Password Security using QR Code

Prof. Ware V. S[1] Swapnali Tippanna Potenavaru[2] Arpita H Galiyal[3] Madhuri S Dhotri[4]
[1]Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]BMIT Solapur, 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: QR Code, CGI, SYNTHIMA Algorithm

I. 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 generates 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.

II. LITERATURE REVIEW

To generate QR code different methods implemented in various applications. SomdipDey etal. Proposed a system which is based on the various methods of encryption. One of the method is encrypted message is treated as a large string and the reverse of the string is generated. This will generate new encrypted message and that is converted into QR Code. LászlóVárallyai et al. presented a paper in which they have given information about QR code storage. The amount of data that can be stored in the QR Code symbol depends on the data type, version and error correction level. Donny Jacob Ohana et al. presented a paper in which they have given information about QR code encoding and decoding. QR codes can be generated using Google API (Google Chart Application Programming Interface). Several common ways to decode QR code symbols are to upload the symbol to a website, scan the symbol with a camera equipped cell phone. M.G.Harish et al. presented an android application for validation of tickets through QR code. Ticket checkers scans the QR code of user, before the user enters or leaves the station. This app automatically detect the passenger's fare according to the distance travelled as well as detects the passenger's identification.

S Ambareesh et al. presented QR-Maps tool that can be used in smartphones to obtain accurate indoor user locations. A user that arrives at an indoor location and wishes to know where he/she is just needs to locate a QR-Code and decode it with the QR-Maps application in the smartphone. NehaYadav et al. implemented a cashless campus using QR code technology. The system is used to make all the transactions inside the campus without cash. The user has to scan the QR code to proceed to payment. If the QR code is valid, purchase amount will be debited from their account. Sankara Narayanan et al. presented the security solutions for QR code. The attack method used in the QR code was that when a user scans the code he is directed towards a website and then a malicious file downloads in the user's device without the knowledge of the user.

Ji-Hong Chenetal. Presented the QR code into two parts, visible and invisible, and then embedded them into cover images. The visible part can directly provide users with related information and the invisible watermark can protect copyright information. Kinjal H. Pandya1et al. presented the different areas in which researchers have experimented with QR codes. Some of these are improving data capacity: color barcodes, use of multiplexing to increase information and scratch removal technique. JiQianyu et.al presented a book which is based on exploring the concept of QR code and benefits of QR code for companies in which there are different topics related to QR code. That are QR methodologies, types of QR codes, QR characteristics, new technologies and its solutions. Devinder Kumar et.al presented a paper which is based on emerging threat to mobile security and protective system. In this paper, they specified that if there is increase in usage of QR code then the threat posed by them to mobile security is also increasing. also this paper presents different kinds of possible attacks that QR code user can be subjected to their future trends.IrannaShettaret.al presented a paper which is a Quick

Response (QR) Codes in Libraries: Case study on the use of QR codes in the Central Library, NITK. In this paper, they given information about QR code,how QR code works and QR code functions. also it includes features of QR codes , how to generate QR codes and QR codes in modern libraries.PhaisarnSutheebanjardet.al presented a paper which is based on QR code generator. QR code is a way of encoding more information than a traditional bar code. In this paper, they show how to create the QR codes via the web browser that facilitates users to easily create their own QR codes for websites, emails, business cards, print ads and so on.

III. SYSTEM ARCHITECTURE

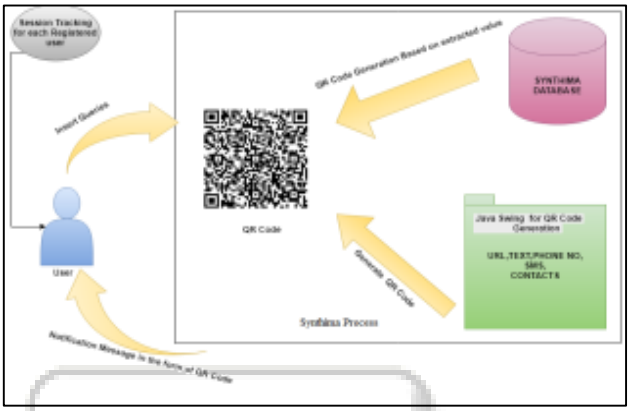

Fig. 1: System Architecture

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.

