Design & Implementation of Secure QR Payment System using Visual Cryptography

Dr G Charles Babu[1], Dr Balasani Venkata Ramudu[2], *G Sathish[3]
[1]Professor, Gokaraju Rangaraju Institute of Engineering and Technology, Telangana
[2]Associate Professor, SVR Engineering college, Nandayala, Kurnool
[3]Assistant Professor, St. Martin's Engineering College, Secunderabad, Telangana–500100
Email: gsathishit@smec.ac.in

ABSTRACT

Design and implementation of a secure link sharing system based on QR codes. QR codes have been extensively used in recent years since they speed up the link sharing process and provide users with ultimate convenience. However, as convenient as they may sound, QR-based online systems are vulnerable to different types of attacks. Therefore, link sharing needs to be secure enough to protect the integrity and confidentiality of every process. Moreover, the link sharing system must provide authenticity for both the sender and receiver of each transaction. The security of the proposed QR-based system is provided using visual cryptography. The proposed system consists of a web application that implements visual cryptography. The application provides a simple and user-friendly interface for to share links through QR Code.

Keywords: Cryptography, QR code, Encryption, Decryption, Authentication.

I. INTRODUCTION

Online payment methods are rapidly developing and gaining traction in many industries. Different implementations that utilise this ground-breaking technology have resulted in the emergence of the digitization of the transation wich is secure and safe for user to make payment. The evolution of online payment is unquestionably one with a potentially much brighter future, from credit cards to NFC-based payment. But as technology evolves, the risks associated with securing it grow. Analysis of several online payment system implementations showed the security is the main and important feature for the users how use the software Payment transactions are typically vulnerable to theft, fraud. The confidentiality, authenticity, and accessibility of the information are at risk due to these security issues. Any online payment system's ability to overcome security obstacles while also delivering the best customer experience and gaining users' trust is crucial to its success.

Large quantities of data may be encoded and stored using two-dimensional matrix barcodes called QR codes [1, 2, 3]. Numerous essential applications, including health, education, and finance, have made substantial use of QR codes because of their quickness and ease [4, 5, 6, 7, 8]. In the literature, a variety of safe QR-based digital payments have been suggested [9–15]. [9] presents many payment options, each of which offers varying degrees of security and speed. The Peer-to-Peer Model and the Operator Centric Model are two examples of these models.

By utilising both public and private keys for each transaction in these models, security is increased. Upon registering a user, they online payment system method suggested in [10] uses both the private and public key. The different set of public and private keys which will be used for authentication and the security purpose for the use to make safe payment and it produced by an RSA key generator. The keys are created using a random seed number, the user or customer ID, and the Mobile Equipment Identity (IMEI). In order to guarantee which is integrated to the produced certificates and the transaction communications between users while ensuring non-repudiation, The scheme proposed in [11] modifies and the scheme [10] by turning off the SHA-256 method of the elliptic curve digital signature technique .Visual cryptography is defined in [12] as a method that employs any quantity of shares to conceal a

picture. The method outlined in [13] combines QR codes with visual cryptography. It is made up of three components: a smartphone, the verification server and the barcodes detectors. The method described in [14] creates two parts using a (2, 2) VCS, and then feeds these two shares through a this decoding function converts into numerical string. It is suggested in the study for usage of QR codes to power a secure online payment system. Two cryptographic methods, visual cryptography and private key cryptography, have been contrasted the necessary security for the suggested system.

The primary limitations of employing public key cryptography in payment systems are the requirements, validation, and achievement of security goals by third parties for the storage of private keys and certificates on the device. the generation of public and private keys. Image encryption, and enables secrecy, integrity, and authentication while requiring the least amount of processing time and computing speed. It also does not involve the sending of any personal information. The proposed online payment system has been given security using visual cryptography as a result of these performance discrepancies. Given that the proposed payment system hinges on sending data-carrying QR codes, the security required will be provided by protecting the QR code itself. by Using the most recent advancements in steganography and cryptographic algorithms, visual cryptography is a way for safeguarding visual data, or the QR code itself in the case of a suggested project. The remainder of this paper is organised as follows: The proposed system's general layout is described in Section II, while its implementation is covered in Section III. In Section IV, the study's conclusion, the findings and future directions for research are discussed.

