International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
***Article Received**: 29 November 2022 **Revised**: 12 January 2023 **Accepted**: 10 February 2023*

Visual Cryptography-Based Secure QR Payment System Design And Implementation

[1]Mysore Venkata Siva Sandeep, [2]Sanskruti Dube [3]Hamsitha Challagundla, [4]Pulaparthi Nikhilesh Chand
[1] School of Information Technology, Vellore Institute of Technology, Vellore, India.
Email: mysoresandeep8@gmail.com
[2] School of Computing Science and Engineering, Vellore Institute of Technology, Bhopal, Madhya Pradesh, India.
Email: sanskrutidube@gmail.com
[3] School of Information Technology, Vellore Institute of Technology, Vellore, India.
Email: hamsitha.c@gmail.com
[4] School of Electronics Engineering, Vellore Institute of Technology, Vellore, India.
Email: nikhileshcp@gmail.com

Abstract: It is important to validate the Merchant and the Client to increase confidence in online transactions. At present, only the Client is checked against the merchant server. The research in this paper will show you how to create and launch a QR code-based payment system that is both secure and convenient for users. As a result of their capacity to facilitate instantaneous transactions and offer unparalleled ease of use, QR codes have seen explosive growth in the past few years. QR-based online payment systems are easy to use but susceptible to various assaults. So, for the level of security given by transaction processing to hold, the secrecy and integrity of each payment procedure must be guaranteed. In addition, the online payment system must verify each transaction from both the sender's and the recipient's perspectives. The study's QR-based method is kept safe through visual cryptography. The suggested approach takes advantage of visual cryptography via a web-based application.

Keywords: QR code, software development, security, cryptography, authentication.

I. Introduction

The rapid development of online payment methods across all sectors has a global impact. The widespread adoption of this cutting-edge technology is a direct result of digitizing the financial transaction process in payment systems. Advances in payment methods, such as credit cards and near-field communication (NFC), point to a brighter future for online shopping. Trust issues are much less prevalent in traditional businesses than in e-commerce systems. Customers and clients typically pay in cash or with a credit card after seeing and examining a product in person. E-commerce eliminates the need for a physical storefront and paper receipts by relying solely on electronic transactions and images of the goods sold [1]. The hardware and software that make up the online payment system enable customers to purchase digitally. Customers need a way to tell if an online store is legitimate before doing business with them.

But as technology advances, so are the hazards in keeping it secure. According to the analysis of many online payment system deployments, security is a big worry for users and business owners [2]. Theft, fraud, and impersonation are frequent threats to payment transactions. These security flaws risk the system's availability, confidentiality, and integrity. Any online payment system's success depends on its capacity to solve security challenges while providing the best user experience and winning customers' trust [3].

Information can be encoded and stored in a QR code, which is a two-dimensional matrix barcode. QR codes' efficiency and ease of use have led to widespread adoption in various vital sectors, including healthcare, education, and the financial industry. There have been many proposed methods of making safe online payments using QR codes. Several payment options are available, each with security and processing time.

Protecting user privacy is essential as multimedia technology utilizes digital photos increasingly frequently. Picture encryption is crucial for the user's privacy and security against unwanted user access [4]. Many industries use image encryption, including telemedicine, medical imaging, multimedia systems, and military communication.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
***Article Received**: 29 November 2022 **Revised**: 12 January 2023 **Accepted**: 10 February 2023*

Many full-color images have been sent, received, and stored via wireless networks and the WWW since the development of multimedia and network technology. Data encryption methods are distinct from image encryption methods. The integrity and confidentiality of the image must be maintained due to the numerous security issues with digital image processing and transmission. Digital images are less sensitive than data since a single altered pixel does not affect the complete image. In other words, a modest adjustment is permitted even if a digital image is more vulnerable to attackers than data [5].

Based on QR codes, a safe online payment method is provided. Public key cryptography and visual cryptography have been evaluated for the level of security needed for the proposed system. The primary drawbacks of employing public key cryptography in online payment systems are the cost of creating the public and private keys, the requirement for a third party to obtain and authenticate certificates, and the need to secure the storage of the private keys and certificates on the device. By offering confidentiality, integrity, and authentication without the need for the transmission of any personal data, visual cryptography, on the other hand, offers speedy computation and minimal processing time. Visual cryptography has been utilized to assure security for the suggested online payment system based on these performance disparities. The suggested payment method requires sending data-carrying QR codes. Hence protecting the QR code will provide security. In the proposed concept, the QR code will be encrypted using visual cryptography, a method made possible by recent developments in steganography and cryptographic algorithms.

