IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Multilevel Authentication Based on QR Codes to Secure Banking Operations

Apoorva Khilare[1], Monika Dhage[1], Dhananjay Ghule[1], Rushabh Masurkar[1]

Student, Department of Computer Engineering, Sinhgad College of Engineering, Pune, India[1]

Abstract: Today, People can do almost everything online (banking, shopping, storing and sharing personal information). To access these services in the most secured manner is very critical. Many authentication methods are available such as username and password, barcode, finger print and face detection. But these methods have some advantages as well as disadvantages. Username and password are not providing security; fingerprints and face identity are the methods which are very costly and not affordable by common users. To overcome all the drawbacks the QR code is introduced. QR code has many applications. QR codes are used in banking transactions for security; it provides more security than barcode. The QR code stores complex password. QR code can be scanned using smart phones. When a user opts for online banking transaction he opens the bank website. On the same page, QR code is displayed after registration, user can scan the QR code image with a scanner. A string is generated after scanning. For authenticating user, IEMI no. of phone is used. The multilevel security is used in this application; therefore this system is very secured method for online transaction than existing system.

Keywords: Barcode, QR code, IMEI no., Finger Print.

I. INTRODUCTION

The internet-banking concept is a part of our lives. It is much more comfortable to make transactions and to check the account status from your home rather than going to a bank or calling a bank-officer. These kind of services are provided by banks to their clients. Because of this, it is very important to consider the security improvement of the authentication tasks. Authentication can be conducted by using simple username and password (that is the weakest method) by multimodal biometrics. But, most of these methods are based on what user is (voice, iris, retina etc.) or what user remembers (a password). The drawback of these methods is either they are very costly or there is possibility that user will forget the key.

Authentication by using QR code is a web based application. It is designed for providing security by using multifactor authentication method. QR(Quick Response) code is two dimensional barcodes. The proposed system makes use of QR codes for ensuring security of user's data by user authentication.

The Proposed system is a multilevel authentication system. The user is asked to enter his/her details. System admin will verify a user and allow him/her to proceed further. After successful login by using one time password and hexaflip password, the system will generate a random number which will be encoded into a QR code. This QR code will be scanned by using camera equipped mobile phone. While scanning IMEI (International Mobile Equipment Identity) no of the phone will be captured and a string which will be combination of the random no(stored in QR code) and IMEI no. of the mobile phone will be generated and it will be sent to system. An another string will also gets generated in the system by using the IMEI no (that user has registered while registration process) and the random no. Further the system will crosscheck the sent string with the string available in database. According to connection mode the system will authenticate user and user will be able to do the further transactions.

II. PURPOSE

In order to overcome weaknesses and inconvenience of security, our proposed authentication system is designed to provide greater security and convenience by using OTP, hexaflip password and two-dimensional barcode.

III. RELATED WORK

Several authentication methods have been proposed from simple username and password to costly multimodal biometrics, in the last decade. This section will give a brief idea about all these available methods.

A. Different methods of authentication

Internet banking applications can be connected in a variety of ways. The most popular ones comprise of using a user and a static or dynamic password.

1. Username and static password:

This is the most flawed method to validate tha data. In this, one must register by giving relevant information. A week later, the bank sends an activation email to gain access to the application. This is followed by a link that contains the provision to set an initial password. After this step is completed, the user can enter his/her details to login.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

When user enters correct credentials, they can proceed to account's main page and go on to alter personal data, examine the account statement and facilitate fund transfers.

This page does not have a provision for changing the current password. In case someone fails to remember the password, he or she can change the password or alter personal data only by contacting respective call center and validating their identity by responding to queries posed to them. This provision is not safe as a person<s detail can be stolen by phishing and a complete stranger can contact the call center, claiming to be somebody else. Also, banking applications use single pass word, hence if the password is hacked, the banking assets are at total risk. So, this method of verification is too risky, hence not feasible.

2. Username and dynamic password:
Mobile banking is used to get dynamic password. So SMS OTP process is needed to be used to complete verification process. The contact no needs to be registered on the account by the user. After entering the login credentials, the users cell phone receives an SMS which has a one time password that should be entered in the authentication form. Then user gains access to his or her account. For this, it is required to register the user's phone number on his/her account.

3. Biometrics:
This word has Greek origin and is formed from "bios" (life) and "metrikos" (measure). It consists of complicated ways of automating the identity of a person by using recognisable (face geometry, iris, retina, fingerprint, voice, etc.) and/or manual (writing dynamics, signature, etc.) properties of a people. A wide variety of biometric properties such as: fingerprint, iris, hand geometry, face geometry, gait, vein pattern, retina, keystroke pattern, voice, ear, signature and many others. Most of these are use to identify identity over internet but others such as DNA can only be used in medical forensics and when internet is not available. Such multiple methods of testing identity through biometrics can increase security manifold.

