

Security Empowerment Using QR Code and Session Tracking For Cued Recall Based Textual Password Users

Megha Rajagopal¹

¹PG Scholar, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thiruvilamala, Kerala, India

Abstract - Now-a-days, web authentication becomes more vulnerable to attacks. During Login many of us forget to remember the password. To recall the password we have used Cued recall based textual passwords. By generating hints or cues based on Contact list details user can easily map that hints to passwords. For each registration user information and related password hash values are stored in the database. In this paper, proposed the concept to secure the database from attacks. Details of registered user information's which are stored in the database are extracted and converted to QR code. Also Introduced a Java based QR Code generator for making Contact, SMS, URL, TEXT, Phone number details to QR Code for better communication purpose through web and User Sessions are protected by using Session Tracking Technique.

Keywords: Authentication Cued Recall, QR Code, QR Code Generator, Session Tracking

1. INTRODUCTION

A password hint generation scheme which makes use of a user's contacts list, which constitutes an available and familiar information source to the user, to automatically generate an on-the-fly, easy-to-remember password hint that is learned upon the first login. To use this technique, a user has to mentally associate contact names from his/her contact list with the correct passwords. Hints will be instantly generated from the contact list, which helps to trigger the memory of the user to remember the password. During signup, user will enter the password, for that password, salt value will be generated then attached and shows to the user to enter for the first time. After entering the password with salt value, Hash code will be generated for the password with salt value, and hash code will get stored in the database. Salt value will be extracted and stores it in the System Drive. For login in to the application user has to enter the password without salt value. Salt value will be extracted from the System Drive and concatenate with the password, Hash code will be generated for the same. If stored hash code matches Login successful. Else Hash code mismatched, compare the matching word to the password in the contact list, and display the hints with respective to that. If user unable to remember the password, even after the hints, it will display invalid password. Hint generation is based on SYNTHIMA algorithm for reducing no of invalid login attempts and then thereby Improving memory recall. SYNTHIMA will maintain a copy of contact list. Password Salting Function and Cryptographic one way Hash function is the main concepts used in algorithm. Through Modulo Operation convert the resulting hash values to

smaller values that fit the contact list size. Contact list operations such as Insertion, Update, Deletion has to be performed, and there by working of algorithm related to Operations will generate hints.

2. PRIOR WORK

2.1 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.

2.2 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, multi-format 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.

2.3 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 users. For each of the tracking methods, possible defenses 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 decreases privacy threats.

2.4 Proxy Re-Encryption

K.Lakshmi [4] Proposed In barcodes, machine readable Information's are encoded ,a human can't differentiate whether it's a valid or a maliciously manipulated code. While humans might Undergo for phishing attacks, automated readers likely vulnerable to SQL injections and command injections. In this approach both encoding rate and interference level will be optimized with two robust error correction methods. Existing systems uses techniques like Steganography, DCT, DFT and Secret (N, N)-Threshold QR Code Sharing Approach. But in proposed system convolution coder is has been used for encoding the QR Code at the transmitted side and decode the same at the receiver side.

2.5 Strength of QR Code

Lokesh S.[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.

2.6 A Desktop Application of QR Code

Partiksha Mittra [6],Proposed technique Contains two modules QR code generator and QR code reader. the user will be able to generate a QR code using text and image. QR code base on text and the other one is QR code based image ,by entering the Image Location.User can encrypt the QR code by setting Password. Once the password is entered, the encrypted QR code will be generated accordingly. Once a QR code is generated, it will be displayed on the screen as well as saved as an image file at a specific destination folder/directory within the hard drive of the user PC. After the QR code is generated, the user will be able to scan it through the "Scan" option present in our field that will become visible below the generated QR code.

2.7 QR Code Steganography

Pei-Yu Lin [7],Proposed In this article, explored the characteristic of QR barcode and design a QR barcode steganography mechanism. The private information can be embedded into a cover QR tag with high secret payload. In case of a normal scanner, from the marked QR code a browser reveal the cover QR content. Only the authorized user/scanner can reveal the private secret information from the marked QR tag. Based on the Result, the new algorithm can convey a better secret payload in to a QR tag. This is efficient and feasible for private QR applications. To protect the confidential secret of QR tag and barcode reader directly decoded it.