Under the scope of this article, we will develop and execute a secure QR payment paradigm. Despite widespread adoption and convenience, QR code-based payments are vulnerable to many threats. Every transaction must be authenticated for both the sender and receiver to ensure security and confidentiality. When transferring substantial sums of money, it is common for large corporations to prefer to keep their wallet addresses/UPI IDs/etc. Under the proposed method, the receiver will have access to a web-based program allowing them to encrypt the original QR Code for the transaction before transforming it into a picture and the associated link being made available to the sender in the form of a QR Code. This QR code can be scanned to reveal a link to an accompanying image and then decrypted within the app to reveal the authentic QR Code for payment.

II. Problem Statement

A two-dimensional matrix barcode called a quick response (QR) code is information storage and encoding. Due to their speed and convenience, QR codes are now widely used in various important fields, such as finance, healthcare, and education. Several QR-based online payment methods put security first. There are numerous payment options, each with speed and security features. Which technique offers less security and encryption? The architectures are depicted in Figs. 1 to 3 and include three examples: the Operator Centric Model, Bank-centric Model, and Peer-to-Peer Model (Image source: [20]).

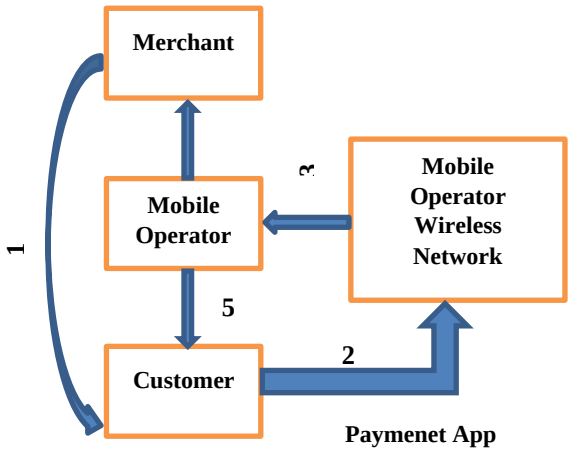

Fig. 1. Operator Centric Model (OCM)

The steps of OCM are given below:

Step 1: The merchant gives information to the customer.
Step 2: Submit to Mobile Payment Application.
Step 3: Transaction Information
Step 4: Accounts Payable.
Step 5: Sending Wireless bill to the customer.

The steps of BCM are given below:

Step 1: Customer passes information
Step 2: Merchant initiates transaction
Step 3: Request Payment
Step 4: Confirm the payment
Step 5: Settle the transaction

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
Article Received: 29 November 2022 Revised: 12 January 2023 Accepted: 10 February 2023

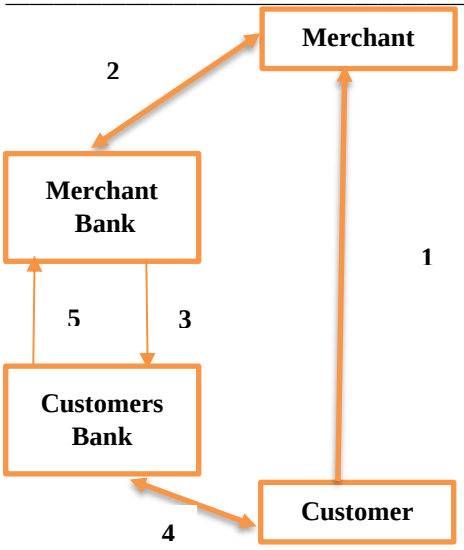

Fig. 2. Bank Centric Model (BCM)

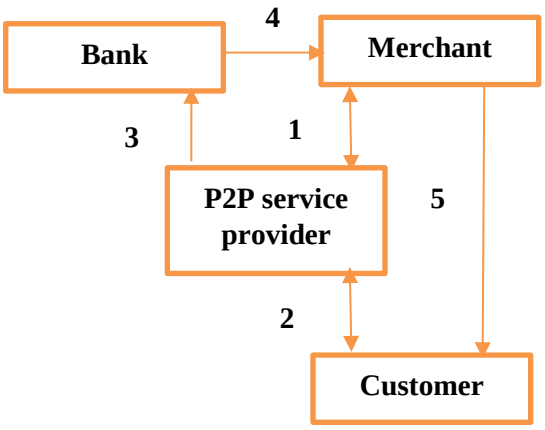

Fig. 3. P2P Model

The steps of P2P model are given below:

Step 1: Initiate the transaction
Step 2: Confirm the transaction
Step 3: Issue Transfer
Step 4: Settle the amount
Step 5: Delivery to the customer

The major objectives of the work include:

(i). Security for QR-based transactions should be achieved using visual cryptography techniques.

