



SECURED QR-CODE BASED COD PAYMENT THROUGH MOBILE BILL PRESENTMENT SYSTEM REPLACING THE POS MACHINE WITH AN ELECTRONIC DEVICE

Hareesh Kumar¹, Ravi Shankar², Ajaya Kumar K R³

^{1,2}Electronics & Computer Science, ³Computer Science, Tumkur University, (India)

ABSTRACT

In Online shopping cart COD(Cash on Delivery) and POS(Point Of Sale) is the most widely accepted method of payment worldwide. There are plenty of limitations in these methods which includes mainly the risk behind handling hard cash where chances of getting fake notes are at the high point, the service charges which has to be paid by the merchant during every transactions in a POS machine is considered as a loss in the merchant's perspective and getting the network connectivity in every location of the POS machine is also very challenging task. Here a new technology known as Secured QR Code based COD payment through MBPS (Mobile Bill Presentment System) is getting introduced which overcomes all these above said limitations and also provides additional features which is helpful for the merchant as well as the customers by scanning the Secured Quick Response (QR) Code of the bill through a Smartphone.

Keywords: POS, COD, QR Code, MBPS, AES

I. INTRODUCTION

Secured QR Code based COD payment through Mobile Bill presentment System is a Mobile Application which enables the user to pay bill by scanning the Secured QR code present in the Bill. The mobile acts as an intermediate which scans the Secured QR code and takes the user to the payment gateway and enables the user to pay the bill without much difficulty.

It is a unique and new product present in the current market scenario. The bill has a unique Secured QR code encrypted with Rijndael Algorithm (Advanced Encryption Standard) present in it, which could be only read after decrypting using the Mobile application and navigate to a secure mode of bill payment.

This is an electronic version of the traditional bill payment system which would help our customers to make the payment of their bills by scanning the Secured Quick Response (QR) Code of the bill through a Smartphone

1.1 Existing Technology on cod

- 1.1.1 COD: This is one of the most common and simple methodology which is existing among the customer for making their payment in the current online shopping market scenario. Once the customer places their order, the merchant provides the facility of home delivery to the customer to avail their ordered product.

The customer has to pay the amount of their product only at the time of delivery of the product. The main feature of cash on delivery which attracts the customer to make their payment using this method is that the customer need not worry about their ordered product and also need not track the destination of the product since he is not losing his penny even if the product does not reach him on time. Again once the product reaches the customer, this method plays a very simple role as he can pay the required amount to the merchant and very easily avail the product with no other further complications. Due to all these features COD still remains to be the most widely used method to make payments for online shopping applications worldwide.

1.1.2 POS: Most of the shopping cart is widely using POS machine or collecting hard cash for their COD facility. POS or EPOS is the place where a retail transaction is completed. It is the point at which a customer makes a payment to the merchant in exchange for goods or services. At the point of sale the retailer would calculate the amount owed by the customer and provide options for the customer to make payment. The merchant will also normally issue a receipt for the transaction.

The POS in various retail industries uses customized hardware and software as per their requirements. Retailers may utilize weighing scales, scanners, electronic and manual cash registers, EFTPOS terminals, touch screens and any other wide variety of hardware and software available for use with POS. For example, a grocery or candy store uses a scale at the point of sale, while bars and restaurants use software to customize the item or service sold when a customer has a special meal or drink request.

The modern point of sale is often referred to as the point of service because it is not just a point of sale but also a point of return or customer order. Additionally it includes advanced features to cater to different functionality, such as inventory management, CRM, financials, warehousing, etc., all built into the POS software. Prior to the modern POS, all of these functions were done independently and required the manual re-keying of information, which can lead to entry errors.

