

Generating and Protecting the QR Code of User Details and Allowing Access to Selected Users

¹Mrs M Srimathi, ²G Chandrashekar, ³Sk Rehman, ⁴T Akshaya

¹Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

srimathi.marella@gmail.com

²BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

gundlachandrashekar9@gmail.com

³BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

rehman.b2001@gmail.com

⁴BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

akshayathummanapally630@gmail.com

Abstract: Nowadays, it is almost impossible to secure and hide personal confidential information like system credentials, Ticket Passenger Name Record (PNR), Aadhar and PAN card details, etc. QR (Quick Response) codes are two-dimensional barcodes with the ability to encode different types of information. Because of their high information density and robustness, QR codes have gained popularity in various fields of application. Securing and hiding personal confidential information has become a challenge in these modern days. Due to the lack of security and confidentiality, forgery of confidential information can cause a big margin loss to a person. Personal confidential information needs to be securely shared and hidden with the expected recipient and he should be able to verify the information by checking its authenticity. QR codes are being used increasingly to share data for different purposes. In information communication, QR code is important because of its high data capacity. However, most existing QR code systems use insecure data format. Securing and hiding personal confidential information has become a challenge in these modern days. Due to the lack of security and confidentiality. Personal confidential information needs to be securely shared and hidden with the expected recipient and he should be able to verify the information by checking its authenticity. QR codes are being used increasingly to share data for different purpose. For better security we can allow QR code access to selected users only. So that non selected users cannot access to the QR code.

Keywords: Quick Response (QR) Code, Secure QR Code (SQRC), RSA, Encryption, Decryption, Verification, Validation.

I. INTRODUCTION

A QR code is a type of matrix bar code or two-dimensional code that can store data information and designed to be read by smartphones. QR stands for “Quick Response” indicating that the code contents should be decoded very quickly at high speed. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL or other data. The QR code was designed to allow its contents to be decoded at high speed. The popularity of QR codes is growing rapidly all around the world. Nowadays, mobile phones with built-in camera are widely used to recognize the QR Codes.

QR Codes are created by the Toyota subsidiary Denso Wave in 1994, and was initially used for tracking inventory in vehicle parts manufacturing. The idea behind the development of the QR code is the limitation of the barcode information capacity (can only hold 20 alphanumeric characters). While they are developed for tracking parts in vehicle manufacturing, QR codes now are used in many other fields, from commercial tracking to entertainment, in-store product labelling, and in those applications that are aimed at smartphone users. Users may open URL; receive text after scanning QR codes. By using QR code generating sites or apps,

users can generate and print their own QR codes for others to scan and use. The QR code system consists of a QR code encoder and decoder. The encoder is responsible for encoding data and generation of the QR Code, while the decoder decodes the data from the QR code.

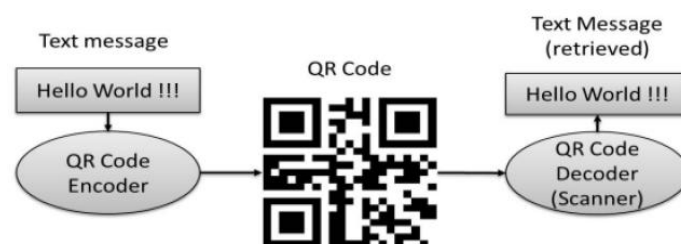


Fig.1 Working (overview) of QR Code

Figure 1 shows the overview of the QR code working. The plain text, URL, or other data are given to the QR code encoder, and it generates the required QR code and when we want to access the data of the QR code, QR code is decoded via QR Code decoder (scanner) which retrieves the data of QR code.

INFORMATION CAPACITY AND VERSIONS OF THE QR CODE

The symbol versions of the QR Code range from Version 1 to Version 40 [4]. Each version has a different module configuration or number of modules. (The module refers to the black and white dots that make up QR Code.) "Module configuration" refers to the number of modules contained in a symbol, commencing with Version 1 (21×21

modules) up to Version 40 (177 × 177 modules). Figure 2 shows the module configuration of the basic QR codes

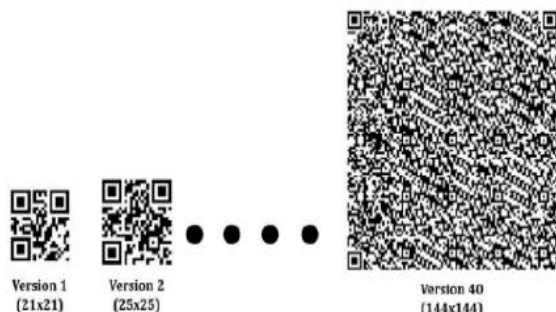


Fig.2 Version module configuration of the QR Codes

Each QR Code symbol version has the maximum data capacity, according to the amount of data, character type and error correction level. In other words, as the amount of data increases, more modules are required to comprise QR Code, resulting in larger QR Code symbols. Table 1 show the data capacity of version 40 for different type of data.

