Verification of the users using QR code in Banking Systems

[1]Jimil Shah, [2]Rushikesh Sonawane, [3]Shubham Lad , [4] Sunil Wankhade
[1]Student BE, [2] Student BE, [3] Student BE , [4]Mentor
Department of Information Technology,
MCT's Rajiv Gandhi Institute of Technology, Mumbai, India

Abstract: This work contributes in the structure and usage of an imaginative secure verification technique which uses a QR code; an open source confirmation of-idea validation framework that utilizes a two-factor confirmation by consolidating a secret key and a camera-prepared cell phone, going about as a verification token. QR code is incredibly secure as all the delicate data put away and transmitted is scrambled; anyway it is additionally a simple to utilize and cost-effective arrangement. In the QR code a mind boggling secret phrase is put away. Advanced mobile phone is utilized for examining the QR code. The code is examined with the QR code scanner. Filtering result create one string which is the blend of IMEI number of a mobile phone which is registered by the client and the arbitrary number, where irregular number is produced by the irregular number capacity. On the off chance that the system is accessible on the advanced cell, at that point that created string is naturally gone into the login page and landing page of bank is open. Otherwise six digit pin code is created and it needs to physically enter in the login page and landing page of bank is open for exchanges. In a cutting edge world where we can do nearly everything on-line (banking, shopping, conveying, putting away and sharing individual information...), it is these days a basic issue to have the option to get to these administrations in the most made sure about way. In fact, as infections and breaking strategies become increasingly unpredictable and ground-breaking continuously, the accessible security procedures must improve too, permitting clients to ensure their information and interchanges with the most extreme certainty. The point is to build up a confirmation strategy utilizing a two factor verification: a confided in gadget (a cell phone) that will peruse a QR code and that will go about as a token, and a secret phrase known by the client.

Index Terms–IMEI Number, Two-Factor Confirmation, Verification token, QR code**.**

I. INTRODUCTION

Presently a day's practically all the things we can do on the web (like banking, shopping, conveying) and right now is that while doing this things online our data isn't get harmed. In fact, as the technique for deciphering the security code get increasingly unpredictable and ground-breaking. There is have to grow all the more remarkable security application. These incredible applications permit client to take a shot at untrusted PCs certainly. This work depends on the two way validation framework. Right now code gives security. QR code is the Quick Response code .The current framework having security techniques, for example, password, user name, biometrics, and face detection. In any case, in these strategies security isn't sufficient, so there is have to grow such security framework which gives high security. The ongoing enthusiasm for the utilization of visual labels in regular daily existence is a characteristic result of the innovative advances found in current cell Phones .The QR code is a framework comprising of a variety of array of nominally square modules orchestrated in a general square example, including an extraordinary example situated at three corners of the image and proposed to aid simple area of its position, size and tendency .A wide scope of sizes of images is given together four degrees of mistake remedy. Module measurements are client indicated to empower image creation by a wide assortment of systems.

.

Fig. 1.1: Structure of QR code

There are two areas right now. In the encoding area transformation of information to a QR image happens. Right now investigation and encoding is done then after Error adjustment coding the last message is structures. Following the Module arrangements in network with covering another segment is the Decode area. This segment contains translating of the info QR Code picture and shows the information contain that QR code.

The deciphering method begins with the rearrangement of high contrast module at that point Decode position data.

There are two sections in this system. In the encoding section conversion of input data to a QR Code symbol takes place. In this the data analysis and encoding is done then after Error correction coding the final message is structures. Following the Module placements in matrix with masking another section is the Decode section. This section contains decoding of the input QR Code image and displays the data contain that QR code. The decoding procedure starts with the reorganization of black and white module then Decode format information.

II LITERATURE REVIEW

Patric Elftmann in his work [1] has given detail information regarding authentication. He has mentioned briefly about password-based authentication mechanism, graphical-based authentication mechanism and keystroke-based authentication mechanism. Also he has described about threats and attacks by attacker and security issues faced by user while authentication. His all focus was to provide an accurate and reliable means of authentication.