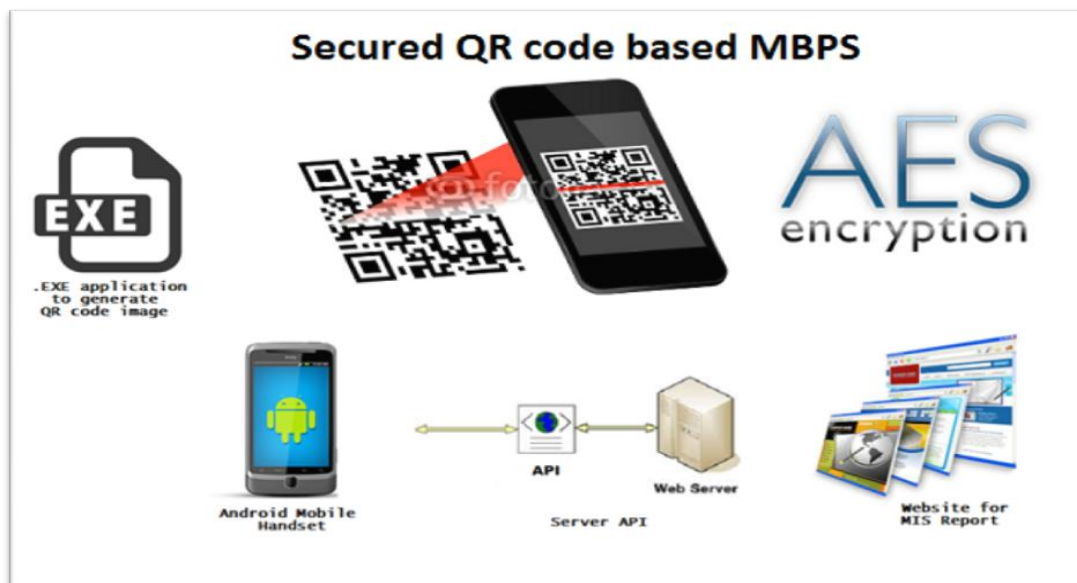
1.2. Limitation of existing technology

1.2.1 COD: There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all. This method may appear to be very simple and accessible for the customers to make their payments, but there exists a lot of risk in cash handling. The main problem which is faced in cash handling is the high risk of getting fake notes which is not easily caught by the sales executives at the time of delivery. Providing amount by tendering the exact change is again a difficult task faced by the customer as well as the sales executive at the time of delivery which can make loss at the customer's as well as the merchants side. Carrying cash in hand is always risky and this may lead many fraudulent activity as well as misplacing, accounting etc. major issues may occur.

1.2.2 POS: Many people have remained with their cash registers not because of their benefits over POS, but because of they want to avoid the cost of purchasing all brand new POS systems. Replacing old technology can be pricy, especially if the business has multiple retail locations. Small business owners in particular tend to avoid upgrading to a new cash register system because of this.

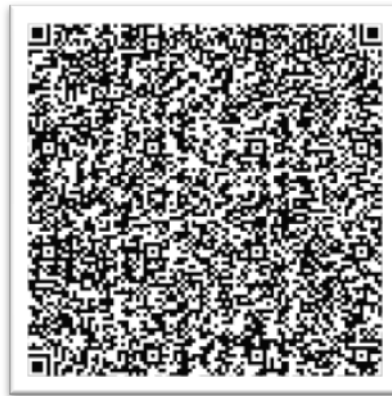
II. METHODOLOGY

To overcome the above mentioned limitations of the existing payment system we have introduced an innovative application which makes a hassle free payment and is known as Secured QR Code based COD payment through Mobile Bill Presentment system (MBPS). This application contains five modules: 1. An EXE application which has to be integrated on the merchant software to generate Secured QR bills. 2. Encrypting QR Code image to increase the security using Rijndael Algorithm 3. An android Mobile application to read this Secured QR code image and make payment through payment gateway. 4. Server Application Programming Interface (API). 5. A website for merchants to generate various MIS Reports.



2.1 .EXE Application: Firstly an EXE application has to be created using certain mandatory parameters which has to be displayed as the bill details to the customer. For e.g. Customer id, Bill number, bill date, bill amount, description etc. The Secured QR code image differs according to the values passed to the parameters. While creating the Secured QR code image we have to consider certain security mandates to secure the bill. Using an appropriate key, the information will be made available after applying the encryption. The bill data in the QR Code image is secured through Rijndael Algorithm. To ensure reliability of the client bill data, it is further encrypted in the URL of the application. The entire URL data is further provided encryption to 64 bit data. This secures the QR image from getting read and decrypted from a third party application. Finally this application has to be integrated on the merchant's software to generate secured QR code image on Bills.