(ii). For users to conduct the encryption and decryption processes for QR codes during transactions, user-friendly web-based software must be created.

III. Literature Work

Designed to be swiftly decoded by smartphones, QR codes are two-dimensional matrices that may store more information than traditional 1-dimensional barcodes. QR codes provide many advantages over traditional barcodes, including the ability to hold more information, be scanned, be read from any direction, be error-correcting and come in many variants. There are a few different types of QR codes that users can select from: logo QR codes, encrypted QR codes, and QR Codes. Today, more and more people are making use of this technology. With the proliferation of smartphones, QR codes have found widespread acceptance. There are a lot of papers out there about how to make transaction processing systems safer. This section only briefly discusses a small handful of works that are relevant to the topic at hand.

The authors of [6] examined the models used for mobile payments. Researchers have suggested a mobile payment approach that, by requiring the retailer to initiate the transaction, boosts transaction speed and security. This is because the third-party service providers' (bank, mobile companies) connection to the merchant will be quicker than its own.

Using a novel method based on 2-D barcodes, the authors of [7] introduced a payment system for mobile users. A mobile payment system was proposed, along with its architecture, design, implementation, and other QR 2D barcode-based security measures. Its payment options allow for seamless cross-border transactions through smartphones or tablets.

QR code technology, its advantages, its many possible applications, and its impact on marketing and the world of technology were all explored in [8]. Quick Response code, or QR code, for short. It's a 2-D matrix code built with two things in mind: the need to hold more information than conventional 1-D barcodes and the desire for rapid decoding on mobile phones and other portable devices. There are several benefits to using QR codes, including the fact that they can store much information, be scanned, be read from any direction, and even correct mistakes.

Researchers in [9] developed a novel method for protecting customers' personal information while facilitating funds

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
***Article Received**: 29 November 2022 **Revised**: 12 January 2023 **Accepted**: 10 February 2023*

transfers during online purchases. Without complex cryptographic calculation, Visual Cryptography can break down a secret captcha into two irregular patterns of images called shares. The unique QR code devised by the authors of [10] has two levels of information storage: a personal level that unauthorized parties cannot access and a public level that any conventional QR reader can read. Using the theory of visual cryptography in the suggested system lowered the computational cost of the algorithm (VCS). And the QR code's most valuable feature—it is capacity to remedy mistakes—was kept intact. The proposed technique was shown to be practical and reasonably secure through experiments, and its performance was much better than that of prior designs [11].

In [12], the authors performed research. They suggested a unique mechanism for QR code security anti-counterfeit based on the fusion of visual secret sharing (VSS) and QR code (called VSSQR scheme), which may significantly enhance the Security of QR code payment. The inventors of [13] developed a QR code fast pass terminal application system. As a replacement for the previously-used forgeries of static QR code patches, this user-friendly receiving application solution allows for faster and more secure scanning of QR codes, ultimately leading to a more secure payment system. Because of this, both customers and business owners can save money on losses they could have avoided. Based on the network and the current order details, a unique QR code (one for each invoice) can be generated and displayed.

The authors in [14] applied Visual Cryptography to create and improve text-based Captcha, taking advantage of its unpredictability for each encoding process and visual recognizability with naked human eyes. Two common attack models built with deep learning were used in experiments to demonstrate the method's efficacy. This VC-enhanced text captcha design has the potential to reduce the recognition rate. The goal of [15] was to give researchers a high-level perspective from which to choose the most suitable visual cryptography techniques for their specific needs. The research gave an overview of the different types of visual cryptography methods and discussed some recently suggested systems in this area. The study investigated and contrasted more than 40 visual cryptography systems suggested during the past two decades. According to the results, more study is needed to solve persisting issues such as pixel expansion, low recovered-image quality, and computational and memory difficulties.