W. Jensen broadly classified the current authentication methods into three categories which are token based authentication, biometric based authentication and knowledge based authentication [2][3]. As mentioned in the paper, token based and knowledge based authentications are widely used while biometric based authentications are not yet widely adopted which are one of the most secured ones.

A new approach of picture-based authentication was proposed by salim Istyaq[4]. He also classified it into two categories: recognization based and recall based graphical technique. He proposed a new hybrid technology in the graphical password scheme integrated with audio signature to enhance the stability of the system.

Salim Istyaq in his work were successful in developing a new hybrid technology in the graphical password scheme integrated with encode passphrase QR code with OTP to enhance the stability as well as security of the system[5].

Brindha G. and Gopikaarani N. In their work [6] came up with idea of merging IMEI number of phone with OTP for authentication of banking system. QR code is generated first with 3 parameter OTP (enter by user during registration), image size and image format. This QR code after scanned by user device gives rise to a new sequence of 6 digit pin which is a mixture of IMEI number and the OTP. This sequence is displayed on users system which user need to submit in order to authenticate the banking system.

Palasha Rawal, et,al proposed a banking system for both online and offline authentication [7]. In online mode, QR code is generated with the help of IMEI number and random string which user need to scan using his device to authenticate the system. In offline mode, a OTP is generated with the help of pin code generation algorithm which also uses IMEI number to maintain the security of the system.

Jaideep Murkute,et.al in their paper [8] have mentioned about hashing algorithm SHA-256 which is found to be very useful for creating a hashed string from the data of QR code which is appended with IMEI number. SHA algorithm helps in maintaining the security of the system and also prevents phishing attacks by generating different hash string every time which is later used as OTP.

III EXITING SYSTEM

- **OTP**

One-Time Password (OTP) is a technological mechanism through which a single-use password is generated and sent to the registered mobile number for the user to access the website. . OTP lends an additional layer of security to protect the digital identity of the end users

Most online exchanges require a two-advance validation, and the One-Time-Password (OTP) sent by SMS is regularly one of those two stages. The reason for an OTP is to forestall extortion by affirming that the individual making the exchange and the charge card proprietor are indeed the very same. To do as such, a brief code is naturally sent by SMS to the telephone number related with the financial balance used. Once the OTP SMS is gotten, the client types it in the exchange interface and he is at exactly that point ready to conclude his buy. In any case, is the cell phone (tablet or cell phone) used to send and get a SMS harmless? Deplorably, not very. What appeared to resemble a solid verification process when it was first presented is these days effortlessly skirted by portable applications.

Our group recognized two sorts of versatile applications utilizing the OTP interference system: the genuine ones and the pernicious ones. While a safe application will block a SMS OTP to encourage exchanges and make them quick, a vindictive application will capture it so as to submit banking extortion.

Password

A password is a series of characters used to confirm the identity of a client during the verification procedure. Passwords are regularly utilized in conjuncture with a username; they are intended to be known distinctly to the client and permit that client to access a gadget, application or site. Passwords can differ long and can contain letters, numbers and extraordinary characters

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website. Passwords can vary in length and can contain letters, numbers and special characters. Following are the issues faced in password.

Phishing/key loggers/sniffers

The most straightforward approach to find somebody's secret key is to have them disclose to you it. This should be possible by convincing them to type it into a site you control (usually known as phishing), by introducing a key logger (either equipment or programming) on a PC, or by perusing traffic on a decoded remote or wired system. For gatecrashers these techniques have the incredible advantage that it doesn't make a difference to what extent or complex a secret key the client has picked: the interloper can essentially understand it.

Splitting of hashes/animal power

On the off chance that the gatecrasher can't acquire the secret word, at that point he can just utilize a program to create billions of potential passwords (frequently utilizing indistinguishable strategies from are recommended for picking passwords) and attempt every one of them against the record. The crudest method to do this is to just endeavor to sign in utilizing each created secret key: the subsequent surge of secret phrase disappointments ought to be simple for a framework chairman to spot, yet since assailants keep on utilizing this methodology it appears it is still sensibly fruitful. Endeavors might be made against darken validated administrations, for example, SSH and LDAP, to decrease the odds of discovery.