QR CODE ERROR CORRECTION

QR Code employs error correction to generate a series of error correction codewords which are added to the data codeword sequence which enable symbol to be read even if it is dirty or damaged. The QR code achieves powerful error-correction capability by using Reed-Solomon codes, a widely used mathematical error-correction method. Four levels of error correction are

available, higher level has high capability of recovery. Table 2 shows error-correction levels and their approximate ability of error correction. When selecting the level of error correction, environmental conditions as well as the desired size of the QR Code symbol need to be taken under consideration.

Table.1 Error Correction Levels and % of Correction

S No.	Error-Correction Level	Approximate Amount of Correction
1.	L	7%
2.	M	15%
3.	Q	25%
4.	H	30%

For example, Level Q (25% error correction) or H (30%) may be required for factories or other applications where the QR Code is likely to become dirty or damaged. For clean environments and codes containing a large amount of data, Level L (7%) may be selected. In general, Level M (15%) is most frequently used.

II. LITERATURE SURVEY

Quick Response code is usually authenticated with the help of the camera of one’s mobile phone. QR codes can

easily scanned through mediums like Tablets, laptops and personal computer desktops. The system automatically generates the ID of the user and its password. The characteristic which makes QR codes stand out is they can still be scanned even if they are partially damaged.

QR codes are a 2 dimensional printing code on a paper or a screen which makes it pretty vulnerable from various type of cyber-attacks. It can harm your device by unknowingly directing you to a virus contaminated page or website. To avoid this, one must verify the origin of a particular QR code and must have a full understanding of the data type of that particular QR code. There are many attacks involving QR codes as well as their solutions. QR codes are becoming quite popular nowadays because of the rapid increase in smart devices by the normal people around the world. Obviously, 2D QR code is way better and store huge amount of encoded information compared to the old traditional 1D codes. People are using smartphones to do authentications and for this the QR codes are the most ideal way to do it. Many types of QR codes are getting popular nowadays including logo QR code, encrypted QR code, iQR Code etc.

QR codes are becoming popular day by day in the upcoming generation as it offers

way easier authentication than the traditional old fashioned user id and password. QR codes offers many advantages such as greater storage capacity, fast readability, 360 degree reading, small print size, error correction, support for more languages and durability against soil and damage. Many firms who are relatively new in the online business are tend to use these codes instead of normal login process.

To fix the QR information / security issue, Xiaohe Cao proposed a safe QR code scheme based on visual cryptography. The security problem of QR code is severe, such as data loss and data tampering as the implementation of QR Code is wide enough. The QR code is spilt into two shared pictures which will be transmitted singly. The development of the two shared pictures is based on the pseudo-random matrix, i.e., the pixels are determined by the pseudo-random matrix values in the two shared pictures. The two images shared can only be stacked to revive the information. Simulation output demonstrates that the picture of the QR code can be masked well and can be efficiently reconditioned.

Peter Kieseberg has examined how both automated systems and human interaction can be attacked using QR Codes. As the encoded data is meant to be machine

readable only, one cannot differentiate between a legitimate and a harmful corrupted QR code. While automated readers are very much endangered to SQL injections and command injections, individuals might be prone to phishing attacks. Peter Kieseberg contribution is a survey of the QR code as an attack vector, demonstrating different attack plans for the attackers to read and explore their implications

There has been significant research on the topic of secure QR codes in recent years. Some key areas of focus in this research include QR code spoofing: This refers to the practice of creating fraudulent QR codes that look legitimate but lead users to malicious websites or perform unwanted actions. To prevent this, researchers have proposed various techniques such as using digital signatures, watermarking, and cryptographic hash functions to authenticate QR codes.

QR code vulnerabilities: Researchers have also identified various vulnerabilities in QR codes that can be exploited by attackers. For example, QR codes can be modified without being detected, and the data encoded in them can be accessed by unauthorized parties. To address these vulnerabilities, researchers have proposed various security measures such as

encrypting the data in QR codes and using secure communication protocols.

QR code privacy: The use of QR codes can also raise privacy concerns, as they can be used to track users and gather personal information. To address these concerns, researchers have proposed various techniques such as using anonymous QR codes and privacy-preserving QR code generation and scanning methods.

Overall, the research on secure QR codes is ongoing, and there is still much work to be done to ensure the security and privacy of QR code-based systems.