II. PROPOSED SYSTEM DESIGN

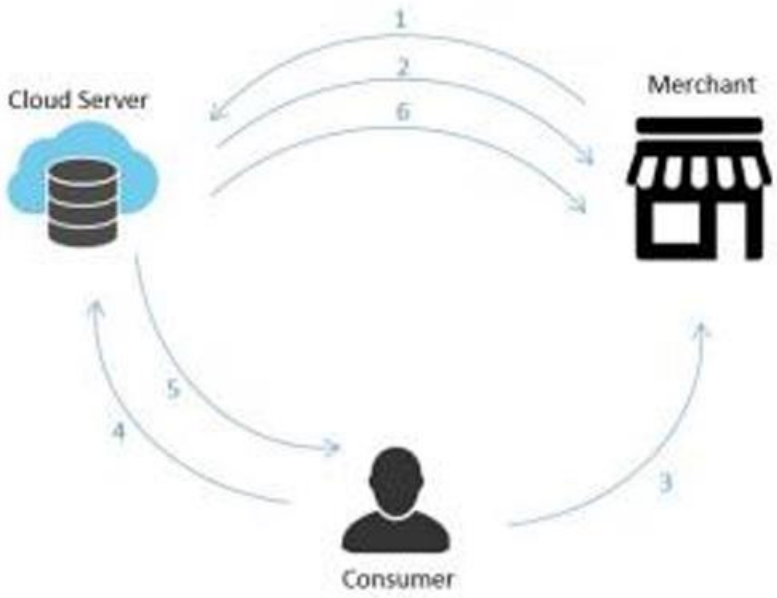

Fig. 1. General workflow of the proposed QR payment system

An explanation of the suggested QR-based online payment system is given in this section. In the first subsection, the system's functional description will be provided, along with specific operational processes. After that, the second sub-section discusses security issues. The possibility of establishing consumer and merchant accounts has been examined in this research. In order to increase security, consumer accounts have the option to receive and transfer credit, whilst merchant accounts can only accept money. In Fig. 1, the suggested QRbased online payment system's architecture and operational flow are depicted. The system is made up of the three components—the cloud server, the consumer, and the merchant—as seen in the image.

The three parties' communication during a payment transaction is described by the operational processes below:

Step 1: The first stage entails from the cloud server the merchant requesting a per-bill Quick Respond
Step 2: The second stage is when a QR code with a share embedded in it is sent by the cloud server.
Step 3: involves scanning a QR code by a customer to begin a transaction.
Step 4: involves submitting a payment request to the cloud server's backend system.
Step 5: the cloud server completes the transaction and sends the conformation number to the user.
Step 6: The merchant receives the processing results for approval.

Security Considerations

The visual cryptography scheme (VCS) algorithm which is employed in the design to secure user-to-user transactions, is used. It is built on a (2, 2) VCS, where two shares are formed, and the two shares must be stacked to display the original image. The input can be encrypted at one end and then decoded at the other due to the bidirectional nature of the technology. The encryption and decryption of images, as well as QR codes, are carried out on the server's end to increase security and eliminate any chance of manipulation at the client's end. A merchant requests payment to start and provides an estimated amount in advance before the service is rendered. One of the produced shares is transferred by the programme to the merchant in the form of a scannable Quick Response code. Using the merchant data provided by the server, it creates the standard Quick Response code, feeds it into VCS, and outputs the code. The other portion will be kept by the server. When the Quick Response code is scanned, the corresponding twin share will be purchased along with the other share, and a successful transaction will be completed. Fig. 2's left side illustrates the process of making two shadows from a Quick Response code, and its right side illustrates the procedure for verifying a Quick Response code after scanning.