Disconnected breaking

Savage power assaults are substantially more subtle if the gatecrasher can acquire a duplicate of an encoded secret key, for instance if a framework's secret key record can be downloaded, if a hash has been remembered for an open document, or if an obscure machine can join a validation gathering. When the interloper has at least one scrambled passwords he can do the beast power speculating on his own machine (utilizing present day equipment and calculations this may take just a couple of moments for short passwords), or even utilize a cloud administration, and afterward come back to login to the objective once the right secret word has been found.

IV IMPLEMENTATION

The system is basically divided into two modules:
1) Generation of QR code
2) Banking System

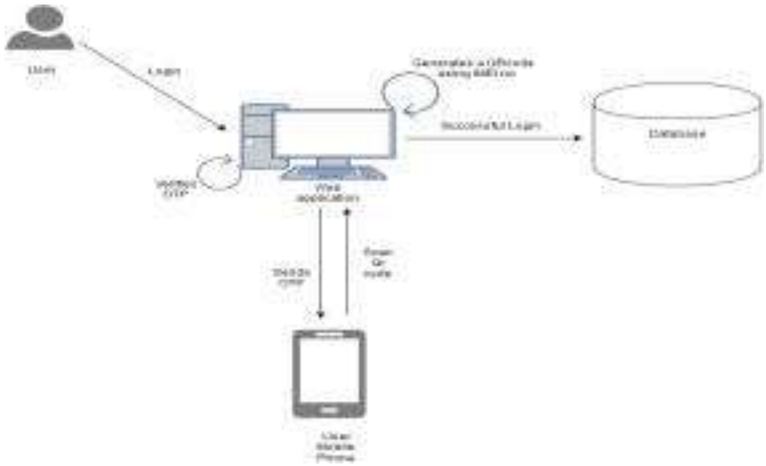

Figure 4.1 Working of the QR code system

1) Generation of QR code

Use of QR code makes it sure that the information will be decoded by legal and real client just observing that a translating gadget will be imperative to disentangle it. QR code envelops the subsequent designs in particular planning design, discoverer design, arrangement design, group data and information cell. The QR code is a square module where all the four sides are encompassed by the very zone fringe. Capacity designs furthermore, encoding locales are inserted in a QR code. To execute coarse situating for the QR picture, the restriction of QR code utilizes the discoverer examples to acquire the surmised district of QR code as for the discoverer designs. Information and blunder adjustment strategies guarantee that the QR code will be perused successfully regardless of whether some bit of is harmed up to 25 percent.

2) Banking System

Right off the bat the customer fills in the subtleties of a financial balance and submits it to the bank worker. The worker spares and stores all the data into the database framework. This Banking framework at that point sends an OTP to the customer. The customer continues for the confirmation procedure and next is advised to change the secret key after the fruition of the confirmation procedure for better safety .The customer when re-logins into the framework with the username and new secret phrase prompts sending a demand for age of a QR code. This creates a QR code when the solicitation is sent to the server which is shown on the customer's machine. The customer will at that point check the QR code with the cell phone with the assistance of Random no. what's more, IMEI no. which will be put away in the framework database. In conclusion it checks the method of association.

Above all else the IMEI and the arbitrary numbers are scrambled utilizing the open key. This scrambled string is utilized to create the required QR code with the assistance of a QR code age work present in java. Next, this QR code picture is shown on the customer machine for the client to filter it utilizing a cell phone. According to figure 4.1 , in an online mode transaction(which implies in the accessibility of web on telephone) , the produced string (IMEI number and arbitrary number) consequently gets went into the login page which after effective login coordinates the customer towards the home page of the bank. There is no compelling reason to recollect the secret word which is the blend of your IMEI number and the irregular number for your login right now. The server decodes the string utilizing the client open key and checks and guarantees that a passage exists in the exchanges table and afterward likewise alters the column of exchange table. Consequently the server confirms that the IMEI against confirm and misrepresentation ones and doles out that IMEI to the right client. On the off chance that the login is fruitful, the exchange push is then erased. This guarantees each time the created QR code picture is one of a kind and unique. Next, the PHP meeting is made and when client logsoff , the meeting is decimated.

VI RESULT:

Figure 5.1 Explains what details has the customer has to add the details for registration during the first time. After the user add's these details then the data is been saved on the server for future use.