IV. WORK CARRIED OUT

A. For Software Project:

1) Acquiring Domain Knowledge:

A domain name is your website name. A domain name is the address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Computers use IP addresses, which are a series of number. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses.

A domain name can be any combination of letters and numbers, and it can be used in combination of the various domain name extensions, such as .com, .net and more. The domain name must be registered before you can use it. Every domain name is unique. No two websites can have the same domain name. If someone type in it will go to your website and no one else's.

V. DECIDING THE ALGORITHM

A. MD5():

The md5() function calculates the MD5 hash of a string. The md5() function provides Data Security. The MD5 Message-Digest Algorithm: The MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem.

Syntax-md5(string)

String: Required. The string to be calculated.

VI. PROGRAMMING LANGUAGE

A. PHP:

PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP reference implementation is now produced by The PHP Group. While PHP originally stood for Personal Home Page, it now stands for the recursive backronym PHP: Hypertext Preprocessor.

PHP code may be embedded into HTML code, or it can be used in combination with various Web template systems and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.

Standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

VII. SERVER: XAMPP

XAMP is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing purposes. Everything needed to set up a web server – server application (Apache), database (MariaDB), and scripting language (PHP) – is included in an extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server extremely easy as well.

VIII. DATABASE: MYSQL

MySQL is an open-source relational database management system (RDBMS), in July 2013, it was the world's second most widely used RDBMS, and the most widely used open-source client–server model RDBMS. It is named after co-founder Michael Widenius's daughter, My. The SQL acronym stands for Structured Query Language. The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation. For proprietary use, several paid editions are available, and offer additional functionality.

MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other "AMP" stacks). LAMP is an acronym for "Linux, Apache, MySQL, Perl/PHP/Python." Free-software-open source projects that require a full-featured database management system often use MySQL. Applications that use the MySQL database include: TYPO3, MODx, Joomla, WordPress, phpBB, MyBB, Drupal and other software. MySQL is also used in many high-profile, large-scale websites, including Google (though not for searches), Facebook, Twitter, Flickr, and YouTube.

IX. WEB BROWSER: GOOGLE CHROME

Google Chrome is a freeware web browser developed by Google. It used the WebKit layout engine until version 27 and with the exception of its iOS releases, from version 28 and beyond uses the WebKit fork Blink. It was first released as a beta version for Microsoft Windows on September 2, 2008, and as a stable public release on December 11, 2008. As of December 2015, StatCounter estimates that Google Chrome has a 58% worldwide usage share of web browsers as a desktop browser. It is also the most popular browser for smartphones, and combined across all platforms at about 45%. Its success has led to Google expanding the 'Chrome' brand name on various other products such as the Chromecast. Google releases the majority of Chrome's source code as an open-source project Chromium

X. CODING

For our Project we are done the coding in PHP Languge. PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. PHP code may be embedded into HTML code, or it can be used in combination with various Web template systems and web frameworks.

PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable.

And also we used the java scripting language for getting the online appointment scheduling. JavaScript is a "Client Side" programming language. This means JavaScript are read, interpreted and executed in the client which is our web browser.