2.1.1 Securing QR code image using Rijndael Algorithm: The Advanced Encryption Standard (AES), also known as the Rijndael algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys of 128, 192 or 256 bits.

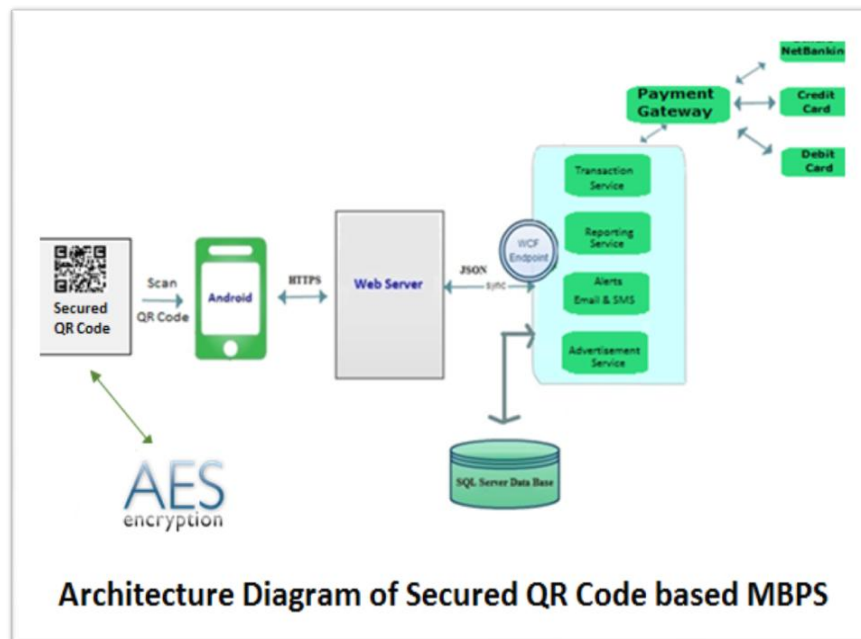


Secured QR Code image encrypted with Rijndael Algorithm

- 2.1.2** Here we pass the index while encrypting JSON string. We have created encryption class with index of dynamic value to strengthen the image. Here image will be created with encrypted values and a random number will be generated on each and every request. This random number with summation with our own static value will result on getting a number and at this number position we will be placing our public key. While decrypting the string, we will be searching for the key position to decrypt the string. This will add more security because to find the position of key is not an easy task for outsiders as encrypted string looks like a combination of letters which a junk value is thus making it very tough to decrypt.
- 2.1.3 Android mobile application:** An android mobile application is being created to read the Secured QR code images from bill using standard QR Library which will be available in android. Since the QR image is secured by encryption methods on bill as mentioned above, it has to be decrypted using the appropriate key. After extracting the required information from bill the same will be displayed on the handset and be made available for the customer to make the payment. For making the secured payment using credit/debit card or net banking a payment gateway is already integrated in this mobile application with the help of which customers will be able to make their bill payments using the mentioned mode of payment.
- 2.1.4 Server API:** This application acts as an interface between the mobile application and the database. All authentication mechanism will be happening at the server level. Mobile application will send a request to the server and which further performs the action and send back the response to the mobile. Mobile application will display the result based on the response given by the server. It is basically a handshake between the mobile handset and server using JSON Method which is more compact, secured and light weight. Certain information will be made available in database for further requirements. The Application Server (App server) forms the Service layer architecture, where Windows Communication Foundation (WCF) service is deployed. Windows Communication Foundation (WCF) is a framework for building service-oriented applications where in data is sent as asynchronous message from one service endpoint to another. The WCF listener accepts the request from Client layer through End Point service. The design features of WCF - Service Orientation, Interoperability, Service Metadata, Security, Encodings and multiple transport, reliable queued durable messages offer manageable approach to create Web service and web service clients. Request initiating from smartphone -> Server receives the

request and process -> server is using database to store the details -> after processing the details, server will give response to smartphone -> smartphone reads the response and display appropriate message.