Figure 5.2 Explains that when the user wants to access his/her account the user has to enter his/her registered email id and if that matches which the database then the system automatically generates a QR code which the customer can scan and login to his/her account.

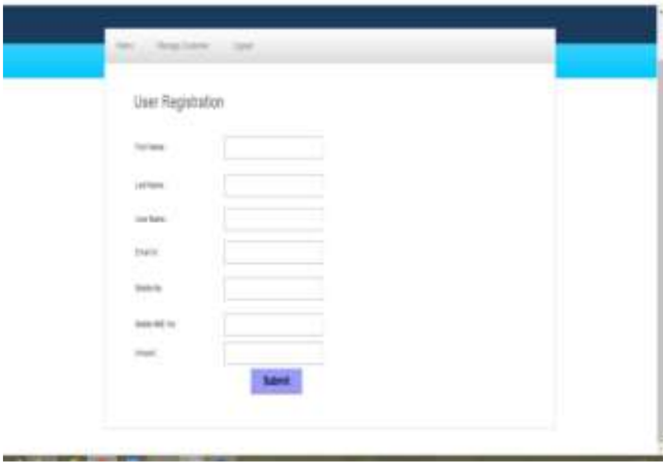

Figure 5.1 Admin User database

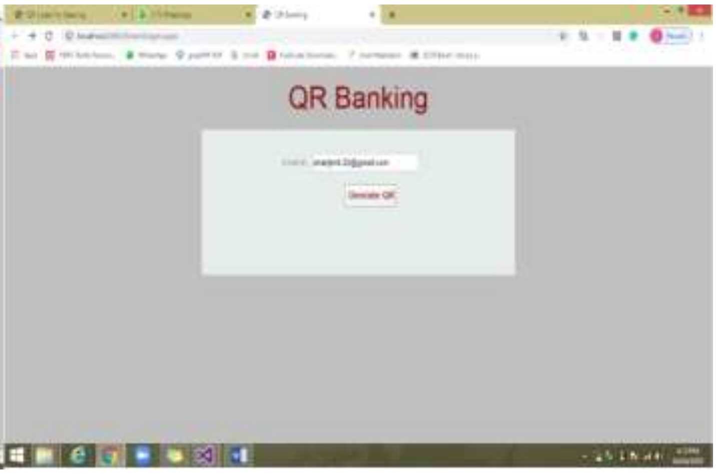

Figure no 5.2 Generation of QR code

VI CONCLUSION

This system provides a high level security to the customers of the bank as there are very less chances of a getting attacked by a attacker. The system is using the IMEI Number of the customer mobile which can't be stolen or cannot be used by someone else. So from the customer point of view this system is better than the existing systems available in the market right now. An important measure of individuals living in a created nation would have an advanced cell ready to take pictures and output QR codes which makes this validation approach a genuine the normal verification technique, as it is situated in a two factor verification technique and not in the typical username also, secret key methodology. QR-based verification offers a extremely secure and quick verification strategy that must be considered to safely and effectively validate.

REFERENCES

1) Patric Elftmann, Diploma Thesis, " Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006

2) W. Jensen, "Authenticating Mobile Device User Through Image selection" in Data Security, 2004

3) W. Jensen, "Authenticating Users on Handheld Devices" in proceedings of Canadian Information Technology Symposium, 2003

4) Salim Istyaq, "A New Approach Of Graphical Password with Intergration of Audio Signature Combination of Recall and Recognition" in internation journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN(P): 2249-6831, ISSN(E): 2249-7943 Vol. 6, Issue 4, Aug 2016, 45-50.

5) Salim Istyaq World Academy of Science Engineering and Technology International Journal of Computer and Information Technology vol:10 no:6, 2016

6) SECURE BANKING USING QR CODE in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 12, December 2014 ISSN: 2278 – 1323

7) Secure Employed using QR Code for Banking System
International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICIATE - 2017 Conference Proceedings

8) Online Banking Authentication System Using QR-code and Mobile OTP
Jaideep Murkute, Hemant Nagpure, Harshal Kute, Neha Mohadikar, Chaitali Devade / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622