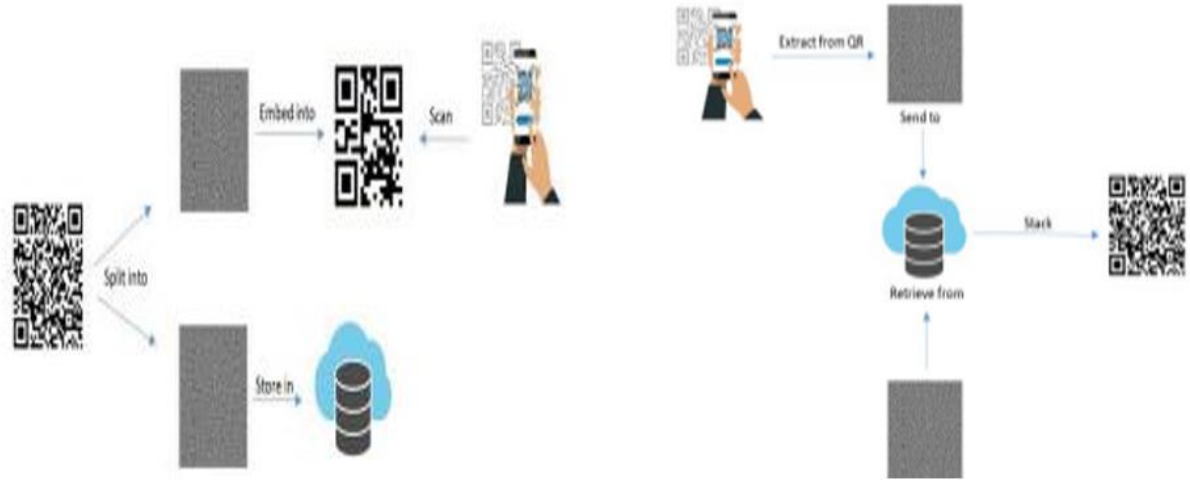

Fig. 2. (left) Construction of (2, 2) VCS, and (right) Stacking of (2, 2) VCS

III. SYSTEM IMPLEMENTATION

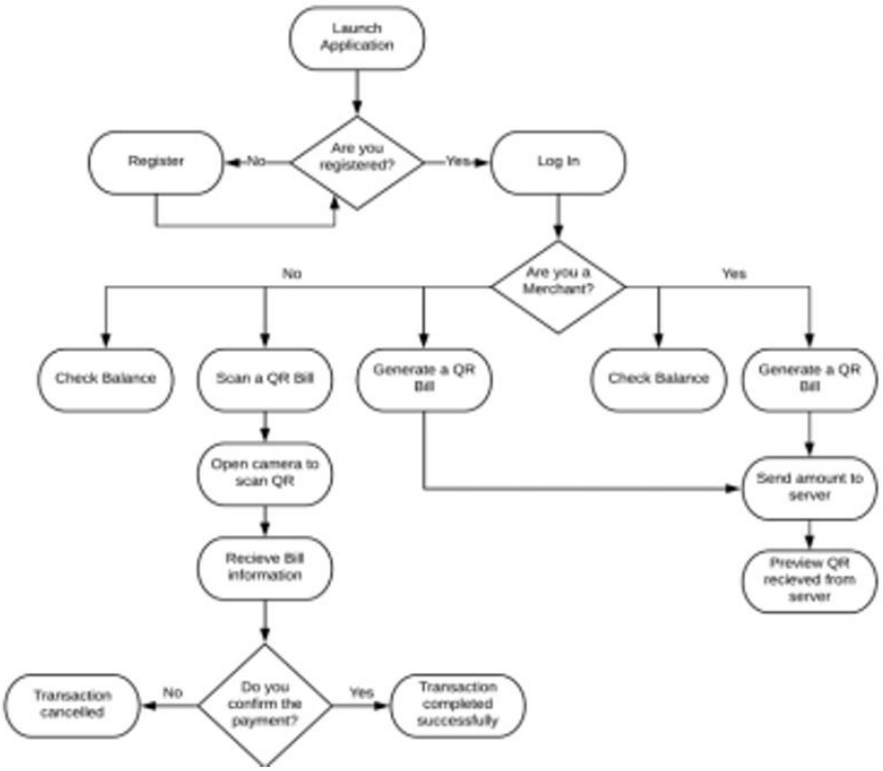

Fig. 3. High-level functional implementation of the proposed payment system

It employs a method based on software. The user's mobile device was the only piece of hardware necessary to complete the given activities and criteria. The user interface of the Android app launches a server that manages transactions and authentication. Using Android Studio, an integrated development environment for Google's Android platform, this app was created in Java. The server, which was created in Python, joins your home network and serves as a payment gateway for mobile payment applications. When a mobile application makes a request, the server handles the database data that is kept in its own storage area and performs the requested processing. The system's entire functional implementation is shown at a high level in Figure 3.