Two Level QR Code (2LQR)

Pallavi Tekade [1], Proposed 2LQR contains two security levels mainly called as public level and private level. This layered design provides privacy and security during personal message sharing and document authentication. Publicly showed information are stored in public level. The secret and private information are stored in the Private level. By using any standard QR scanner, only public information's will be shown. Here tried three different types of characterization patterns: mean patterns, median patterns for the private message sharing process and original patterns for the document authentication process. The mean and median characterization patterns will give

approximately the same results of pattern detection. The best pattern recognition results were obtained, while using original patterns as characterization patterns. During Standard QR Code generation by encoding public message there exists a pre-defined library Zxing which has to be imported for making Standard QR code scanning more easily. Reed Solomon's algorithm is used for generating Private QR Code. For 2LQR code creation 2 steps has to be performed. The first one is Pattern generation and second is Replacement of black modules with generated patterns of the Standard QR code. Here creates patterns for all the alphanumeric characters along with the special symbols and those patterns are stored in the database. Both QR Code generation and Cryptography algorithms are used.

Fast QR Code Detection

Xiang Zhang [2] ,Proposed The Two Algorithms Zbar and Zxing algorithm are open source bar codes and QR code detection algorithms. Zbar is an open-source software suit which helps to read bar codes from various sources, such as video streams, image files and raw intensity sensors. The layered implementation facilitates bar code scanning and decoding for any application. Zxing is an open source, multiformat 1D

or 2D barcode image processing library implemented in Java that contains ports that are connected to other languages. Zbar and Zxing methods achieve the high detection rate. A two-stage component-based detection concept has been proposed.

Web Tracking: Mechanisms, Implications Tomasz Bujlow [3], Defines for User Tracking Purpose Mainly five main groups of methods have been used, that are based on sessions, client storage, client cache, fingerprinting, and other approaches. A special focus is placed on mechanisms that use web caches, operational caches, and fingerprinting, as they are usually very rich in terms of using various creative methodologies. Identification of Users on the web and connecting with their real names, e-mail addresses, phone numbers, are detailed. Here shows why tracking is being used and its possible implications for each user. For each of the tracking methods, possible defences are also mentioned. Finally, detailing about the user tracking future trends and show that they can potentially Control significant threats to the users' privacy. The user is familiarized with different tracking mechanisms while browsing the web on a regular basis. He or she knows how to properly use simple means of protection as private browsing

mode or Ad Block like browser addons will decrease privacy threats.

Strength of QR Code

Lokesh S. et al.[4], Proposed a new system for image based authentication, where the image is represented as identification of authenticated user. Storing unique id or password into image which helps to restrict unauthorized user access. This proposed algorithm is help to remove the weakness of password authentication and bypass the risk generated from password authentication. Here algorithm takes input string as user name and it is directed to binary search algorithm for availability or unique user name. User enter password as tier1 identification. Using DES encryption technique Encrypting the password string and there by passing to Selective algorithm for generating QR code image. By applying Reed Solomon code or error correcting technique data can be recovered even if part of the printed symbol has been destroyed and Decoding process also explained in detail and security issue with QR code image has been examined.

III. PROPOSED WORK

Actually, SYNTHIMA doesn't store any user credentials in database or file while developing on android application. But In case of SYNTHIMA as web application

the User Information's, Hash values and secret key, copy of Contact list etc are stored in the database for maintaining the copy of data. This Paper Focus on Improving Security Feature of SYNTHIMA Database and also the Session Tracking of each user in Web application.

QR Codes

A QR ("Quick Response") code is a two-dimensional barcode invented by Denso Wave. Information is encoded in both the vertical and horizontal direction, main highlight is holding up to several hundred times more data than a traditional bar code Data is accessed by capturing a photograph of the code using a camera and processing the image with a QR reader.

Characteristics of QR CODES:

High capacity encoding of data

- Small printout size
- Kanji and kana capability
- Capacity of restoring and error correction.

The four layers of error correction of QR Code represented as L, M, Q and H in increasing order of capacity as follow.

1. Level L is approximately 7%
2. Level M is approximately 15%

3. Level Q is approximately 25%

4. Level H is approximately 30%

In relation with the layers of error correction, the capacity of Level L denotes the weakness one, the capacity of level H is the stronger one

- Readable from any direction in 360 degrees
- Structured appending Feature

DEVELOPMENT TOOLS USED

The development tools used include the following:

- **XAMPP**

XAMPP is a free, open-source cross-platform web server solution stack package developed by Apache Friends. It consists of Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages.

XAMPP is designed to be easy to install and to use. It is often used as a local development environment for testing and debugging web applications, as it provides all the necessary components in a single package.

Microsoft Visual Studio Code

Microsoft Visual Studio Code, also commonly referred to as VS Code, is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux, and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git.

We have used VS Code as Code Editor and Compiler. It offers built-in programs and functions for coding and debugging.

Python 3

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming.

