.chb.2015.03.058, 2015.

[***17a] *** - *China Boasts World's Largest Proximity Mobile Payments Market*. Retrieved October 27, 2017, from https://www.emarketer.com/Article/China-Boasts-Worlds-Largest-Proximity-Mobile-Payments-Market/1014053.

[***17b] *** - *Recharge Card Vending POS Terminal*. Retrieved October 27, 2017, from http://www.citi-serve.com/orange-box.html.

[***17c] *** - *Mobile Telecommunication Industry Statistics*. Retrieved October 27, 2017, from http://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5.

[***17d] *** - *Ofcom: Pricing trends for communications services in the UK*, 2017.