2.8 Signing In Using Quick Response Codes

Kalpesh Adhatrao [8],Proposed the emerging threats to user privacy over the internet are increasing at an alarming rate. Signing in from an unreliable terminal into a web account may result in compromising private details of a user such as username and password, by means of keylogger software. A login method is used for signing in Using Quick Response (QR) codes via mobile authentication. Through this method, the user can securely sign-in into a web account by authenticating the user session on an terminal browser, with a mobile device. Also proposed a new login system, which strengthens the virtual privacy of a each user. The objective is to provide a reliable login technique for the user, operating based on an unreliable terminal, such as one in a cyber cafe.

By shoulder surfing, an attacker can retrieve only the characters that are entered via keyboard and the authentication system takes an asymmetric key technique, even if an unauthorized person gets access to the QR code and scans it to grant access to the mobile website and the public key, but the private key will be still safe at the user session on the terminal web browser operated by the user himself. Thus users of this system are safe from shoulder surfing attacks. As one can notice, this system is also secure from screen-capturing, mouse and eye tracking software.

3. METHODOLOGY

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.

3.1 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

3.2 Module Specification

- 1) Extracting Registered User Information from database and Conversion to QR Code
- 2) Development of Java based QR Generator.
- 3) Send QR Image as MMS or Email
- 4) User Session Tracking Technique Implemented

A) Extracting Registered User Information From Database and Conversion to QR Code

Mainly the database contains User Information's Includes email, phone no etc, Hash values and Security Keys of each registered user based on User Id data's are extracted from database and Convert in to QR Code and can be Stored in the system.

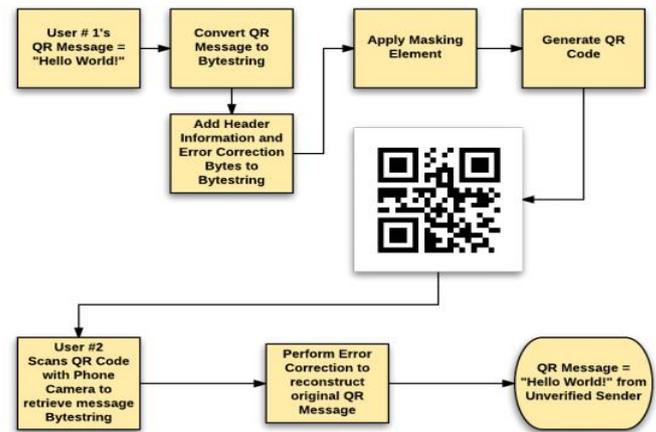


Fig -1: Generation and Scanning of QR Codes in Detail

Fig -1 gives a simplified description of the standard process of generating a QR code from a provided message and scanning the code with a smart phone or a comparable device. When provided a message string, the encoder converts the message into a byte string interleaved with general QR header information, error correction bytes, and a masking element. This modified byte string is then converted to a 2-dimensional matrix of 1's (white) and zeroes (black) which can be synthesized into an image. When this image is scanned by a phone camera, the byte string is retrieved and converted to the intended message, viewable by the person who initiated the scan.

B) Development of Java based QR Code Generator.

Developing a java based QR Code generator helps to make QR Code easily for secured data storing. QR Code Generator contains sections such as *Contacts, SMS, URL, Text, Phone number*

C) Send QR Image as MMS or Email

- Sending QR Images including user information has to be send over through web
- If there is any Updation in Contact list Allocated hints may vary. So notifying user through Msg or Email by encoded with QR Code
- New Vcard Can be generated for sending new contact information
- Alternately, new Vcard can be generate and store to database

D) Session Tracking Technique

Session Tracking Techniques helps to know about each user Session information's such as Username, User Id, Creation Time, Time of Last Access, No of Previous Session etc. Then by can assure that no unauthorized access has takes place. Session tracking helps a user to track a user's work status over multiple servlets or on HTML pages. A session is stated as a series of related browser requests that produces from

the same client within a certain period of time. Session tracking knots a series of browser requests that may have some meaning. HTTP is a “stateless” protocol: each time a client retrieves a Web page, the client access a separate connection to the Web server and the server does not automatically maintain major information about the client. A session is linked with a specified client. When the session is created on the server, it is associated with a personal ID. The browser must provide this session ID with its request in order for the server to find the session data again. The server tries to store this ID using: Cookies and Hidden Form Field.

3.4 System Architecture

Registered user will insert query to database which results in extracting user information including hash value and Security key of Synthima process and Converting to QR Code which helps to increase the security of database and user information. Java Swing application helps to retrieve data user wanted data in the form of QR code. For communication with users these generated QR Codes are used. While processing SYNTHIMA, the changes such as updation ,deletion of Contact list information or hint changes will be notified to users. Sessions of each Registered Users are tracked.

