# Enhance The Security Strength of QRCode Using ECC Algorithm for Online Transition

**Alok Tripathi**
Department of Computer Science & Engineering, PIT
Bhopal (M.P) India
aloktripathi432@gmail.com

**Asst. Prof. Surendra Vishwakarma**
Department of Computer Science & Engineering
PIT, Bhopal (M.P) India
s.vish83@gmail.com

**ABSTRACT**

Smart devices play major role in electronic payments transaction. The mobile payments reduce the cost of traditional payments transaction. The payments of mobile devices faced a problem of security threats. The process of mobile payments system used the internet and communication medium. The internet and communication medium compromised with security attacks. The security attacks create some finical frauds and many illegal behaviors over the payments. In this paper present the review of mobile payments system using secured communication and transaction system. The secured mobile transaction used the QR code and many asymmetric cryptography techniques for the prevention of security threats. The capabilities and limitations of mobile devices introduce some challenges for designing effective and efficient authentication mechanisms. Some of the most important differences between authentication requirements and principles in mobile devices.

**Keywords: - ENCRYPTION, DECRYPTION QRCode, ECC, RSA.**

**INTRODUCTION**

Encryption is a procedure that progressions an 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 [1-2].

Encryption is by and large ordered in two fundamental sorts. The essential encryption strategy is symmetric encryption and topsy-turvy encryption [14-15]. 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 is 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 has less difficult computation than hilter kilter encryption [5-7]. Lamentably, the mystery key of symmetric encryption is less secure 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[16].

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[11-13]. 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 [3-4].

Rest of this paper is organized as follows in Section 2 discusses about proposed work as an encryption of QRCODE, Section 3 discusses about the process block diagram of QRCODE encryption and decryption. Sections 4 describe the simulation process of proposed model and finally discuss the conclusion & future scope in Section 5.

**2. PROPOSED WORK**
**(**ENCRYPTION OF QRCODE)

This section discusses the encryption and description process of QRCODE. The process of encryption and decryption used RSA and ECC algorithm. the encryption and decryption process given below

Algorithm of Convert Plaintext to QRCODE

Step 1: write message (text).

Step 2: generate QR code for the message.

Step 3: save QR image as P.

Algorithm of Convert Key to QRCODE

Step 1: write key as numbers or text.

Step 2: generate QR code for the key.

Step 3: save QR image as K.

Algorithm of get Begin Indies of Data Area in QR

Step 1: start.

Step 2: Do loop to get beginning of data area in plain.bmp with width i as height j.

Step 3: end.

Algorithm of Encryption

Step 1: start.

Step 2: load QR image P.

Step 3: load QR image k.

Step 4: define cipher as bitmap file with dimensions' width (wd) & height (hg).

Step 5: Call function to put P(0)(0) to P(i)(j) in cipher(0)(0) to cipher(i)(j).

Step 6: loop statement x=i

loop statement y=j

cipher(x)(y) =P(x)(y) XOR k(x)(y)

next y,x.

Step7: end.

Algorithm of Putting Key in Cipher Bitmap File

Step 1: start.

Step 2: binarization each character or number in key as 8bit.

Step 3: loop statement l

```
If (key(l)=255)
    Key(l)=254;
Else
    Key(l)=1;
End if.
        Next l
```

Step 4: if statement

```
If (key(l)=255)
    Key(l)=253;
Else
    Key(l)=2;
End if.
```

Step 5: end.

Algorithm of Getting Key from Cipher Bitmap File

Step 1: start.

Step 2: loop statement until key(l)=253 or 2

```
If (key(l)=254 or 1)
    Str=concat(str,'1');
Else
    Str=concat(str,'0');
End if
Next l
```

Step 4: collect each 8bit in str and get character of this collection.

Step 5: end.

Algorithm of Decryption

Step 1: start.

Step 2: load QR image c.

Step 3: get width (wd) & height (hg) of c.

Step 4: define plain as bitmap file with dimensions width (wd) & height (hg).

Step 5: Call function to put cipher (0)(0) to cipher(i)(j) in plain(0)(0) to plain(i)(j).

```
Step 6: loop statement x=i
            loop statement y=j
            plain(x)(y)=cipher(x)(y) XOR key(x)(y)
    next y,x.
```

Step 7: end.

