QR CODE GENERATION USING ECC CRYPTOGRAPHY
Mr. Ganesh Bhagwat, Ms. Rajlaxmi Nayak

(Information Technology, Mumbai University, India)

ABSTRACT

Mobile payment system being one of the widely expanding mobile services, it has security concerns that prevented its wide acceptance. Some of the main security services given prior attention in mobile payment are issues of privacy, authentication and confidentiality. This paper used ECC cryptography technique for the encryption of QRCODE. The encryption and decryption of QRCODE is barrier of security issue of mobile payment system. If the encryption time of QRCODE is high. Its invites the security threats for transaction

Keywords: Cryptography, Decryption, Encryption ECC, QRCODE

[1] INTRODUCTION

Encryption is a procedure that progresses and information into a mystery code. It is one conceivable method for concealing information so that lone approved clients can read it. Mystery key or secret word is expected to empower decoding process. Encryption is the most capable technique to disentangle information [1]. Encryption is by and large ordered in two fundamental sorts. The essential encryption strategy is symmetric encryption and topsy-turvy encryption. The trouble level of topsy-turvy encryption lies in the challenges of numerical computation in tackling modulus for an extraordinary number. Awry encryption utilizes two keys. People in general key
are utilized for encoding plaintext and the private key is utilized for decoding the cipher text. As a result of the multifaceted nature of computation, deviated encryption reassure a considerable amount of time. In the other hand, symmetric encryption is less tedious on the grounds that the key of symmetric encryption additionally have less difficult computation than hilter kilter encryption. Lamentably, the mystery key of symmetric encryption is less secured that deviated on the grounds that the mystery key is shared by the collector and the sender. So it is essential to circulate mystery key of symmetric encryption safely. The dominant part of encryption framework utilizes the symmetric technique since its calculation is single, straightforward and very much acknowledged. The most essential thing is that the era of the mystery key is basic and simple since it utilizes a similar key for encryption and unscrambling. The downside happens when the gatecrasher succeeds stole the mystery key so they can without much of a stretch open the message. Thusly, the key conveyance system ought to be finished with a safe technique to make symmetric encryption secure [1].

[2] QR CODE ENCRYPTION

Amid critical exchange utilizing versatile installment, all information ought to be secured. Accordingly, a few information concealing technique ought to be utilized to guarantee that the data is right and is gotten or sent by confirmed gathering. In this paper, Encrypted QR Code through PKI is examined for securing data in the portable installment framework. Securing encryption key needs trusted-outsider that has obligations to guarantee that both sides are genuine clients. The examined framework is appeared in Figure [1]. This installment framework can be utilized for the immediate installment framework and online installment framework. In view of Fig., the primary client ought to give their client ID to the vendor. The dealer will ask for an open key to the outsider. This outsider ought to be trusted. In the wake of getting a demand from dealer then outsider check client ID to database and produces a couple segment of key (open and private key).

People in general key and the private key is constantly created for every exchange and has a specific time restrict. their versatile installment framework uses a key match plan to create distinctive open and private keys for different individuals in the meantime, and even a similar individual gets different keys at various circumstances. To bolster key combine period, the clock of the client, shipper, and the outsider must be synchronized. After open and the private key is produced, then people in general key is sent to the vendor gadget, and the private key is sent to the client. To get the correct private key, the client ought to sign into the application on his cell phone. These two methods for verification technique will guarantee that the client is a genuine gathering.

In the wake of accepting the general population key, this open key is utilized by the vendor to encode exchange data. From that point forward, the vendor will create QR Code from the encoded data of the exchange. In this versatile installment framework, QR Code is utilized to store installment data, for example, cost and shipper's record number. QR Code is utilized as shared verification amongst trader and customer. Just particular purchaser can read the QR Code and paid it to the record number. Other than that, by utilizing this common verification strategy, it will ensure the client as the pays party from undesirable withdrawal installment by the wrong party. It additionally shields the shipper from extortion parties which have the probability to hoodwink installment affirmation to another record number.
Figure 1.1: QR Code encryption through PKI.

At last, QR Code prepared to be checked by clients. QR Code that created by vendor go about as virtual record number installment. There is a restrict period to check the QR Code in light of the fact that the key match (open and private key) has constrained time. On the off chance that the client does not affirm the installment amid as far as possible, the QR Code will be terminated. In the wake of affirming the installment, the QR Code can't be utilized any longer. In this installment framework, shared confirmation is finished by the outsider that guarantees legitimating amongst client and shipper. It is likewise significant not putting away login data and secret key on the telephone. All information ought to be prepared and put away in the server.

Prior to the information leaving cell phone, all data should be scrambled.

Process block diagram of encryption and decryption
Figure 1.2 shows the process of encryption and decryption of QRCode.

[3] PROBLEM STATEMENT

Several implementations have emerged as the key methods to use a cellular phone in remote network authentication. One such solution focuses on using cellular phone as a standalone OTP token [6]. The phone is a computational platform to generate the OTP code. The OTP generating software, user’s secret seed and counter value are stored in the cellular phone. In operating the token, the user activates the software. The phone generates the OTP code. The user reads the OTP code and enters it into a PC or Internet device for 2FA need. Once authenticated, the user is allowed to access the network. These simple mobile tokens usually do not have any capability to resist the OTP seed (K) tracing by MITM interception or Shoulder-surfing attacks. Moreover, it stores the secret seed and counter value. These secrets can be exposed if the phone is lost or stolen [7,8]. The network security is comprised then. Amid critical exchange utilizing versatile...
installment, all information ought to be secured. Accordingly, a few information concealing technique ought to be utilized to guarantee that the data is right and is gotten or sent by confirmed gathering. In this paper, Encrypted QR Code through PKI is examined for securing data in the portable installment framework. Securing encryption key needs trusted-outsider that has obligations to guarantee that both sides are genuine clients [9, 10].

[4] QR CODE GENERATION ARCHITECTURE

QR Code generation: QR code era is the primary module of their talked about approach. In that they will produce a QR code with included encoding procedures which coverts their unique private information into various QR codes. Regularly QR code is an enhanced encoding system which implies it scrambles given information and in addition packs the scrambled into decreased size. The span of given information will be lessened when utilizing an encoding strategy. QR code is additionally performs like an encoding component. QR codes are presently utilized over a considerably more extensive scope of versatile applications and business applications [4].

Figure 1.3: QR Code Generation Architecture

[5] COMPARATIVE RESULT

Figure 1.4: comparative performance for www.google.com with elapsed time using RSA and ECC method in our implementation.
CONCLUSIONS

In this dissertation we enhanced the security strength of QR code. For enhancement of security of QRCODE we used ECC cryptography technique. The ECC cryptography technique is public cryptography technique and more secured in compression of RSA and other cryptography algorithm. Selection of ECC asymmetric encryption among asymmetric encryptions improves efficiency and speed of encryption calculation of QRCOE is calculated and data is decrypted with very high speed in ECC method and its security is higher than that of other asymmetric algorithms. The encryption for securing mobile payments reached in the work is as such mature. It makes use of the industry standard technology for wireless PKI and in it the generally agreed models have been adopted. For a payment system, the functionality of the system is, however, quite limited.

REFERENCES