4. Barcode:
A barcode is an machine-readable, optical representation of data. Data can be systematically represented using barcodes to alter the gaps and widths of parallel lines. Barcodes are called as one-dimensional (1D) or linear. Barcodes are useful in a lot of instances, such as in tracking of people and also a wide variety of objects such as express mail, parcels, rental airline luggage, registered email, cars and even nuclear wastes. Another function of barcode is to keep track of time spent on a job and to scan customer orders in the applications that control floor wise cataloguing supermarkets and retailer shops. Despite being useful, barcodes have their disadvantages such as it has data capacity of storing 120 characters only. Barcodes cannot be updated, If it gets partially damaged, data stored in it cannot be read.

5. RFID code:
RFID needs a lot of manual work before it can be utilized. The RFID tags are individually attached to things, containers and pallets. A wave having frequency in the range of radio waves is given out of the small antenna of the RFID tag. A wireless reader of RFID tags captures and interprets the signal emitted by this wave, thus securing details about the object that the tag is attached to the uses of RFID are almost similar to those of barcodes but RFID tags are quite expensive.

B. Internet banking
Internet banking is also known as virtual banking ,online banking or e-banking. It is provision designed by financial institutions like banks which can be used over the internet by the account holders and other customers to manage their bank accounts and to facilitate fund transfers. The user uses pre-existing verification methods to login and visit a safe website provided by the bank. These days, internet banking can be performed by visiting the bank's webpage online through a browser. However, initially, banks designed independent software applications which had to be installed in the desktop.

IV. QR CODE

The QR codes stands for the Quick Response Code. The barcode mentioned earlier was a one dimensional authentication method. The QR code is a barcode that is two dimensional. It is a barcode that uses a matrix and was first designed in Japan for automotive industry. A barcode has details of the object to which it is affixed and can be interpreted by a machine known as a barcode reader.
To efficiently store data, a QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary); extensions can also be used.
As compared to general UPC barcodes, QR codes can be scanned faster and can store a greater amount of data. These characteristics made the QR code famous outside the Japanese automotive industry. Quick Response codes are used for managing documents, recognisability of objects, general marketing and tracking of products and time. A QR code consists of a white background along with square shaped modules that are blank in colour and arranged in a square shaped matrix, which are in the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

foreground. This code can be read by scanners and cameras and mistakes are removed by the Reed-Solomon technique till the image is aptly scanned. Vertical and horizontal components of the image contain patterns that can be chosen and selected to obtain needed data.

A. Finder Pattern:
The finder pattern is used to trace the exact location of the QR code. Geometric properties of the code, such as the dimension and the angle can also be examined. A more significant use of the finder pattern is in the detection of the code in angles that are round the clock. Distortion post scanning is made correct using Alignment patterns which are very useful. The correction of this distortion is facilitated by the black module in the central area of the Alignment Pattern.

B. Timing Pattern:
If an error pitch is present in the middle part of cell, it can be recognised in both, vertical and horizontal directions using supporting patters called Timing Patterns.

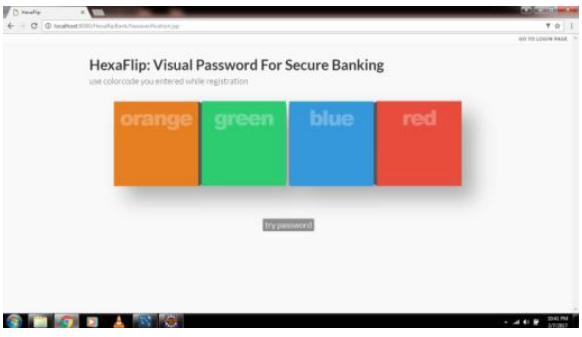
C. Quiet Zone:
The function of the data embedding technique can be simplified by recognising the QR code from it's relatively complicated backgrounds using this zone.

D. Data Area:
Confidential information can be stored in this section. The black and white sections can be allotted zeros and ones in either of the two possible combinations and thus, information can be hidden in binary format. For the rectification of mistakes and the respective embedding of data ,the Reed-Solomon codes can be used.

C. Links and Bookmarks
All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL your paper, you must type out the address or URL fully in Regular font.

V. HEXAFLIP PASSWORD

HexaFlip is an javascript plugin that allows a user to flip the cube on drag with 3D animation effects. Good for animated 3D slider, Time Picker, slideshow and more.



HexaFlip visualizes arrays as cube interfaces.
Transform arrays of any length into cubes with infinite sides. HexaFlip was born out of the time-picker interface in the iPhone app ChainCal. It's been expanded to visualize arbitrary arrays of any length.
Steps to create code of hexaflip password are:
Create an instance by passing a DOM element and a key-value set of arrays:

```
Var cubeSet = new HexaFlip(documentGetElementById('my-el'),
  {
     prince: ['For You', 'Prince', 'Dirty Mind', 'Controversy', '1999', 'Around the World in a Day'],
     curtis: ['Curtis', 'Roots', 'Super Fly', 'Back to the World', 'Got to Find a Way', 'Sweet Exorcist']
  }
);
```

you can also pass a selector string and HexaFlip will take the first matching element:

```
var firstDiv = new HexaFlip('div');
```