QR codes have found widespread application, but security concerns have arisen due to their large storage capacity and speedy machine recognition. As a solution, we suggest using three-tiered QR codes for a group of people, with the first and second tiers containing information that is both publicly and easily readable. In contrast, the third tier contains private data encrypted using visual cryptography. Analysis and experimental results show that the proposed scheme improves upon the previous schemes in several ways and can encode three-level information in multiple distributed QR codes [16]. The work [17] introduces a QR code-based, expansion-free, meaningful visual cryptography method to reduce noise-like sharing in traditional VCS. This method avoids attackers when distributed over public networks. QEVCS keeps visual cr18yptography computation-free and recovery image size the same as intimate images by limiting halftoned image grey levels. QEVCS protects image privacy, according to experiments.

The authors in [18] present a security solution for QR codes that address the worries of both consumers and creators. The system can work with any current QR code encoder, which complies with the current standard. An Android mobile app is used to develop and test the system. It was discovered that there is some lag time involved in the system for integrity checking and content validation. The wprl flow of this work is shown in Fig. 4. The security systems are incorporated in several cloud systems also for server reliability [19]

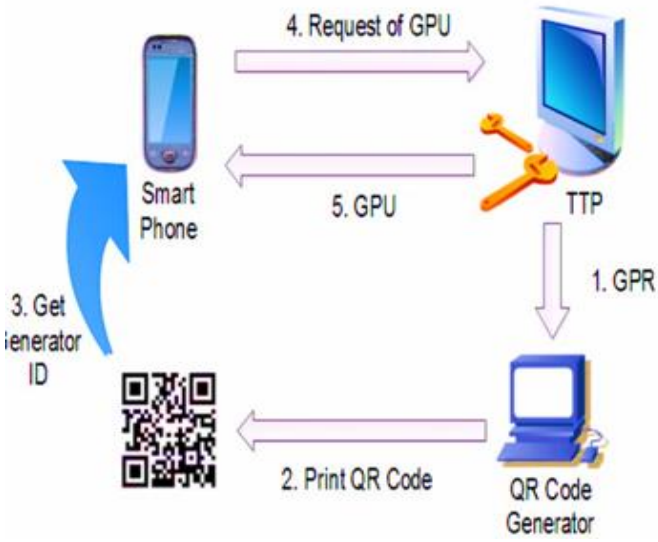

Fig. 4 Flow of the work in [18]

IV. Proposed Work

A completely new system for exchanging links is proposed in this project. It is based on image encryption and QR

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
Article Received: 29 November 2022 Revised: 12 January 2023 Accepted: 10 February 2023

Codes, both barcodes. The URL will be encrypted after it has been transformed into a QR code; the URL of the encrypted QR code will then be transformed into a QR code once more. Even if we share the QR Code with others, only those with access to an image decryption tool can decrypt it and access the link. This secures the QR Code and prevents anyone from accessing the URL even if we share the QR Code.

(i) The fact that the actual link is obscured and can only be seen by a select few people with system access contributes to the system's increased level of safety.
(ii) There is no third-party involvement.
(iii) Because there is no embedding, there is no reduction in the quality of the QR Code.

The user will be able to view an encrypted visual image as soon as the user has scanned the QR code. We can provide the user with a secure KEY, "which can be generated just once and can also serve the purpose of an OTP in ordinary net banking." With the help of this KEY, he can decrypt the visual representation and, as a result, obtain the authentic QR code that will allow him to pay the money and conclude the transaction. The flow of the encryption and decryption mechanisms are shown in Fig. 5 and Fig. 6.

A cipher in which others repeatedly replace the letters of the plaintext. The replacement technique is an older form of encryption in which individual characters in a message are changed to other letters, numbers, or symbols. With encryption, information can be hidden from prying eyes. When regular text is encrypted in such a way that it is unreadable, we refer to it as cipher text. Each character in plain text is replaced by another character from the same fixed set of characters in a substitution cipher, with the replacement determined by a key. With a single change, A would become B, B would become C, and so on. The QR code can store data horizontally and vertically, unlike the barcode, which can only do so.

