

# SECURING QR CODE OF USER DETAILS THROUGH AUTHENTICATION

1 Mr. J. Mahesh, Assistant Professor, Department of CSE, Teegala Krishna Reddy Engineering College,

Telangana, India. [maheshjella09@tkrec.ac.in](mailto:maheshjella09@tkrec.ac.in)

2 J. Rupa, Department of CSE, Teegala Krishna Reddy Engineering College, Telangana, India.

[rupajogu4@gmail.com](mailto:rupajogu4@gmail.com)

3 K. Yashodhadevi, Department of CSE, Teegala Krishna Reddy Engineering College, Telangana, India.

[yashodhadevi10@gmail.com](mailto:yashodhadevi10@gmail.com)

4 M. Sanjeevana, Department of CSE, Teegala Krishna Reddy Engineering College, Telangana, India.

[sanjeevana.madishetti30@gmail.com](mailto:sanjeevana.madishetti30@gmail.com)

**Abstract:** Protecting and hiding private information about people has become harder in modern times because of the constant danger of identity theft and data breaches. People face big financial and social risks when they are vulnerable to illegal access and fraud. Because of this, we urgently need strong systems to protect private data and make sure it is sent and checked securely. Because of this problem, QR codes have become a useful way to share information between different apps. QR codes are popular in many areas, from personal recognition to tickets and registration, because they can store a lot of different kinds of information tightly and securely. But because QR codes are so popular, they have raised new security worries, especially about the accuracy and privacy of the information they hold. A lot of QR code systems out there use data forms that aren't safe, which means that personal information can be stolen. To fix these security holes, it is important to set up strict access rules and identification systems for QR code use. By only letting approved users scan QR codes, the risk of data

being accessed and changed without permission can be reduced. In conclusion, QR codes make sharing data easier and faster than ever before, but it is very important to keep them safe and private. People can better keep their private information safe from people who shouldn't have access to it by using strong security measures and limited access controls.

*Index terms* – QR code, forgery, Secure, Robust.

## 1. INTRODUCTION

There is a type of bar code called a QR code that can store data and be read by smartphones. It is a two-dimensional code. "Quick Response" (QR) means that the code's information should be read very quickly and very quickly. On a white background, the code is made up of black blocks grouped in a square design. It could be words, a URL, or some other kind of data that is compressed. The QR code was made so that its information can be read quickly. Around the world, QR codes are becoming more and more popular very quickly. These days, most people use

phones with cameras built in to read QR codes. Denso Wave, a Toyota company, created QR codes in 1994. They were first used to keep track of supplies in factories that made auto parts. One of the ideas behind the QR code was that barcodes can only hold so much information (20 alphanumeric characters at most). Though they were first created to keep track of parts used in making cars, QR codes are now used in a huge range of other areas, from business tracking to fun, product labeling in stores, and smartphone apps. Once users read a QR code, they can open a URL and get text. People can make their own QR codes that other people can read and use by using sites or apps that make them. A QR code generator and a QR code reader make up the device. The encoder is in charge of recording data and making the QR Code. The decoder, on the other hand, reads the data from the QR code.



Fig 1 Overview of QR

A quick look at how the QR code works. The QR code encoder is given simple text, a URL, or other data, and it creates the needed QR code. When we need to access the data in the QR code, we use a QR Code decoder (scanner) to read the code and get the data from it.

The different forms of the QR Code sign are called forms 1 through 40 [4]. Each version has a different number or arrangement of parts. These are the black and white dots that make up a QR Code. "Module

configuration" is the number of modules that are housed in a sign. Version 1 has  $21 \times 21$  modules, and Version 40 has  $177 \times 177$  modules.

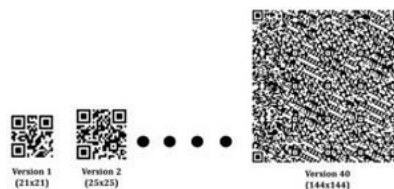


Fig 2 Version module configuration of the QR Codes

## 2. LITERATURE SURVEY

An increasing number of people are interested in using QR codes to hide and verify private information. This is because they could help with security issues in many different situations. Several experts have looked into different ways to make systems that use QR codes safer and more private. Dey et al. [1] suggested using a QR verification method to hide and get back private encrypted data. In the same way, Shetty [2] came up with advanced methods for hiding private data and then using QR codes to get it back.

