Online Session Security System using QR code, OTP and IMEI

Chirag Patil\(^1\), Umesh Naik\(^2\) & Pallavi Vartak\(^3\)

\(^1\)Student, VIVA institute of technology (India)
\(^2\)Student, VIVA institute of technology (India)
\(^3\)Assistant professor, Department of Computer Science & Engineering VIVA institute of technology (India)

Abstract: This work contributes in the usage of a creative secure authentication strategy which uses a QR code; an open source confirmation of-idea verification framework that uses a two-figure authentication by joining a secret key and a camera-prepared cell phone, going about as a confirmation token. Advanced cell is utilized for decoding the QR code. The code is scan with the QR code scanner of cell phone. Examining result produce one string which is the mix of IMEI number of a telephone which is enlist by the client and the arbitrary number, where irregular number is created by the arbitrary number capacity. In a present day world where we can do practically everything on-line (saving money, shopping, imparting, putting away and sharing individual information...), it is these days a basic matter to have the capacity to get to these administrations in the most secured way.

Without a doubt, as infections and splitting strategies turn out to be more mind boggling and capable by the day, the accessible security methods must enhance too, permitting clients to ensure their information and correspondences with the most extreme certainty. The point is to build up a validation strategy utilizing a two variable confirmation: a trusted gadget (a cell phone) that will read a QR code and that will go about as a token, and a secret key known by the client.

Keywords: IMEI, QR code.

1. Introduction

Presently a day's every one of the things we can do on the web (like keeping money, shopping, imparting) and in this the test is that while doing this things online our data is not get harmed. In reality, as the strategy for figuring out the security code get more unpredictable and effective. There is have to grow all the more capable security application. These capable applications permit client to deal with untrusted PCs certainly. The purpose is for the plan and usage of an imaginative secure validation technique which uses a QR code: an open source evidence of-idea verification framework that uses a two-consider confirmation by consolidating a secret key and a camera-prepared cell phone, going about as a confirmation token. The purpose is for the outline and usage of an imaginative secure validation strategy which uses a QR code; an open source verification of-idea confirmation framework that uses a two-calculate confirmation by consolidating a secret word and a camera-prepared cell phone, going about as a confirmation token. The secret key framework gave security against unapproved get to however the development of various assaults like beast drive word reference assault has made this framework inadequate. An option of this framework is given in type of a two variable confirmation which utilizes watchword as the first component and an arbitrarily produced code as the second element.

With preferences of this framework additionally came the disservices for instance satirizing of system, delay in conveyance of the OTP , this framework was supplanted by a more productive framework which utilized a QR code rather than OTP yet didn't tackle the issue identified with conveyance of the code or QR. The new framework we offer produces QR code which comprise of the IMEI number and a 4 digit code. The second component of verification is supplanted by and android application introduced on the enrolled telephone. This framework takes care of the issue of system caricaturing, man in the center and the postponement in getting the one of a kind code.

2. Related Work

In this proposed system, an authentication method using a two-factor authentication: a trusted device (a mobile phone) that will read a QR code and that will act as a token, and a password known by the user. It was proposed that for security, a self-signed SSL certificate would be generated to encrypt all communications, using https and therefore, ensuring that all data sent and received between client and server passes through a secure channel [1].

In this proposed system online banking authentication system they eliminated threat of phishing and to confirm user identity, QR-code which would be scanned by user mobile device can...
be used and weakness of traditional password based system can be improved by one time password (OTP) which can be calculated by user transaction information. The proposed authentication system ensures the user authentication and digital signatures using authorized certificates by using https communication between user and server [3].

It explores a solution to create a cashless mobile payment system. The aim is to provide the most cost efficient and secure alternative to current systems. Current systems use SMS and USSD to process payments. These are not cost effective methods of communication. There is also no current method of processing credit payment on a mobile phone without the need for a specialized piece of hardware [6].

Currently exam conduction is predominantly paper based. This paper provides idea about generating QR code containing (MCQ) questions which can be viewed by students. The QR code can be decoded by the students on their mobile handset, after which the questions can appear on their mobile screen. After answering the questions in a stipulated time period, answers can be sent to the server. The result is calculated on the server and displayed [8].

3. General Description

![Figure 1. QR Code](image)

Fig. 1 shows the diagram of QR code. The QR code is a matrix consisting of an array of nominally square modules arranged in an overall square pattern, including a unique pattern located at three corners of the symbol and intended to assist in easy location of its position, size and inclination. There are two areas in this framework. In the encoding area change of information to a QR Code image happens. In this the information examination and encoding is done then after Error amendment coding the last message is structures. Taking after the Module situations in lattice with veiling another segment is the Decode area. This area contains translating of the info QR Code picture and shows the information contain that QR code. The disentangling methodology begins with the redesign of highly contrasting module then Decode organize data. Taking after the assurance of rendition of QR code and discharging Masking. At that point reestablishing of information and RS code word takes after the Error discovery and after that interpret the Data codeword.