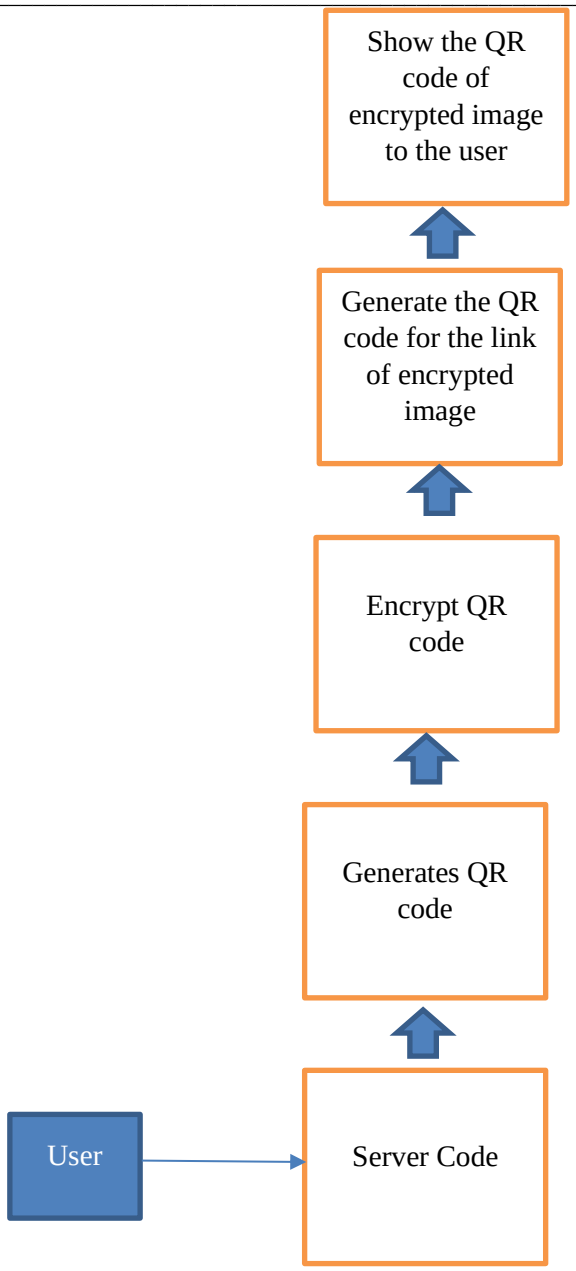

Fig. 5 . Encryption

As a result, the QR code can store almost a hundred times more data.

(i) Go to the URL you wish to share and enter it.
(ii) On the top toolbar, click the trio of vertical dots ().
(iii) Click Share.
(iv) Go to the pop-up and choose QR Code.

Hold your phone up for someone to scan the code, or click Download at the bottom. Theft of data, denial of service

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
Article Received: 29 November 2022 Revised: 12 January 2023 Accepted: 10 February 2023

attacks, fraud, and forged documents are all examples of such attacks. Several intricate defenses have been set up to thwart these assaults.

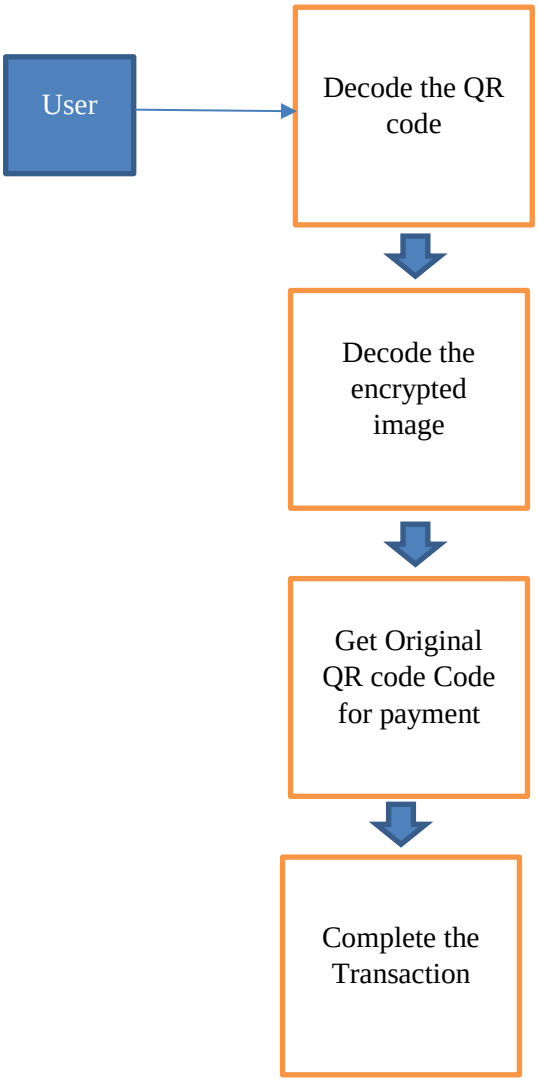

Fig. 6. Decryption

we developed a secure QR Code sharing app and showed how it might be implemented using image cryptography to create more robustly encrypted links. When the customer is ready to proceed, the merchant will generate a QR Code for the URL (it may be the transaction URL if it is a UPI payment; otherwise, it may be the wallet address if it is a blockchain payment). When he presses the "submit" button, a QR Code for the Site is generated and saved in the database.