Gupta et al. [3] talked about how QR codes can be used to make sure that court papers are real. Their study shows how important it is to keep private and accurate information safe, especially in court situations where document accuracy is very important. Using the Advanced Encryption Standard (AES) formula, Bhavar et al. [4] came up with a way to verify messages hidden in QR codes. This made sending data through QR codes even safer.

Even though QR codes make it easy and quick to share information, there have been issues raised about

their security (see literature). Barcode-in-barcode attacks were looked into by Dabrowski et al. [11], which showed that QR codes could be vulnerable to security risks. Their study shows how important strong security steps are to protect private information stored in QR codes from these kinds of attacks.

Cai et al. [12] suggested using sequential module modulation to make QR codes that look good and have a lot of storing space. This method not only makes QR codes look better, but it also makes it easier to store data on them. This creates new opportunities for sending and storing data securely. Focardi et al. [14] did a study that compared security risks and answers for two-dimensional barcodes, such as QR codes. According to their study, QR code systems are weak points and they suggest ways to make them safer from possible threats.

Wahsheh and Luccio [16] looked at how secure, private, and easy to use QR code readers are. This gave us more information about how people use and think about systems that use QR codes. Their results help us learn more about how people use and like to interact with QR codes, which is important for making apps that are both safe and easy to use. Reeder et al. [17] used experience sampling to look into how people react to browser warnings in the real world. The results show how people see and react to security messages in real life. Their study tells us a lot about how well security measures work at making people more aware of risks and encouraging safe behavior.

Overall, the literature review shows that more and more people are interested in using QR codes for safe data transfer and identification. There are also ongoing efforts to deal with security issues and make QR code-based systems more resistant to risks.

### 3. METHODOLOGY

#### i) Proposed System:

The suggested system for safe QR codes includes a thorough method that covers creating, sending, and reading QR codes, all while putting security and resistance to possible threats first. This system uses strong methods and standards for making QR codes and verifying identities. This makes sure that the stored data is correct and real. To protect against risks like QR code fraud, the system uses strong security methods like digital signatures to make sure that QR codes are real. Adopting encryption, secure communication methods, and regular security updates can also help protect the hardware and software systems used to read QR codes from security holes. To meet privacy issues, personal information is collected through QR code scans as little as possible, and steps are taken to protect user privacy. This includes making data anonymous when possible and limiting who can see private data. Overall, the suggested method for safe QR codes uses a multi-layered approach to security, including both technology and routine protection to make sure that QR code-based systems are safe and reliable.

#### ii) System Architecture:

System architecture is the high-level organization of a system that shows how its parts work together and relate to each other. It's a mental picture that shows how a system works and what its structure and actions are.

The system architecture is like a plan for how the system will be designed and built in a project. It helps

the project team figure out how the system is put together and how the different parts will work together to make the system do what it's supposed to do.

Our plan is to make sure that only certain people can view the QR code, and those people should only be given a phone number when the QR code is created. So that unknown people can't use the QR code.

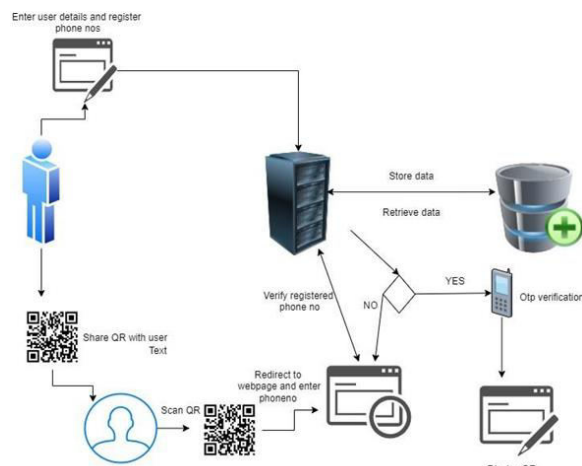


Fig 3 Proposed Architecture

There are several steps needed to complete the QR code project. Python3 is used to make the QR codes, VS Code is used as the code editor, and database connections and GUI frames are added. The steps for implementation are broken down below:

### 1. QR Code Generation Function (Python):

To make QR codes, use the "generateCode()" method. This method should take input from the user and save the QR code it makes in the place given. You can add information about a person to the database by calling the "add()" code.