To enable horizontal rotation (like the photos above), pass it in the options:

```
var horizontalCube = new HexaFlip('\#my-el2',
  {
     letters: ['\alpha', '\beta ', '\gamma', '\delta', '\epsilon', '\zeta', '\eta', '\theta', '\iota', '\kappa', '\lambda', '\mu','\nu', '\xi', 'o', '\pi', '\rho', '\sigma', '\tau', '\upsilon', '\phi', '\chi', '\psi', '\omega']
  },
  {
     horizontalFlip : true,
     size: 300
  }
);
```

To set and get the values of the cubes :

```
cubeSet.setValue({ prince: '1999', curtis: 'Roots' });
cubeSet.getValue();
```

To rotate the cubes to the next or previous sides:

```
cubeSet.flip();
```

VI. PROPOSED SYSTEM

A security system is developed by using QR code for security. The Four important modules in the system are registration and login, hexaflip password verification, QR code generation and scanning, transaction. Another important part of system is camera equipped mobile phone. Here, the mobile phone (which will be used for user authentication) is used for scanning the QR code.

A. Registration and login system
The user can submit his or her credentials like IMEI number of the phone, username and password by going into the registration section on the webpage. Post verification, the database is used to store the relevant data. In a registration if the user does not enter all the values like username, password, IMEI number, mobile number, and email address then registration process will not get

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

completed. Validation is most important part in registration process; if validation is not successful then user is not able to login. Once the verification process is finished the client is asked for changing the password. The client when re-logins the system, with the username and new password generated by the client, then he moves to next authentication process.

B. Hexaflip password verification

While registration, user enters hexaflip code which will be encrypted before storing in database ie. if he enters colour password as 'red green blue', while storing it will be stored as 345 where 3 stands for red, 4 stands for green, stands for blue . The advantage of this type of encryption is that even if the database is hacked, no one can crack the code easily.

C. QR code generation and scanning

After entering hexaflip password it sends request to generate QR code. Once the request is sent to the server, it generates QR code which will be displayed on the client machine. First random number is encrypted using public key. The encrypted string generates the Quick Response Code using it's generation function in java. Now, the client machine displays this image of the QR code. This QR code is scanned by the user using cell phone. By scanning the QR code, he extracts the information (random no.) stored in the QR code. This random no gets combined with the IMEI no. of the user's mobile and a string is generated. This string is matched with the string generated in database. The string in database is generated by combining IMEI no that client has entered while registration and the random no. If both the strings i.e. string sent by user and string generated in database matches then it can be confirmed that user is authenticated. For login each time, new QR code is generated.

So in our system there is no need to remember the password which is combination of your IMEI number and the random number.

D. Transaction

After successful login the home page of the bank is opened. User can check his mini statement, can transfer money to another account holder from the home page

VII. RESULTS

The verification system needs to be quick and safe. In order to make this process faster, the time between the following is measured :user entering his/her login credentials, verification of hexaflip, generation of Quick Response Code ,it's scanning using a cell phone. The server already has the required correct response and if this response coincides with that of the user, then user is redirected to the next page. This is an Android-specific application. Decoding of QR codes requires 3 to 4 seconds. However, the hand may shake while holding the scanner or the lighting may be poor, which may add some more time to the process. Thus, the overall scanning process requires about 3 to 5 seconds.

VIII. FUTURE SCOPE

This new system is limited to Android smart phones. In the future works, system will be developed in such a way that it can be used amongst various smart phone architectures. The potential security risks such as session hijacking, mobile spoofing, man-in-the-middle attack must be tested. Depending on the results of performance measures, it is also planned to develop enhanced versions of this model which shall be using newer versions and alternative modes of QR code with higher data storage capacities.

VIII. CONCLUSION

The security measures initially used in banking transactions included barcodes and fingerprints and they did not provide the required level of safety or appropriate quantity of bit storage capacity. Implementing QR codes with hexaflip as an additional encryption level, we conclude that the security level of banking transactions has considerably increased, thus making the overall process of banking much more convenient.

ACKNOWLEDGMENT

We express immense gratitude and are highly indebted to **Prof. S.A. Joshi** for her assistance, guidance and incessant supervision and also for giving significant information pertaining to the seminar and for her help in completing the seminar.

REFERENCES

[1] "QR Codes and Authentication protection.", IEEE Jing Yang School of Business and Economics State University of New York,2015.
[2] "Android System For Identification of Objects Based on QR code", IEEE, DijanaJagodic, 2015.
[3] "Secure Authentication for Online Banking Using QR codes",volume4,Issue3,March2014,Sonawane Shamal.
[4] "Improving Fingerprint Based Access Control System Using Quick Response Code", IEEE, Xiangpeng,2015.
[5] "Interactive Android-Based Indoor Parking Lot Vehicle Locator Using QR-code", IEEE, Siti Fatimah Abdul Razak, Choon Lin Liew, Chin Poo Lee, Kian Ming Lim ,2015.
[6] "A Two Factor Authentication System with QR codes for Web and Mobile Applications", IEEE, Mete Eminagaoglu,2014.
[7] "Applying QR Code and Mobile Application to Improve Service Process in Thai Hospital", IEEE, chayakrit Charoensiriwath ,Navaporn Surasvadi,2015.
[8] "Two level QR code for private message sharing and document authentication", IEEE, Iuliia Tkachenko, William Puech, 2015.