This QR ode will be converted into an encrypted image using the replacement encryption technique used in visual cryptography. This particular visual image will be given a URL, and that URL will be given a QR Code as well. After scanning the QR code, the individual will be presented with a link to the URL of the visual image. After providing this link for the visual image, the customer will be authorized for the transaction and given the original QR Code, which he can scan to obtain the original URL or wallet address.

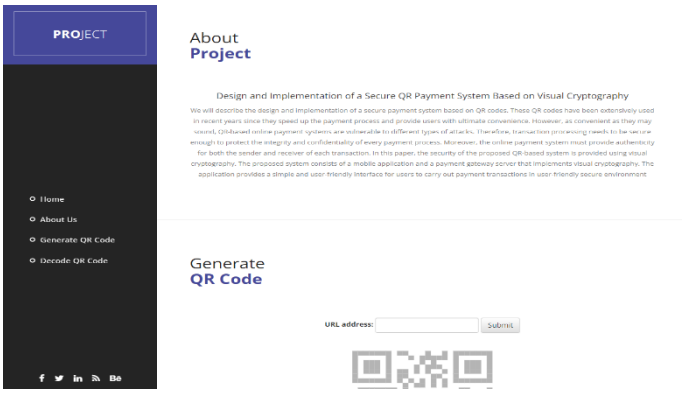

Fig. 7. User Interface Home Screen

Once the customer has done this, the transaction will be completed. The sample screens of the user interface and options are shown in Fig. 7 and Fig. 8. Fig. 7 is the user interface home screen, Fig. 8 is the generating page of the QR code, and Fig. 8 is where you can run the algorithm to make the prediction.

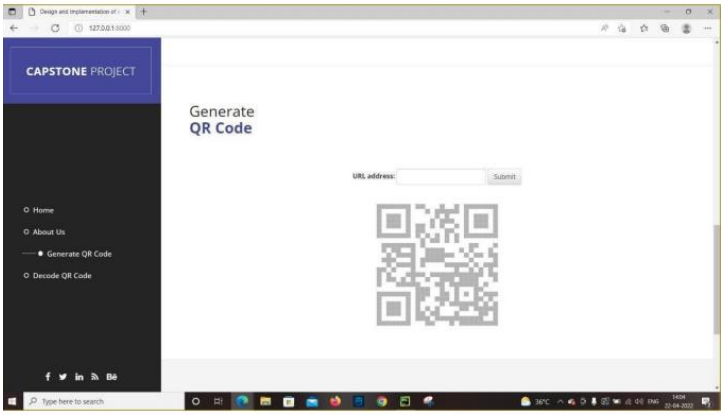

Fig. 8. QR generation code

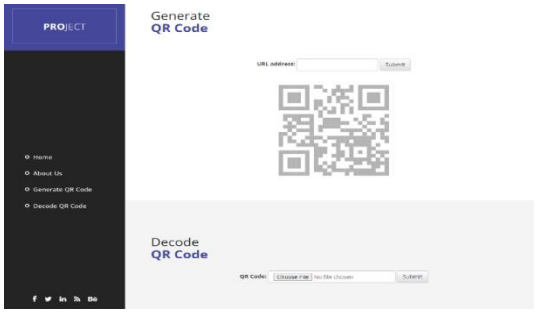

Fig. 9. Prediction Page

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2127
Article Received: 29 November 2022 Revised: 12 January 2023 Accepted: 10 February 2023

V. Conclusion

Improved customer service directly results from the commercial sector's widespread adoption of online payment methods. Because the user is not involved, companies that provide technological alternatives constantly look for new and interesting ways to speed up, secure, and improve the payment process. Internet payment systems are more vulnerable to malicious hacking due to their widespread adoption and ease of use. As a result, mistakes must be tolerated. This attack takes many forms, including information theft, DoS attacks, fraud, and forgery. To counter these attacks, strong defenses have been put in place. Any app that accepts payments might theoretically be modified to use the proposed methodology. More security can be added by using multithreading on the server to erase the QR Codes after a set period and disabling the user's ability to take a screenshot of the QR Code during the payment process.