### 2. Database Connectivity and Data Storing (Python):

Use Python to set up database connection. Connect to the database and set up methods to store information about users in the database. 'sqlite3' libraries are good for SQLite databases, and 'mysql.connector' libraries are good for MySQL databases.

### 3. GUI Frames (Python):

Use Python's "tkinter" tool to make GUI frames that make it easy for people to make QR codes. Design frames that can take user data like name, phone number, etc., and show the QR code that was made.

### 4. Button Generate QR Code (Python):

Use "tkinter" to make a button that will generate a QR code. When the button is clicked, the "generateCode()" method should be used to make the QR code and store the user's information in the database.

### 5. Web Page (HTML/CSS):

Use HTML and CSS to make a webpage that checks phone numbers against a database. Include areas for adding the phone number and a button that will start the comparison.

### 6. PHP Code to Compare Phone Number (PHP):

Write PHP code to compare phone numbers put on the website with those in the database. You can get and compare phone numbers by using PHP's database connection tools.

### 7. Integration:

Add the Python tools that make QR codes and link to databases to the GUI frames. Make sure that the

client (GUI) and server (Python scripts) can talk to each other without any problems.

**8. Testing and Debugging:**

Test the system thoroughly to make sure it works and is reliable. Fix any problems that came up during testing and make sure that the web page, database, and QR code generation all work the way they're supposed to.

By doing these things, the QR code project can be completed successfully, giving users a safe and quick way to create and store QR codes and check phone numbers against the database.

The user's information and phone number will be saved in the database as soon as they enter them.

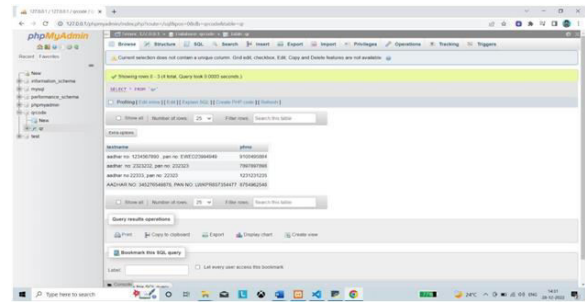


Fig 5 User details stored in database QR

The QR code will be made and saved at the same time in the place chosen by the user.

**4. EXPERIMENTAL RESULTS**

This is the QR code GUI that stores information like the user's name and phone number in the database and saves the generated QR code in the place chosen by the user.

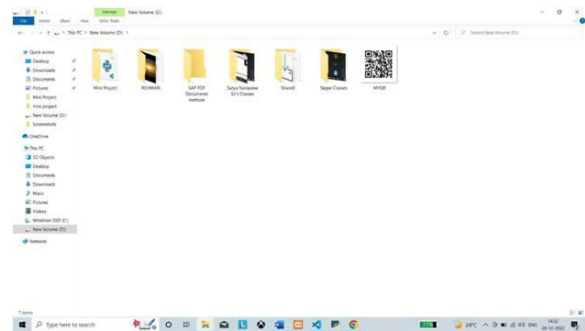


Fig 6 QR code generated and stored in specific location

Take a picture of the QR code and copy the URL.