- 3 **Website for merchant to generate MIS Reports:** Website will be made available for the merchant's administrators to generate various MIS reports such as successful/unsuccessful bill paid reports, date wise reports, item wise reports etc. We can generate the reports even based on the bill id. These information will be fetched from database and generate respective reports after successful authentication to the server.



SERVICE: TRANSACTION

INPUT

```
{
    "BillName": "MERCHANT NAME",
    "CustomerID": "212XXX29",
    "MobileNumber": "97XXXXXX401",
    "BillNumber": "4511XXXXXXX25",
    "BillPeriod": "01.04.2015 to 30.04.2015",
    "TotalAmount": "8500.00",
    "Channel": "G"
}
```

OUTPUT

Success:

```
{
    "ResponseCode": "000",
    "PaymentID": "P112XXXXXXXX00007"
}
```

Payment Failed



```
{  
    "ResponseCode ": "999"  
}  
Duplicate Payment  
{  
    "ResponseCode ": "997"  
}  
Error in Request  
{  
    "ResponseCode ": "998"  
}
```

The description of each key value pair is detailed below –

Input parameters -

- The operation requested is Transaction to mobile application.
- BillerName - Name of the Merchant.
- CustomerID - ID of the Customer registered with Merchant.
- MobileNumber - Mobile number of the Customer registered with Merchant.
- BillNumber –ID of Customer's bill.
- BillPeriod – Billing Period of the Customer.
- TotalAmount –Total Amount of Customer's bill
- Channel –Payment Channel selected by the Customer to pay the bill

All data representation is an encrypted Hash value of the Payment Channel selected by the Customer for making payment.

Output parameters –

For success case -

- Response code: 000 – Response code value to indicate that operation performed is success.
- PaymentID – Payment ID of the Transaction

For failure case of transaction –

- Response code: 999 - Transaction has failed.

For duplicate payment –

- Response Code: 997- The bill has already been paid by the customer.

For Error in Request –

- Response Code: 998 – Invalid parameters in the payment request.

Below mentioned string is generated by our QR code image generator:

{"CONTENTS":"TaSFqf0UWx2wHnraTPQb33g028wxaJXdpiVMgDlnhm6UniFJ9ITvVh3ECZUOp4pKyE/LemgKYTbfyOjqrGHupW1WCDm0fbiye9TrfM0heIKap5b400qEetTXwPWikbVeIB8d9reUhr0Er0ZBoVfBMJfw/biePVyefQyK3NXISYO/sJ0VDmvdU+CxZw1n0MyEzoWn978/5+LtKad81vkTzqJeOfvUNxhS2MJeyOM4KtaUwyfdzJc



M5dtVuVqfzWl6/EkQW3x6R3F6MowsSKwXM5iHPcAfb28FqlXg4JjV7ew**MGD01**ImEbLdCepIYrBdJHSJ0ZTef3gzFsxLwEzUw+9WdAZ0tDrghbJC1XheQpOkDDswiie4u3SfIQaebxwHy0lPBawrqVNaIfALknVwxBKj3Ud8aY7KcI/brP96Umn3sdCqB0=","ID":299,"OPCODE": "QRBILLPAY"}
The above string 313th position, our decrypting key “MGD01” is placed. Logic to get this position is mentioned below:

ID=299 (generated a random number while request)

The formula to find out the key position is [Position=ID+14]

Therefore Position=299+14=313

Placing MGD01 key at position 313. This key is placed between the encrypted strings. Only our decrypting application will be knowing about this position. Accordingly application will find out key at this position and decrypt.

In the above string 313th position, our decrypting key “MGD01” is placed. Logic to get this position is mentioned below:

ID=299 (generated a random number while request)

The formula to find out the key position is [Position=ID+14]

Therefore Position=299+14=313

Placing MGD01 key at position 313. This key is placed between the encrypted strings. Only our decrypting application will be knowing about this position. Accordingly application will find out key at this position and decrypt.