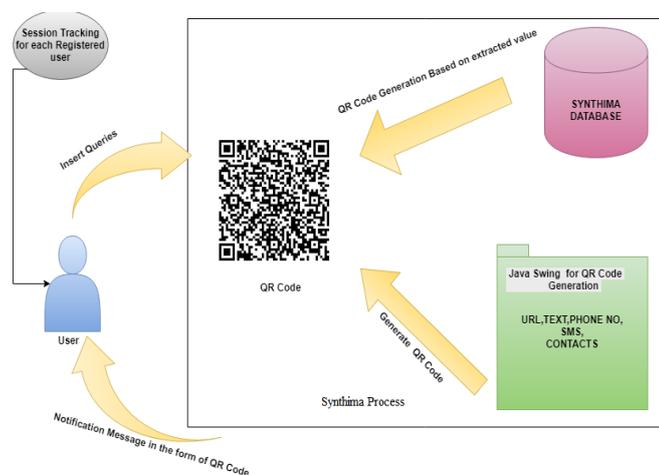


Fig -2: System Architecture

4. RESULTS AND DISCUSSION

Based on the computation of the Web application using Synthima technique, User information on database are not secured. Therefore by implementing QR Code the security features are increased ,Only Registered users can access the the data embedded QR Codes and get notification based on Synthima Process Operations like Updation, Deletion of User Information.Communication process through QR Code Provide much more Security than before. Tracking user Sessions is also added in order to monitor the usage time of each Authorized User and there by reduce attack chance According to the evaluation of the process of web application

Table-1 shows the performance and attack rate without QR code enhancement, whereas Table-2 shows the attack and performance rate with the inclusion of QR code. Finally observed that there is slight variance in the rates with better performance.

Table -1: SYNTHIMA DATABASE WITHOUT QR CODE

Property	Total No. of Attempts	No. of Attempts Succeeded	Result (in%)
Chance of Attacks	40	28	70%
No of Data Retrieval	40	22	55%

Table -2: SYNTHIMA DATABASE WITH QR CODE

Property	Total No. of Attempts	No. of Attempts Succeeded	Result (in%)
Chance of Attacks	40	15	37.5%
No of Data Retrieval	40	10	25%

5. CONCLUSION

In this Paper, Proposed the Concept of Securing Synthima Database by extracting the user information and convert in to QR code. Then developed Java based QR Code generator for Creating QR code of Contact ,SMS,URL,TEXT ,Phone number for better communication purpose through web and User Sessions are protected by using Session Tracking Technique

REFERENCES

- [1] Pallavi Tekade1, Anub Vamadevan, “Implementation of Two Level QR Code (2LQR),” International Journal of Advanced Research in Computer and Communication Engineering, ISO 3297:2007 Certified, Vol. 6, Issue 4, April 2017
- [2] Xiang Zhang, Hangzai Luo, “Fast QR Code Detection,” 978-1-5386-3148-5/17/\$31.00 © 2017 IEEE
- [3] Tomasz Bujlow, Valentín ,” A Survey on Web Tracking: Mechanisms, Implications, and Defenses”, Proceedings of the IEEE (Volume: 105, Issue: 8, Aug.2017)
- [4] K.Lakshmi, D.Jeyamanilatha, “QR Code Security Using Proxy Re-Encryption for Private Data Shared Barcodes,” International Journal of Electronics & Communication Technology, IJECT Vol. 8, Issue 1, Jan - March 2017

- [5] Lokesh S. Khedekar Prajakta S. Kale," Strength of QR Code over Design and Implementation of Authentication System", International Conference on Communication and Signal Processing, April 6-8, 2016, India 978-1-5090-0396-9/16/\$31.00 ©2016 IEEE
- [6] Partiksha Mitra, Nitin Rakesh,"A Desktop Application of QR Code for Data Security and Authentication", Inventive Computation Technologies (ICICT), International Conference on,DOI: 10.1109/INVENTIVE.2016.7824809
- [7] Pei-Yu Lin and Yi-Hui Chen, "QR code steganography with secret payload enhancement", Multimedia & Expo Workshops (ICMEW), 2016 IEEE International Conference on, DOI: 10.1109/ICMEW.2016.7574744
- [8] Kalpesh Adhatrao, Aditya Gaykar," A Secure Method For Signing In Using Quick Response Codes With Mobile Authentication", International Journal of Student Research in Technology & Management, Vol 1(1) pg 01-11