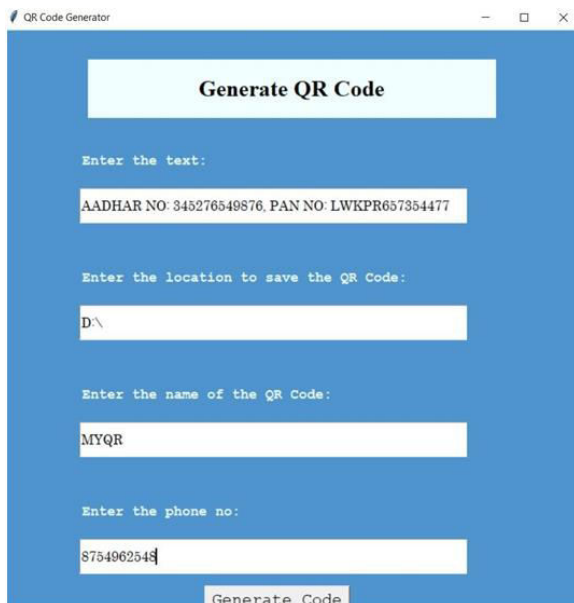


Fig 4 QR code generation GUI

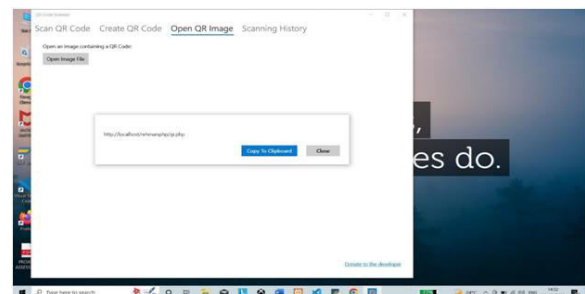


Fig 7 Scan the generated QR code

Paste the URL

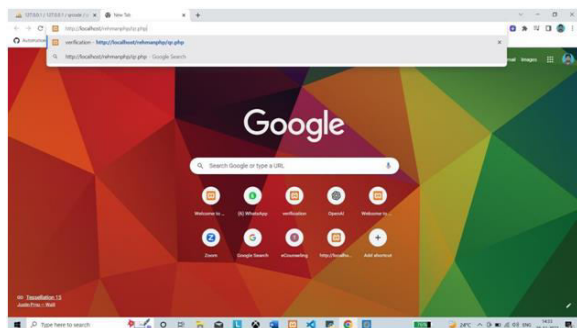


Fig 8 Paste the copied URL

Type in the number of a phone that you used to make the QR code. The phone number will now be checked against the database. The information about the person will be shown if it is in the database.

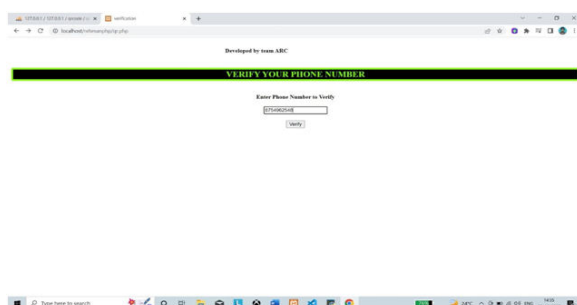


Fig 9 Enter the registered number

After the phone number is confirmed, the person information is shown.

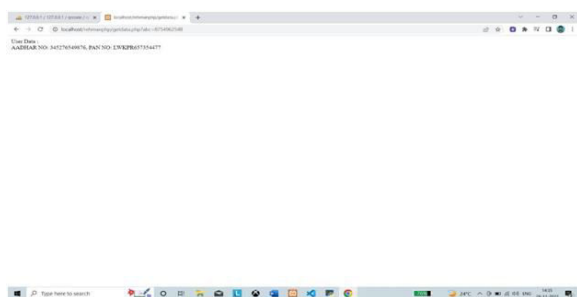


Fig 10 User details displayed

## 5. CONCLUSION

In conclusion, we were able to create and execute a Secure QR Code (SQRC) system that provides a strong way to share private and sensitive data safely. We make sure that only approved users can read and interpret the information saved in the QR codes by using security measures like encryption, identification, and limited user access. The SQRC method not only makes it easier to share personal information safely, but it also meets the urgent needs for privacy and data security in many real-life situations. When sharing private papers, proving identity, or making sure legal transactions are real, SQRCs are a reliable way to keep personal information safe from people who shouldn't have access to it or who want to change it. SQRCs are also very flexible, so they can be used in a lot of different businesses and situations. They are a quick and easy way to send private information safely. People and businesses can improve data security, lower the risk of identity theft, and protect the safety and security of private information by using SQRC technology. In general, the SQRC system is a big step toward building trust and faith in the ways that people share data while still keeping the highest standards of privacy and security.