This JSON string will attach to a URL and pass as a parameter between servers. The entire URL data is further provided encryption to 64 bit data. Below encrypted URL is mentioned:

<https://www.abccompany.com/BillPayWEB/PrePay.aspx?INPUT=cx8/ibnSTxWm+PJwmEk3JOLo4I+/bx3/CSU612hFjUFRBGiNkfEPX+JHX0Qsi/6JNm1kgxH+n52SVoQac6ADiiJqzJ/L4HV5Qg66ZAJmtear1pumsuaqPnsh+nL5fu3pfn3f4GtZHFVFBM6giMGZe9oFUGNcKt2iyASxT2KZTZTzQUpViYI3s79O7h9f7Ob0rr3YP CeX9NnxaHDzSQ/uzafLuywDVJq34XAGhieCJZS8gI+L/DvHfT9i/TejNVJFB3BIUzkaHLvhHQLJMHfuDY1HppdHtj+xLQVX4LjfJq9T3/nZ8Dj9OUMdeMsS4RxKON2KNWo+9Hv7eVKAAdgWApfVbtDUD9im7Izw6KBbGaUA84SIRg11dHCecXkKWLpGDSvfMV7Mp4d86Sye4p6BI95tdhNQxXSMp3oaeFoEGklpTlQwQPycEvzmVaCg2O+iLBR/7M2jDQ1BN/+D+NcUpvALvLvNY7oYM3qhnbmjyRSdH7cELNfuvpyhRdmCyh1gDqqNOxMDGvqqA2Fo8zKg43Cil1cUrgCNJMOGuH7Iu71fqWwYnokDCGZg4ZknHw/tGSeKxGFZpiUW5xVa4Pox1btqLXOkTY7TA/4RLti7q5MWt4fpQA2ZzJhgwiwvJQjm9>

III. RESULT AND CONCLUSION

A new innovative dimension of all types of bill payment has been invented here which is named as Mobile Bill Presentment System (MBPS). Using various technology, we have evolved with a very useful and compact way of bill payment which is highly convenient for the customer and economically feasible for merchants.

This innovative product overcomes all the limitations of the present bill payment scenario. MBPS is completely travelling on a secured electronic channels which does not involve any sort of paper receipts. This product is highly useful for the customer and the merchant as it is user friendly and economic. MBPS is also an ecofriendly

product as it completely avoids all kind of paper wastage because no hard cash and no paper receipts are provided in MBPS which will give us a greener environment.

REFERENCES

- [1]. Online Etymology Dictionary". Etymonline.com. Retrieved 15 November 2013.
- [2]. "Beyond Buying: Motivations Behind Consumers" Online Shopping Cart Use, Angeline G. Close, Ph.D and Monika Kukar-Kinney, Ph.D.
- [3]. Hobson-Jobson". Dsal.uchicago.edu. 2001-09-01. Retrieved 15 November 2013.
- [4]. Williams, John. "Cash Is Dead! Long Live Cash!", Federal Reserve Bank of San Fr
- [5]. The Benefits and Risks of Cloud Point-of-Sale via Tapas Technologies
- [6]. Jump up, Frazier, Bob (April 19, 2014). "Restaurant POS Software List". POS Advice Link.
- [7]. Kaplan, Karen. "Do-It-Yourself Solution: Small Grocery Chain Has Big Plans for Its Retailing Software", "Los Angeles Times".
- [8]. Jump up Micro-payment systems and their application to mobile networks, InfoDev report
- [9]. Kim, Ryan. "GoPago's line-skipping mobile payment system launches in San Francisco". Gigaom. Retrieved 2012-11-09.
- [10]. National Institute of Standards and Technology, Data Encryption Standard, FIPS 46-2, 1993.
- [11]. J. Daemen and V. Rijmen, AES Proposal: Rijndael, version 2, 1999.
- [12]. B. Schneier and D. Whiting, A Performance Comparison of the Five AES Finalist, 15 March 2000.
- [13]. J. Daemen and V. Rijmen, The Design of Rijndael, published by Springer-Verlag, 2002.