The smartphone app features an intuitive user experience for payment system users. It just serves as a communication channel between users and the payment gateway server. Depending on the registration procedure, which involves giving personal information that will be hashed and transferred to the server, users can either be customers or merchants.

Depending on whether they are users or merchants, users can generate or scan a QR code after logging in. Figure 4 shows the registration screen (left),where a new user must provide personal data, including name, email, password, phone number, and whether they are a customer or a merchant.

Fig. 4. (left) Registration page, (center) Home page for merchant, and (right) Home page for customer

After signing in, the user is brought to the homepage, where options like Generate Quick Response (QR), Scan Quick Response code(QR), and Check Balance are provided according on the type of user they are. Fig. 4 displays the homepages of both a consumer and a merchant user (centre and right). When a user selects the Generate QR Code option, the application then directs them to Fig. 5, where they are asked to enter the appropriate bill amount to begin the payment process. Following an unsuccessful attempt to connect with the server, the application replies with a QR code containing the share. The resulting QR code does not contain any user-specific data.

When a consumer chooses to pay a Quick Respond code invoice, the application is brought to the Scan page once the Scan Quick Response Code option has been chosen. In Fig. 6, a camera is what makes up the scan page. For access to the phone's camera, the application must first receive permission from the user. When access is granted, the camera will immediately begin to scan the QR code and transfer the information sent to the server for feather processing. Then the server has confirmed the payment transaction, the client is provided a confirmation box

with the bill amount and the receiver of the funds, giving them the option to accept or reject the transaction.