## 6. FUTURE SCOPE

Encryption, digital signatures, interactive content, two-factor identification, and adaptable risk assessment could be added to QR codes in the future to make them safer. By adding these security features, QR codes can protect you better against being hacked, intercepted, or accessed without permission. As technology improves, QR codes' security features will probably change to keep up with new risks and user needs. This will make sure that they stay relevant and useful in many situations.

## REFERENCES

- [1] Dey S., Nath A., and Agarwal S., "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," International Conference on Communication Systems and Network Technologies, DOI 10.1109/CSNT.2013.112, 2013
- [2] Shetty M., "Hiding of Confidential Data and its Retrieval using Advanced Algorithms and QR Authentication system," IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e- ISSN: 2278- 1676, p-ISSN: 2320-3331, Volume 9, Issue 6 Ver. II, PP 01-05 www.iosrjournals.org, Nov – Dec. 2014
- [3] Gupta N., Mokashe N., and Parihar M., "QR code: A safe and secure method of authenticating legal documents," International Journal of Engineering Research and General Science Volume 3, Issue 1, ISSN 2091-2730, January-February, 2015
- [4] Bhavar S., Jadhav J., Kulkarni N., and Patil K., "Authenticate Message Hiding in QR code Using AES Algorithm," International Engineering Research Journal (IERJ) Volume 2 Issue 1 Page 367-369, ISSN 2395- 1621, 2016
- [5] "QR code Tutorial," <http://www.thonky.com/qr-code-tutorial/>
- [6] "ZXING- QR code Library," <http://code.google.com/p/zxing/>
- [7] "Encrypted QR Codes and Parts of a QR code," <http://www.qrcodestickers.org/qr-code-articles/encrypted-qr-codes.html>
- [8] [https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed\\_solomon\\_codes.html](https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html)
- [9] <http://www.qrcode.com/en>.
- [10] Zara Rizwan. Do People Use QR Codes in 2017? The Answer Will Definitely Surprise You. 2017. Available online: <https://scanova.io/blog/blog/2017/08/04/do-people-use-qr-codes/> (accessed on 16 April 2020).
- [11] Dabrowski, A.; Krombholz, K.; Ullrich, J.; Weippl, E. QR Inception: Barcode-in-Barcode Attacks. In Proceedings of the 4th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'14), Scottsdale, AZ, USA, 7 November 2014; pp. 3–10. [Google Scholar]
- [12] Cai, H.L.; Yan, B.; Chen, N.; Pan, J.S.; Yang, H.M. Beautified QR code with high storage capacity using sequential module modulation. *Multimed. Tools Appl.* 2019, 78, 22575–22599. [Google Scholar] [CrossRef]
- [13] Akta, C. The Evolution and Emergence of QR Codes, 1st ed.; Cambridge Scholars Publishing: Cambridge, UK, 2017. [Google Scholar]
- [14] Focardi, R.; Luccio, F.; Wahsheh, H. Security Threats and Solutions for Two Dimensional Barcodes: A Comparative Study. In *Computer and Network Security Essentials*; Kevin, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2018; pp. 207–219. [Google Scholar]
- [15] DroidLa. QR Droid Private. 2016. Available online: <http://qrdroid.com/> (accessed on 16 April 2020).

[16] Wahsheh, H.; Luccio, F. Evaluating Security, Privacy and Usability Features of QR Code Readers. In Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), Prague, Czech Republic, 23–25 February 2019; pp. 266–273. [Google Scholar]

[17] Reeder, R.W.; Felt, A.P.; Consolvo, S.; Malkin, N.; Thompson, C.; Egelman, S. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; p. 512. [Google Scholar]

[18] Focardi, R.; Luccio, F.; Wahsheh, H. Usable Security for QR Code. *J. Inf. Secur. Appl.* 2019, 48, 102396. [Google Scholar] [CrossRef]