A. The QR code generated has following standard structure

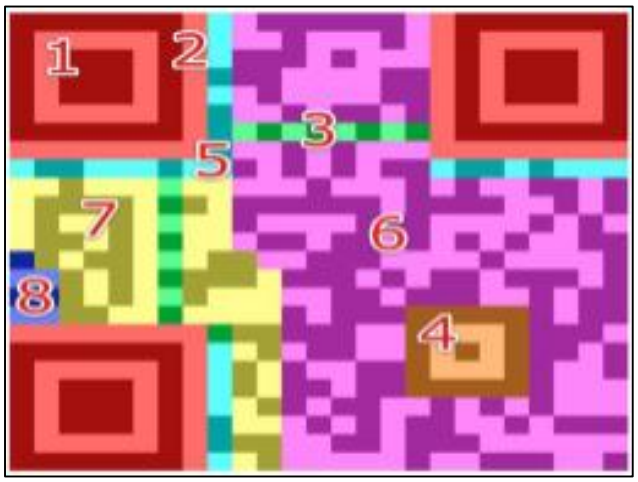

Fig. 2: Structure of QR Code [2]

1) Finder Pattern: The three identical structures that are located in the upper corners and in the bottom left corner enable the decoder software to recognize. The QR code and determine the correct orientation. These patterns also allow 360 degree high-speed reading of the code. These structures consist of a 3 X 3 black square surrounded by white modules that are again surrounded by black modules.
2) Separators: The white separators that surround the Finder Patterns have width of one pixel and make it easier to distinguish the patterns.
3) Timing pattern: A sequence of black and white modules that help the decoder software to determine the width of a single module.
4) Alignment Pattern: This pattern allows the QR reader to correct for distortion when the code is bent or curved. The alignment pattern appears on version 2 and higher and the number of alignment patterns used depends on the version selected from the encoding.
5) Format Information: This section consists of 15 bits and contains the error correction rate and the selected mask pattern of the QR code.
6) Data: After the data is converted into ReedSolomon-encoded data bits, it is stored in 8 bit parts in the data section.
7) Error Correction: The data codeword's are used in order to generate the error correction (EC) codeword's, which are stored in the error correction section.
8) Remainder Bits: This section contains empty bits if the data or the error correction bits cannot be divided into 8 bit code words without a remainder.[2]

XI. TRIALS AND TESTING

Software testing is a process of executing a program or application with the intent of finding the software bugs. It can also be stated as the process of validating and verifying that a software program or application or product: Meets the business and technical requirements that guided it's design and development. The purpose of software testing is to access or evaluate the capabilities or attributes of a software program's ability to adequately meet the applicable standards and application need. Testing does not ensure quality and the

purpose of testing is not to find bugs. Testing can be verification and validation or reliability estimation. The primary objective if testing includes:

- To identifying defects in the application.
- The most important role of testing is simply to provide information.
- To check the proper working of the application while inserting updating and deleting the entry of the products.

XII. REGISTRATION FORM VALIDATION

These pages will show how to process PHP forms with security in mind. Proper validation of form data is important to protect you from hackers and spammers!

In our registration form anyone can do the fake registration it's not possible because we check the QR code is fake or real through the OTP no after entering the OTP no. user registration successfully done.

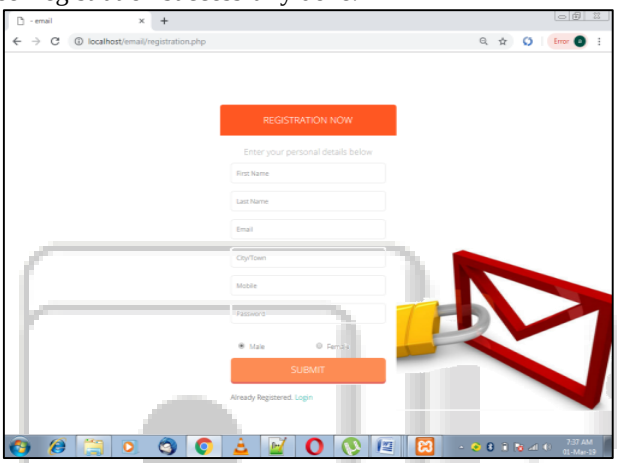

Fig. 3: Registration Form

User Login validation: In login form we providing user EmailID and password as a QRCode image for secure authentication.