**3. PROCESS BLOCK DIAGRAM OF QRCODE ENCRYPTION AND DECRYPTION**

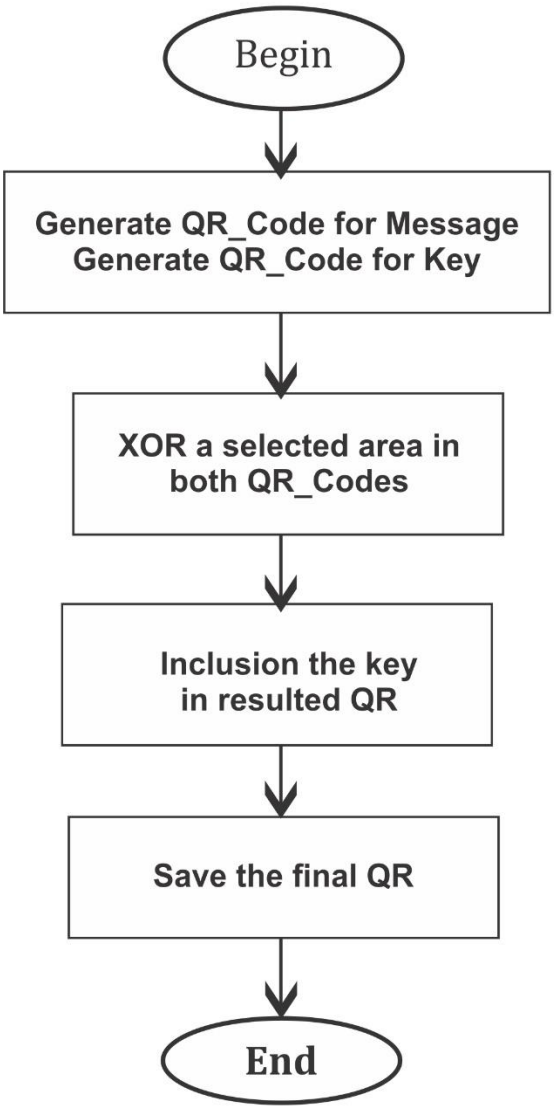


Figure 1: shows that process of encryption of QRCOE

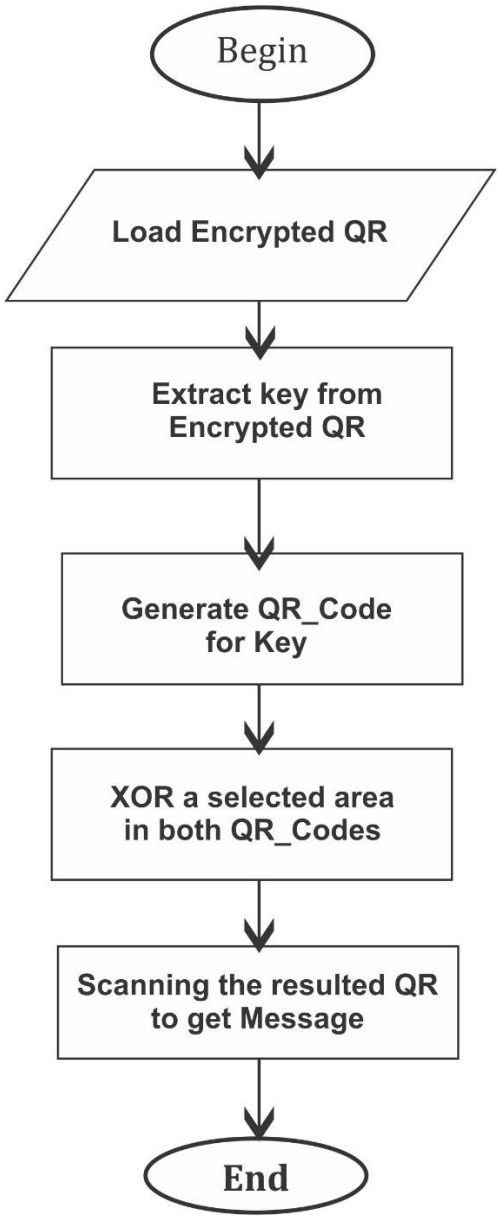


Figure 2: shows that process of decryption of QRCOE

.

**4. EXPERIMENTAL RESULT**

To evaluate the performance of QRCODE Encryption for online mobile payment transition. For the encryption of QRCODE used to algorithm one is RSA another is ECC. For the implementation of QRCODE and encryption algorithm used ASP.NET. For the scanning of QRCODE used android based mobile application the name is QRCODE scanner. The QRCODE scanner redirects the link of QRCODE massage.