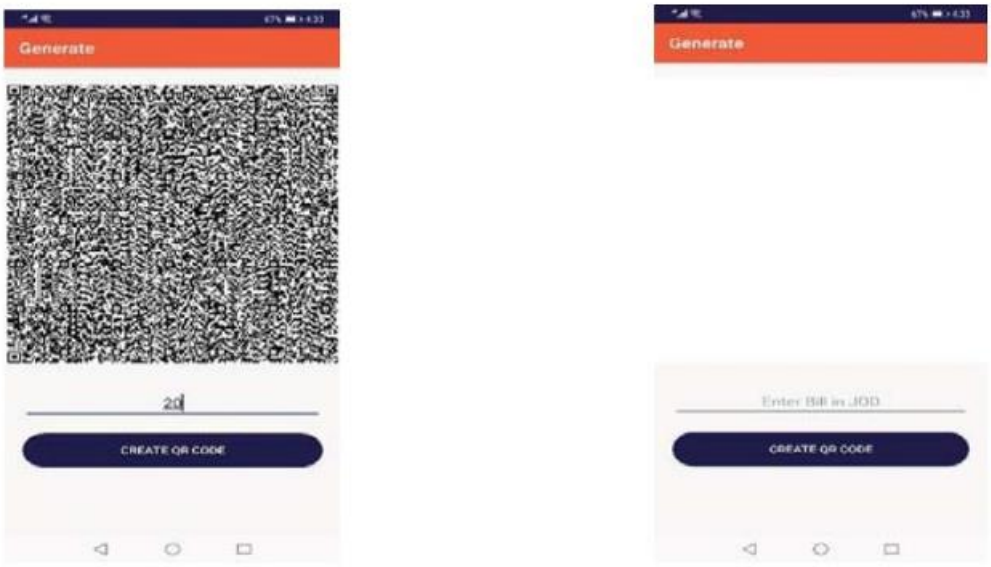

Fig. 5. 'Generate Quick Response code' page with a requested amount of 20 JOD

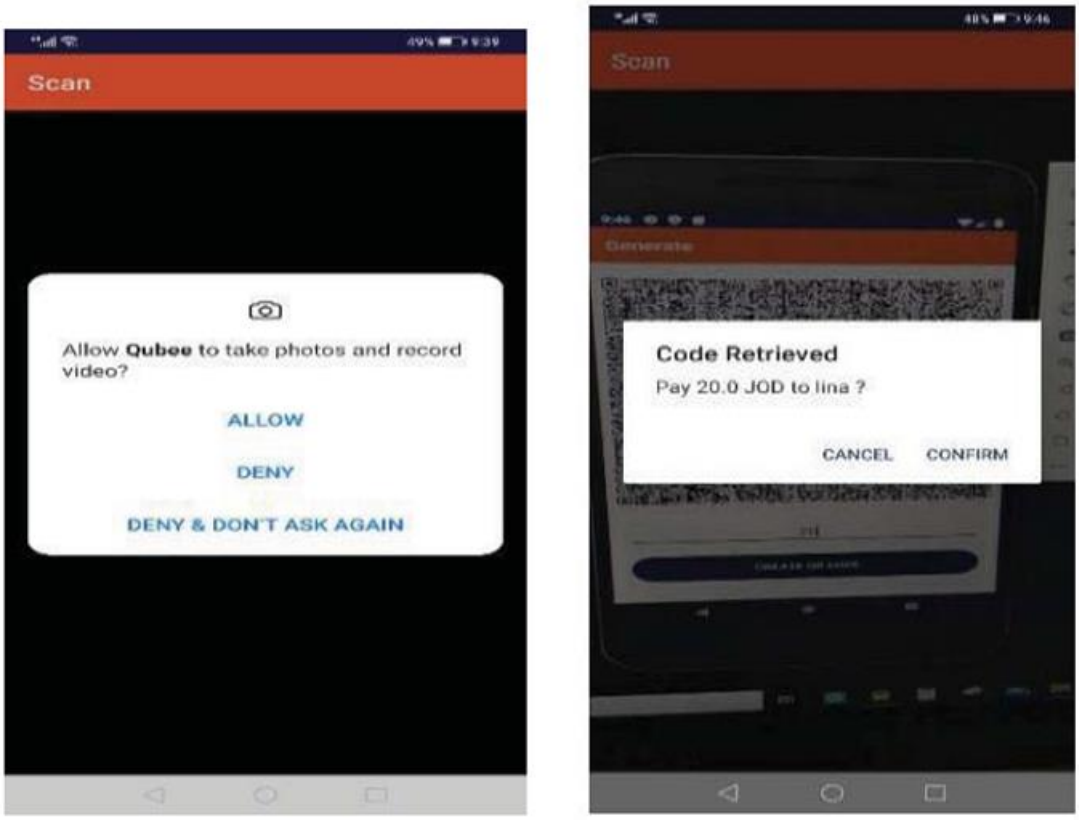

Fig. 6. Scan QR-code Page

IV. CONCLUSION

In conclude, companies have greatly profited from the developments in online payment technology, which have also markedly increased customer pleasure. Due to the fact that the payment process is concealed from the user, technology replacements are looking into ways to speed up, make it safer, and make it more inventive. Online payment errors cannot be accepted because of how easily a variety of cyberattacks are now conceivable because to the ease of online payment systems. Data leak, denial of service, fraud, and forgeries are a few of the

assaults. Numerous strategies of various complexity have been proposed to lessen these hazards. This study suggests a secure QR-based online payment solution.

The recommended system's security stands out since it modifies a single algorithm to provide the necessary security services: To provide authentication, confidentiality, and integrity, visual cryptography is utilised. Users will soon be able to create static Quick Response codes that are connected to their accounts exclusively owing to a new feature that will be included. These static Quick Response codes are read, allowing the payee to enter the minimum payment but without saving the balance.

Sessions may be used to keep users registered in as an added convenience rather than the current programme, which requires the user to log in each time the software is launched.

A last security update includes setting up multiple threads on the server to detect and remove Quick Response codes that have been saved for further than five minutes.

REFERENCES

[1] Francisco Liébana-Cabanillas “User behaviour in QR mobile payment system: the QR Payment Acceptance Model” University of Granada, Granada, Spain, https://www.tandfonline.com/doi/abs/10.1080/09537325.2015.1047757?cookieSet=1

[2] SUEBTIMRAT, Panupong “User behaviour in QR mobile payment system” Graduation School of Business, Assumption University https://koreascience.kr/article/JAKO202100569464364.page

[3] Nishant Goel; Ajay Sharma; Sudhir Goswami” A way to secure a QR code:”, publisher: IEEE: https://ieeexplore.ieee.org/abstract/document/8229850

[4] I.J. Information Engineering and Electronic Business, 2022, 3, 10-18 “QR: Approaches for Beautified, Fast Decoding, and Secured QR Codes” Published Online June 2022 in MECS

[5] Li-Ya Yan.Kampar, Malaysia “QR code and mobile payment”, Universiti Tunku Abdul Rahman, Kampar, Malaysia: https://www.sciencedirect.com/science/article/abs/pii/S0969698920313084#!