Tkinter Framework

Tkinter is a Python binding to the Tk GUI toolkit. It is the standard Python interface to the Tk GUI toolkit and is Python's de facto standard GUI. Tkinter is included with standard Linux, Microsoft Windows and macOS installs of Python. The name Tkinter comes from Tk interface

- **MySQL Connector**

MySQL Connector is a Python driver that allows you to connect to a MySQL server and execute SQL queries using Python. It is a third-party library, not a part of the Python standard library.

To use MySQL Connector with Python, you will need to install it first. You can do this using pip, the Python package manager, by running the following command:

```
pip install mysql-connector-python
```

The Implementation steps for our proposed system are as follows

Step 1: Start the Apache and MySQL services in XAMPP Control Panel.

Step 2: Importing all the required Python libraries.

Step 3: Make two functions for Generating QR Code and Database Storage.

Step 4: Generate the QR Code GUI using Tkinter.

Step 5: Create a web page for taking the phone number.

Step 6: Program the PHP code for comparing the phone number with database.

Step 7: Run the python file and it will generate the GUI.

Step 8: Ask the user to enter user details and phone number and click on GenerateQR.

Step 9: The user details get stored in database and simultaneously QR code will be generated.

Step 10: Scan the QR and it will redirect to web page

Step 11: Enter the phone number

Step 12: If the entered phone number is matched with the phone number present in database, then it will display the user details else it will display error message

SYSTEM ARCHITECTURE

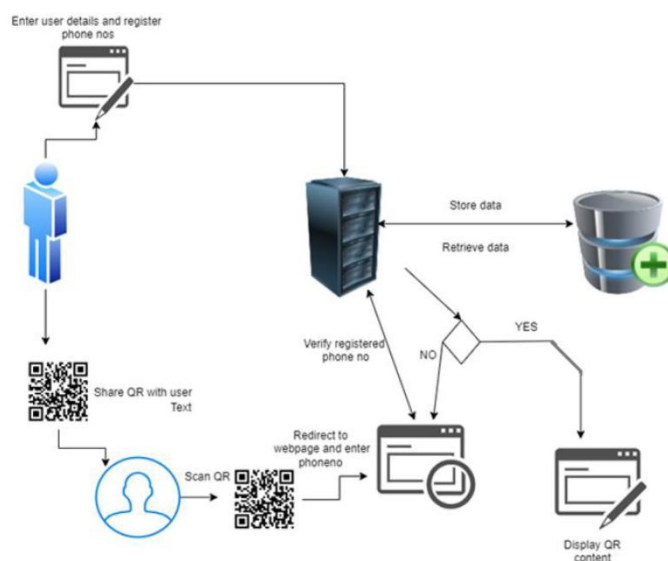


Fig.3 Proposed System Architecture

System architecture is a high-level structure of a system, which describes the relationships and interactions between the components of a system. It is a conceptual

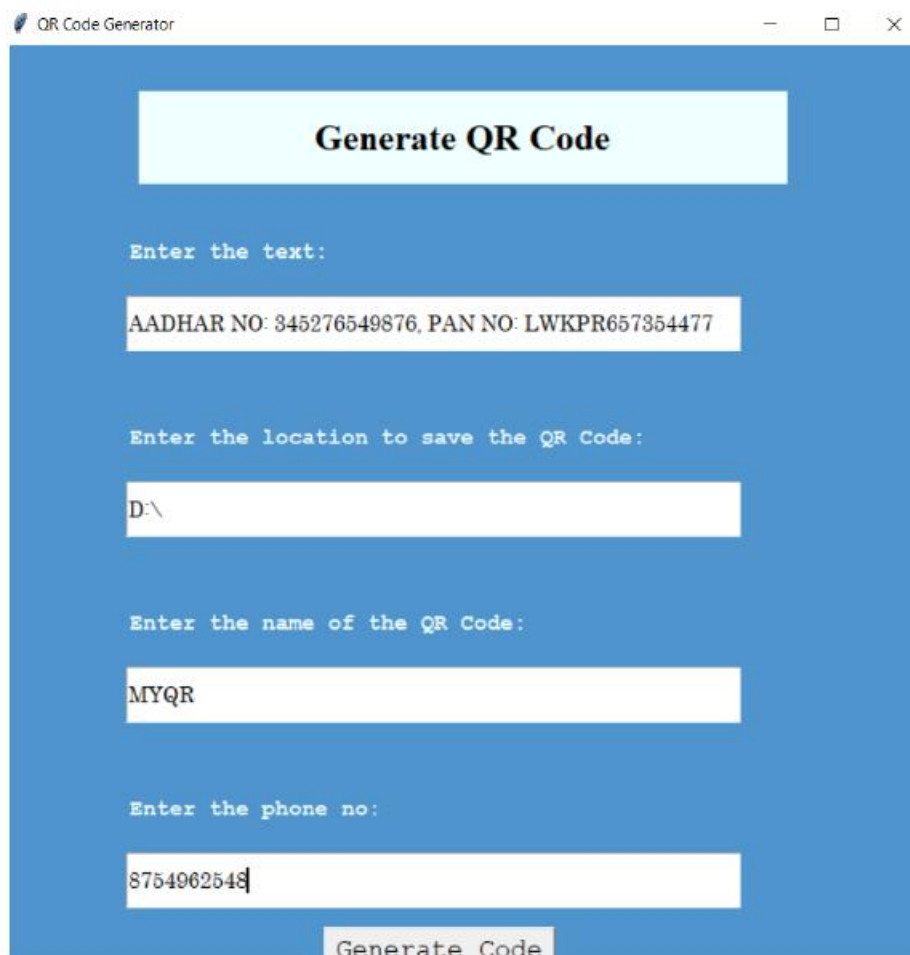
model that defines the structure, behaviour, and more views of a system.