Figure 3: Window show that the QRCode generator creates QR code of www.bhopalorg.com address.

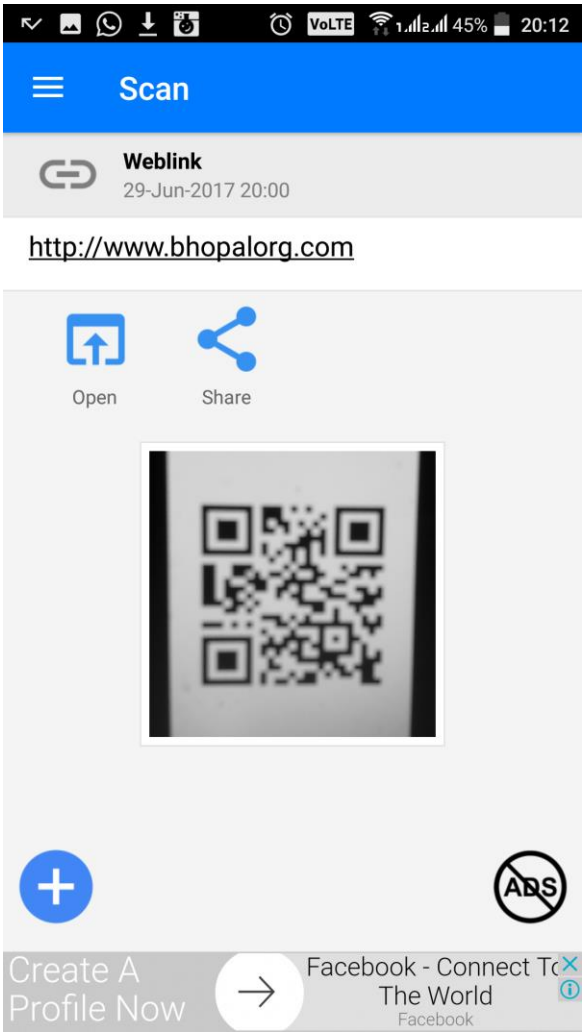


Figure 4: Window show that open view of our software with right sign to capture QR code automatically website show with http://www.bhopalorg.com, which is installed in our android platform.

| NAME OF TECHNIQUES | ELAPSED TIME |
|---|---|
| RSA | 1.856 |
| DES | 1.0444 |

Table 1: Comparative performance evaluation using QRCODE of www.bhopalorg.com for RSA and DES techniques.

| NAME OF TECHNIQUES | ELAPSED TIME |
|---|---|
| RSA | 1.157 |
| DES | 9.451 |

Table 2: Comparative performance evaluation using QRCODE of www.google.com for RSA and DES techniques.

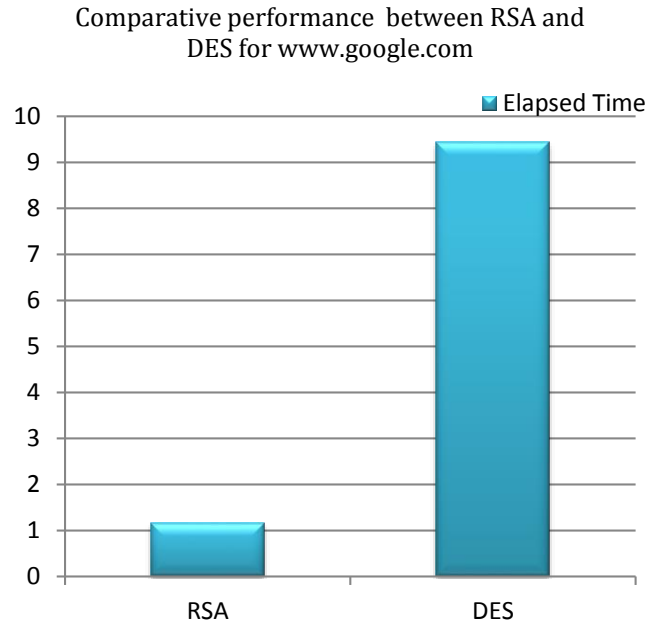


Figure 5: comparision performance for www.google.com with elapsed time using RSA and DES method in our implementation.