![Figure 2. Sequence Diagram Of Proposed System](image)

Fig. 2. demonstrates the arrangement chart of the proposed system. First the client logs into the website. The login points of interest are registered with the database. If the login is successful, the client sends the demand for QR code era to the database. Accordingly the database sends the QR code on the customer's machine. The client then outputs the QR code utilizing his mobile (IMEI). This data is sent to the database. If the IMEI looking at flops, then he is not permitted to get to. Else he can get to the web based managing an account framework.

4. Proposed System

![Figure 3: Online Authentication Mode](image)

Figure 3 demonstrates the online method of validation of the proposed framework. As appeared,
in this First IMEI number and arbitrary number are scrambled utilizing the general population key. This encoded string produces the QR code utilizing the QR code era work which is available in java. Presently this QR code picture is shown on the customer machine. Client examines this QR code utilizing cell phone. Subsequent to examining, in online mode implies net is accessible on telephone the created string (IMEI number and arbitrary number) is naturally get gone into the login page. After effective login the landing page of the bank opens.

Figure 4.Architecture Diagram

The ATM design outline is appeared with Fig. 4 In this module the extra security to the client has been given as far as QR code verification. Here the customer goes into ATM focus to exchange the cash starting with one ATM card then onto the next ATM card for which he needs to enter his own PIN number to verify himself. A short time later ATM machine checks his PIN with the database; if the PIN coordinates then he is given validation. After confirmation he continues towards cash exchange alternative. For exchanging cash starting with one ATM card then onto the next ATM card, he needs to enter his own particular ATM number then the add up to be exchanged and finally he needs to enter the ATM number of the other individual. Subsequent to entering the second record number the fly up message is appeared to affirm the exchange by physically affirming the given data of the other individual. In this framework additional measures have been given to forestall senseless errors. The security is as QR code confirmation. The QR code will be shown promptly in the wake of hitting the following catch at the exchange level. By filtering that QR code we will get the beneficiary's data on the screen of our cell phone. After the confirmation of the data on our cell phone the exchange will be prepared else declined.

5. Implementation

The proposed framework will work precisely as required by the client, if framework will keep running on the equipment and programming prerequisites as specified some time recently. The proposed web-based interface will be simple for comprehension to a wide range of clients i.e. client can be another client or general clients. The entrance will be outlined in a manner that moderate speed will be maintained a strategic distance from.

Fig. 5. demonstrates the login page for customer. The customer is said to login with the username and secret word i.e. OTP at first time login. The normal aftereffects of our proposed framework are:

1). The customer will login with the username and secret word i.e. OTP at first time login. The customer will do the confirmation procedure and once the check procedure is done the customer will change the secret word. The customer when re logsins the framework with the username and new secret key created, it sends demand to produce QR code.
2). Once the demand is sent to the server, QR code will be created. It will be shown on the customer's screen. The customer will check the QR code with the versatile, with the assistance of [Random no + IMEI no] which will be put away in the framework database.
3). Then the customer will do the exchange procedure by entering the points of interest and sum.

For ATM framework:
1). In the login page, the customer will enter the record no. what's more, the secret key for the procedure of the withdrawal of cash.
2). After validation, the customer will choose the cash exchange choice. For exchanging cash starting with one ATM card then onto the next ATM card, the customer will enter his/her own particular ATM number, then the sum will be exchanged, in the wake of entering the ATM number of the other individual.

6. Conclusion

Consequently the proposed framework gives extra security the conventional method for online
validation of keeping money; which incorporates username and secret word. Nonetheless, by including QR code validation the safety efforts for saving money are improved. Two calculate validations are viewed as this framework. With the assistance of this QR code security is expanded amid the login of the specific bank. Contingent upon the confirmation just the customer will have the capacity to play out the exchange. Presently a days, utilization of web based keeping money application are expanded. Security is an imperative issue for taking care of such administrations. we propose web based keeping money confirmation framework utilizing QR-code and OTP. The bank creates the QR-code utilizing client input exchange data and after that client need to perceive as to peruse the code utilizing their cell phone, after produce the OTP code utilizing exchange data and the hashed client’s cell phone number in their cell phone. At last, end the exchange by client writing of produced OTP code on the screen.

7. References