In a project, the system architecture serves as a blueprint for the design and development of the system. It helps the project team to understand the overall structure of the system and how the

different components will work together to achieve the desired functionality.

Our idea is to implement that, the QR should be accessed only by specified people and specified people phone number should be given at the time of QR generation only. So that non specified people can't access the QR

IV. RESULTS



QR Code Generator

Generate QR Code

Enter the text:

AADHAR NO: 845276549876, PAN NO: LWKPR657354477

Enter the location to save the QR Code:

D:\

Enter the name of the QR Code:

MYQR

Enter the phone no:

8754962548

Generate Code

Fig.4 QR Code Generation GUI

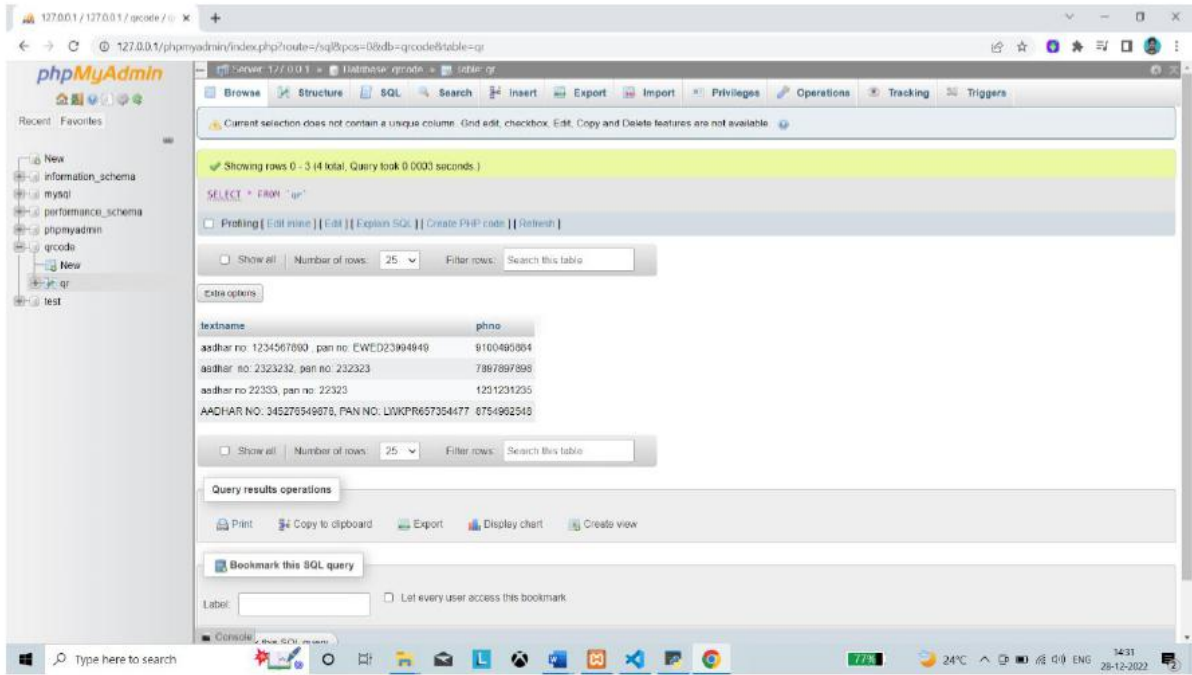


Fig.5 User Details stored in Database

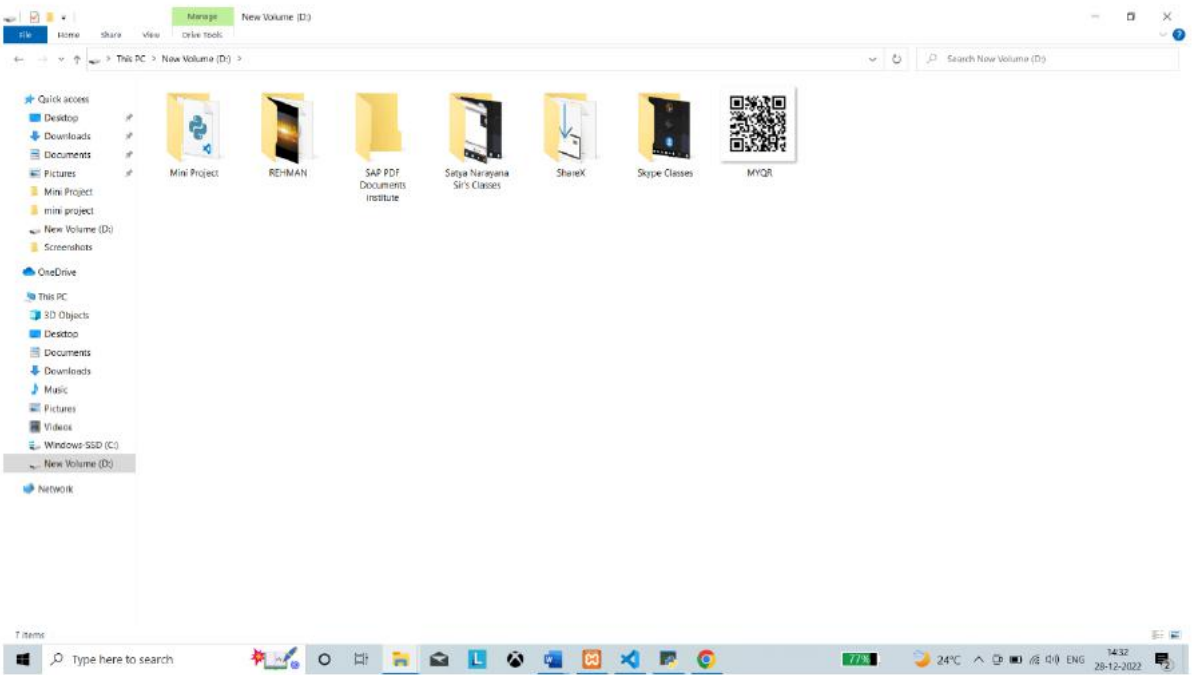


Fig.6 QR Code generated and stored in specified location

Scan the Generated QR Code

Scan the generated QR code and copy the URL

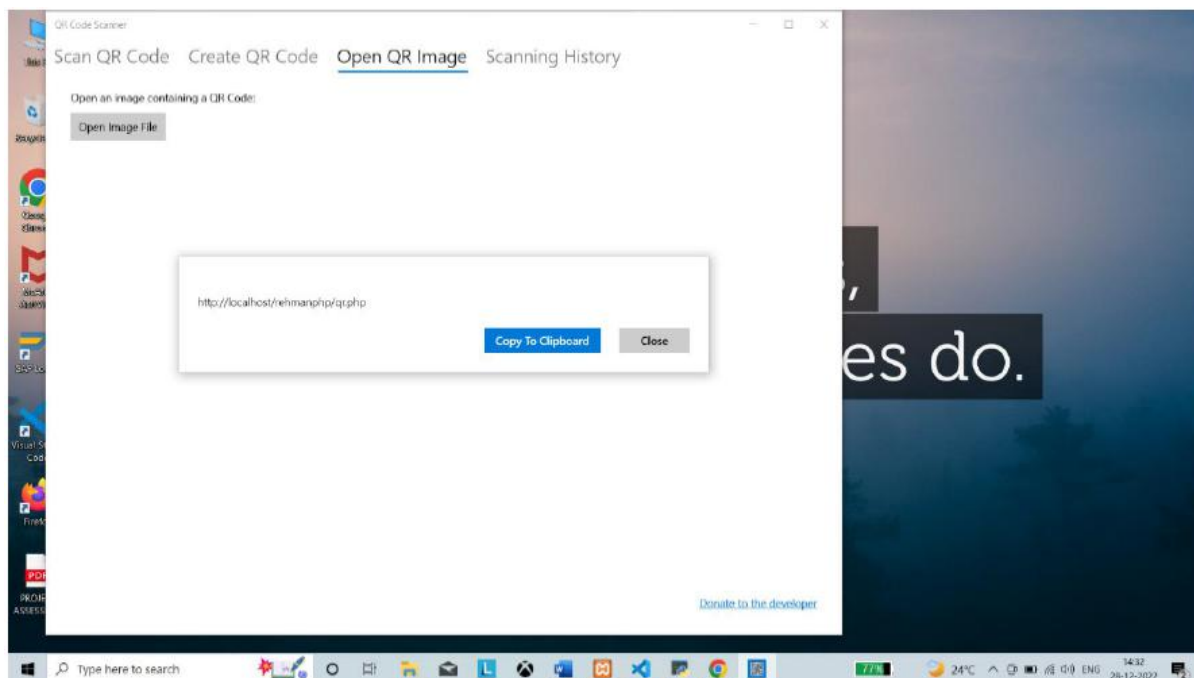


Fig.7 Scan the Generated QR Code

Paste the Copied URL

Paste the URL.