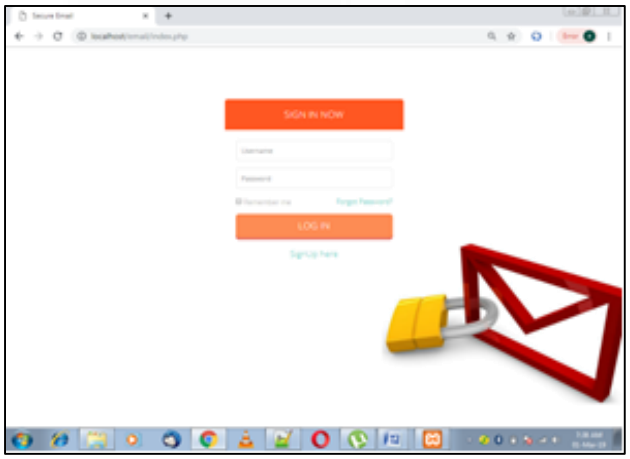

Fig. 4: Login Form

XIII. OUTPUT

A. *Snapshots of Project output*

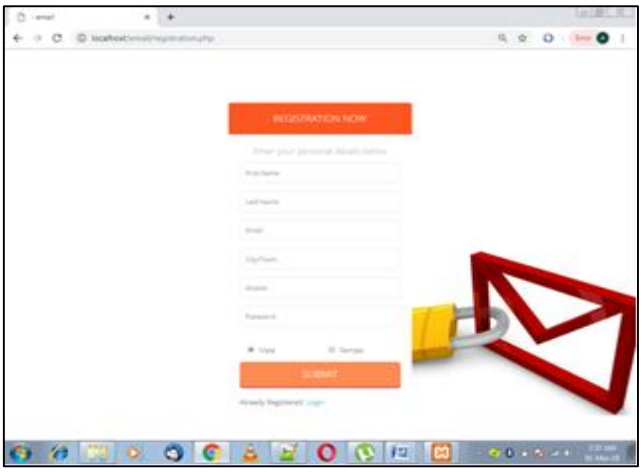

Fig. 5: Registration form

Fig. 6: Login Form

XIV. RESULTS AND DISCUSSIONS

In this paper, QR codes are analyzed from the perspective of their significance and uses. The working of QR code is discussed to make reader familiar with the QR codes. QR code can store complex information within a small code. As awareness increases about the usefulness of these codes, we can expect them to be used in more public domains.

XV. CONCLUSION

In this Paper, Proposed the Concept of Securing Synthima Database by extracting the user information and convert into QR code. Then developed QR Code generator for Creating QR code of Contact Email, TEXT, image for better communication purpose through web and User Sessions are protected by using Session Tracking Technique.

ACKNOWLEDGEMENT

We would like to thank our guide Prof.Ware V.S. Assistant Professor at Dept. of CSE, BMIT Solapur, for his guidance and support. We also thankful to our project co-coordinator Prof. Dodmise U.S for her valuable support. We will forever remain grateful for the constant support and guidance

extended by guide as well as project coordinator, for the completion of paper

REFERENCES

[1] Real User Corporation: Passfaces, [online] Available: www.passfaces.com.
Show Context Google Scholar
[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, Rubin, "The design and analysis of graphical passwords", Proceedings of USE NIX Security Symposium, August 1999.
Show Context Google Scholar
[3] Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing".
Show Context Google Scholar
[4] PallaviTekade1, AnubVamadevan,"Implementation of Two Level QR Code(2LQR),"International Journal of Advanced Research in Computer and Communication Engineering, ISO 3297:2007 Certified, Vol.6, Issue4, April2017
[5] XiangZhang,HangzaiLuo,"FastQRCodeDetection,"978-1-5386-3148-5/17/$31.00©2017IEEE
[6] TomaszBujlow,ValentÍn,"A Survey on Web Tracking: Mechanisms, Implications, and Defenses", Proceedings of the IEEE(Volume:105,Issue:8,Aug.2017)