REFERENCES

[1] Cun, Q., Tong, X., Wang, Z., & Zhang, M. (2023). A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing. *The Visual Computer*, 1-20.

[2] Zhao, J., Wang, S., & Zhang, L. (2023). Block Image Encryption Algorithm Based on Novel Chaos and DNA Encoding. *Information*, *14*(3), 150.

[3] Xiong, L. S., & Badarch, T. (2023). Research on Designs of Modern Payment Systems in China. *American Journal of Computer Science and Technology*, *6*(1), 10-19.

[4] Lakshmi, T. N., Jyothi, S., & Kumar, M. R. (2021). Image Encryption Algorithms Using Machine Learning and Deep Learning Techniques—A Survey. In *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Latest Trends in AI, Volume 2* (pp. 507-515). Cham: Springer International Publishing.

[5] Reddy, K. U. K., Shabbiha, S., & Kumar, M. R. (2020). Design of high-security smart health care monitoring system using IoT. *Int. J*, *8*.

[6] Nseir, S., Hirzallah, N., & Aqel, M. (2013, March). A secure mobile payment system using a QR code. In *2013 5th International Conference on Computer Science and Information Technology* (pp. 111-114). IEEE.

[7] Ma, T., Zhang, H., Qian, J., Hu, X., & Tian, Y. (2015, January). The design and implementation of an innovative mobile payment system based on a QR bar code. In *2015 International Conference on Network and Information Systems for Computers* (pp. 435-440). IEEE.

[8] Tiwari, Sumit. (2016). An Introduction to QR Code Technology. 39-44. 10.1109/ICIT.2016.021.

[9] Rajguru, P., Dhomse, J., & Pawar, P. Y. (2018). Securing Online Transaction Using Visual Cryptography. *J Telecommun Syst Manage*, *7*(158), 2167-0919.

[10] Cheng, Y., Fu, Z., Yu, B., & Shen, G. (2018). A new two-level QR code with a visual cryptography scheme. *Multimedia Tools and Applications*, *77*, 20629-20649.

[11] Fu, Z., Cheng, Y., & Yu, B. (2018). Visual cryptography scheme with significant shares based on QR codes. *IEEE Access*, *6*, 59567-59574.

[12] Wan, S., Yang, G., Qi, L., Li, L., Yan, X., & Lu, Y. (2019). Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code. *Mathematical Biosciences and Engineering*, *16*(6), 6367-6385.

[13] Baidong, H., & Yukun, Z. (2019, February). Research on Quickpass Payment Terminal Application System Based on dynamic QR Code. In *Journal of Physics: Conference Series* (Vol. 1168, No. 3, p. 032059). IOP Publishing.

[14] Yan, X., Liu, F., Yan, W. Q., & Lu, Y. (2020). Applying visual cryptography to enhance text captchas. *Mathematics*, *8*(3), 332.

[15] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. *Multimedia Tools and Applications*, *80*, 31927-31952.

[16] Fu, Z., Fang, L., Huang, H., & Yu, B. (2022). Distributed three-level QR codes based on visual cryptography scheme. *Journal of Visual Communication and Image Representation*, *87*, 103567.

[17] Ren, L., & Zhang, D. (2022). A QR code-based user-friendly visual cryptography scheme. *Scientific Reports*, *12*(1), 7667.

[18] R. M. Bani-Hani, Y. A. Wahsheh and M. B. Al-Sarhan, "Secure QR code system," *2014 10th International Conference on Innovations in Information Technology (IIT)*, Al Ain, United Arab Emirates, 2014, pp. 1-6, doi: 10.1109/INNOVATIONS.2014.6985772.

[19] Kalyani, B. J. D., & Rao, K. R. H. (2018, April). Assessment of physical server reliability in multi cloud computing system. In *AIP Conference Proceedings* (Vol. 1952, No. 1, p. 020045). AIP Publishing LLC.

[20] Ahmad, L., Al-Sabha, R., & Al-Haj, A. (2021, March). Design and Implementation of a Secure QR Payment System Based on Visual Cryptography. In 2021 7th International Conference on Information Management (ICIM) (pp. 40-44). IEEE