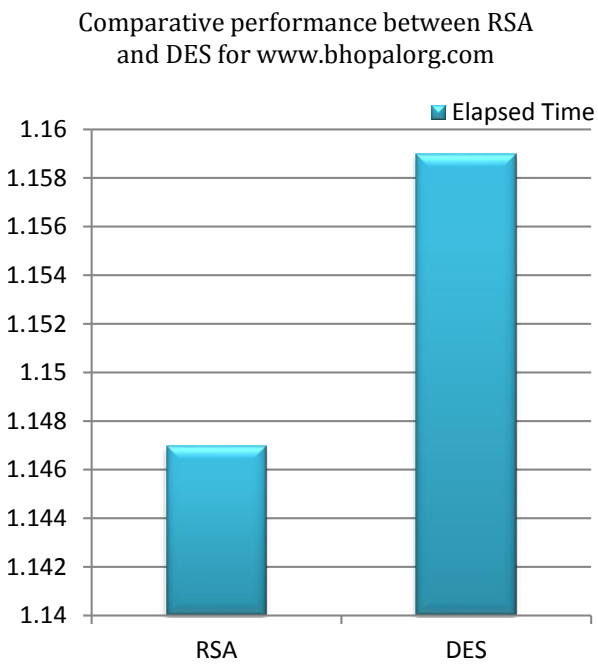


Figure 6: comparision performance for www.bhopalorg.com with elapsed time using RSA and DES method in our implementation.

## 6. CONCLUSION AND FUTURE WORK

In this dissertation enhanced the security strength of QR code. For enhancement of security of QRCODE 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 QRCODE 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

[1] Ariana Tulus Purnomo, Yudi Satria Gondokaryono and Chang-Soo Kim "Mutual Authentication in Securing Mobile Payment System using Encrypted QR Code based on Public Key Infrastructure", IEEE, 2016, Pp 194-198.

[2] Boris Pokrić, SrđanKrčo and Maja Pokrić "Augmented Reality based Smart City Services using Secure IoT Infrastructure", IEEE, 2014, Pp 1-6.

[3] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun and Kouichi Sakurai "Authentication in mobile cloud computing: A survey", Elsevier, 2016, Pp 1-23.

[4] R. Sharmila and m. Mohamed sithik "smartphone base d secure color qr code using visible light communication", IJARBEST, Pp 314-319.

[5] Najmeh Mashhadi "Authentication in mobile cloud computing by combining the two factor Authentication and one-time password token", Ciência e Natura, 2015, Pp 220-229.

[6] Norbert Pohlmann, Markus Hertlein and Pascal Manaras "Bring Your Own Device for Authentication (BYOD4A) – The Xign–System", Springer, 2015, Pp 1-10.

[7] Maarten H. Everts, Jaap-Henk Hoepman and Johanneke Siljee "UbiKiMa: Ubiquitous authentication using a smartphone, migrating from passwords to strong cryptography", ACM, 2013, Pp 1-6.

[8] Tao-Ku Chang "A Secure Operational Model for Mobile Payments", Scientific World Journal, 2014, Pp 1-14.

[9] Nael Hirzallah and Sana Nseir "a mobile payment system with an extra token of security", International Journal of Computer Engineering and Applications, 2014, Pp 81-93.

[10] Fumiko Hayashi and Terri Bradford "Mobile Payments: Merchants' Perspectives", Federal Reserve Bank Of Kansas City, 2014, Pp 33-57.

[11] S. H. V. C. Silva, E. L. Flôres, G. A. Carrijo, A. C. P. Veiga, and M. B. P. Carneiro "SWEP Protocol and S-Wallet System - Mobile Payments using Near Field Communications", Hindawi, 2014, Pp 1-7.

[12] Florian Otterbein, Tim Ohlendorf and Marian Margraf "Mobile Authentication with German eID", arXiv, 2017, Pp 1-12.

[13] Preeti Garg and Dr. Vineet Sharma "Secure Data Storage in Mobile Cloud Computing", International

Journal of Scientific & Engineering Research, 2013, Pp 1154-1159.

[14] Piotr K. Tysowski and M. Anwarul Hasan "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds", IEEE, 2013, Pp 1-13.

[15] Adam Ali.ZareHudaib "E-payment Security Analysis in Depth", IJCSS, 2014, Pp 14-24.

[16] V.N.V.H Sudheer and J.Ranga Rajesh "Secure Ciphering based QR Pay System for Mobile Devices", International Journal of Emerging Trends in Engineering and Development, 2013, Pp 662-669.