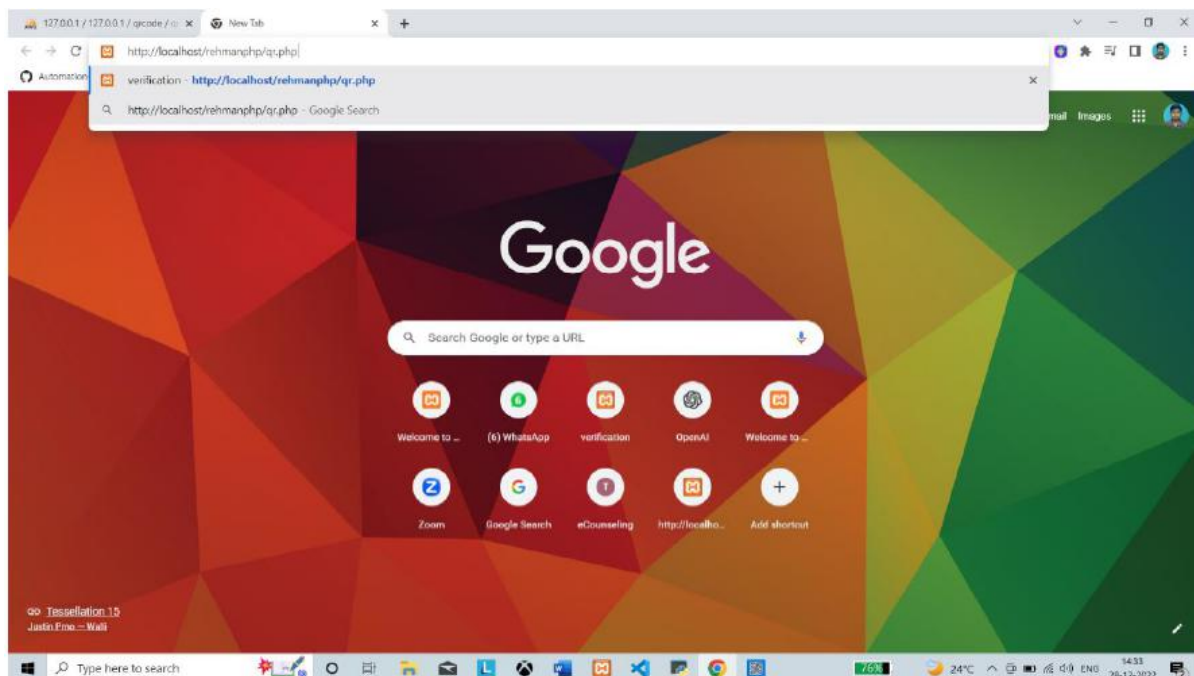


Fig.8 Paste the Copied URL

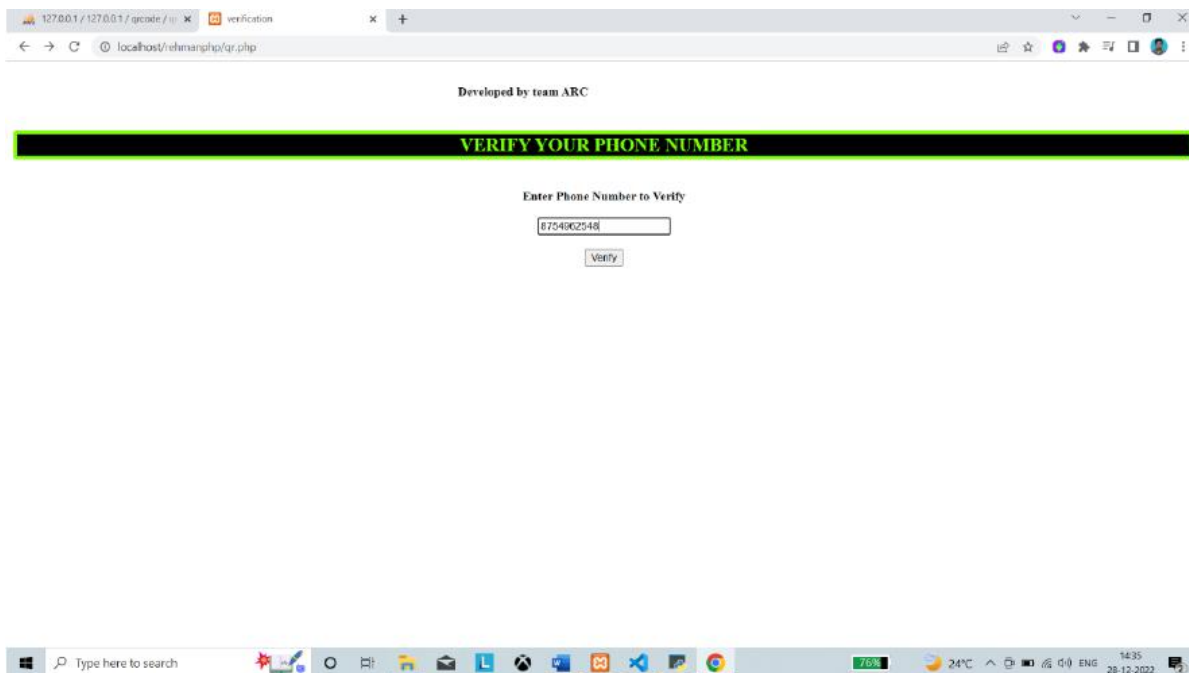


Fig.9 Enter the Registered Number

Enter the Registered Number

Enter the phone number which you have entered while generating the QR code. Now the phone number will be compared with the data base. If it is present in the database then the user details will be displayed

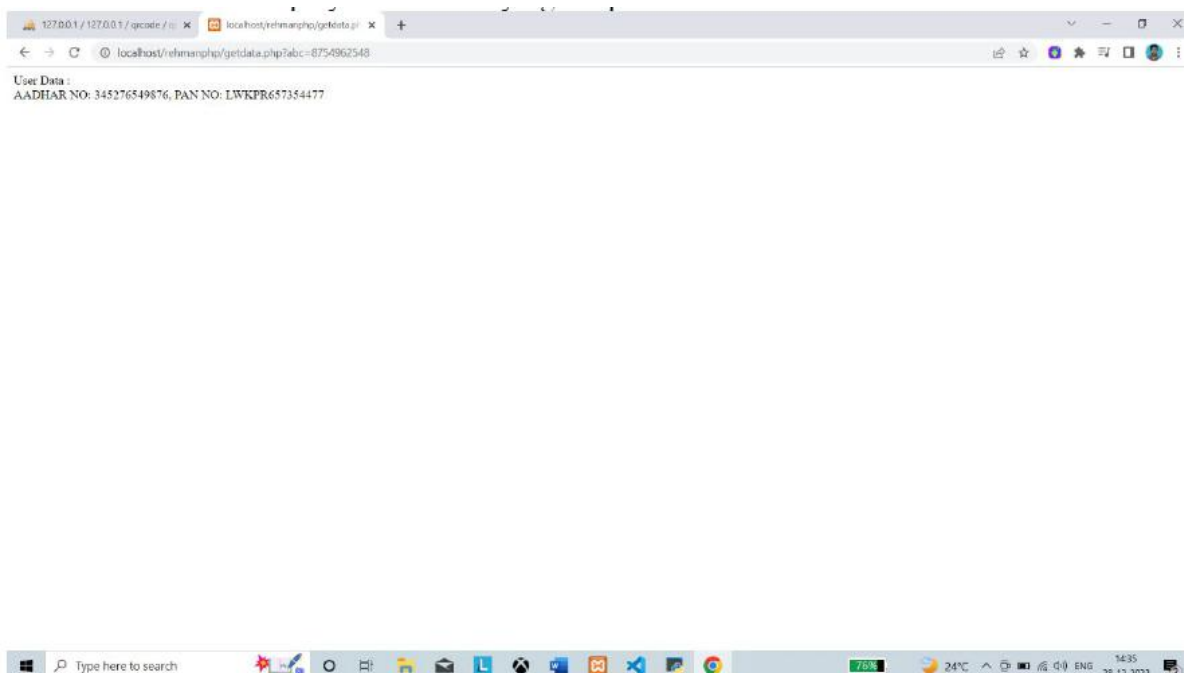


Fig.10 User Details Displayed

QR Code generated and stored in specified location

Simultaneously the QR code will be generated and saved in the user specified location

V. CONCLUSION

There are many QR codes in which everyone can access it. If user wants to share the QR with particular persons then it's not possible. So, we implemented the QR access only to the specified persons. We have illustrated that how we can easily generate the QR codes and can incorporate these QR codes to implement security and hiding user information into QR code. In these QR, we are storing and providing security for the details of user. In this project we have done the generation of the QR code by taking the user details and taking the phone number so that only registered phone number can access the QR.

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., "AuthenticateMessage 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/reesolomon/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] Prasadu Peddi (2019), "Data Pull out and facts unearthing in biological Databases", International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.