Secure Banking System Using QR Code Authentication

Devendra Jadhav, Shivam Shinde, Krisha Shah

Abstract— This work includes use of QR codes for improving the authentication process of banking website and makes it more secure. In a modern world where we are able to do almost everything online (banking, shopping, communicating, storing and sharing personal information...), it is nowadays a critical matter to be able to access these services in the most secured manner. Indeed, as viruses and cracking methods becomes more complex and powerful by the day, the available security techniques must improve as well, allowing users to protect their data and communications with the maximum confidence and trust. This system includes a QR code, an open source authentication system that uses a two-factor authentication by combining a Random number with the IMEI number of the mobile phone and generate a string which is hidden behind the QR code that needs to be scanned by a camera-equipped mobile phone scanner, acting as an authentication token. Our aim is to develop an authentication method for banking website using a two-factor authentication: a trusted device (a mobile phone) that will read a QR code that will act as a token, and a password known by the user.

Index Terms— QR code, IMEI, Security, Bank, AES, Authentication, Scanner.

1 INTRODUCTION

Now a days, activities like shopping, commucation, banking transactions are all done online. The problem faced by most is that there is little to no assurance of the safety of the information flowing over the internet. With every passing minute, hackers are dedicatedly attempting to break the security systems that protect our data online and improving their techniques to break into systems. Considering the previous observations, the need of the hour is to keep developing ways to thwart the hackers attempts by improving the security applications deployed to protect our systems. Thus, the users of secury applications can work with confidence on untrusted computers. Hence, we will be using a system that uses two factor authentication to develop a secure banking system for the users**.** In this the QR code provides security. The existing systems have security methods such as password, username, finger prints, and face detection. But in these methods security is not up to the mark, so there is need to develop such a security system which provides high security. 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. A wide range of sizes of symbols is provided together with four levels of error correction.

Fig. 1: Structure of QR code

2 PREVIOUS 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.

Different methods of authentication for Internet banking applications can be connected in a variety of ways. The most popular ones comprise of using a userame and a static or dynamic password.

2.1 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.

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 provision is not safe as a person's details 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.

2.2 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 number 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.

2.3 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. Such multiple methods of testing identity through biometrics can increase security manifold.

2.4 Barcode:

A barcode is a machine-readable, optical representation of data. Data can be systematically represented using barcodes to alter the gaps and widths of parallel lines. Barcodes are 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. 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.

3 PROPOSED FLOW

The system is divided into two modules:

3.1 Generation of QR code

3.2 Banking System

3.1 Generation of QR code:

QR code comprises of following patterns: finder pattern, timing pattern, format information, alignment pattern, and data cell. Use of QR code ensures that data will be decoded by legitimate user only as decoding device will be required to decode it. The figure 1 shows the structure of QR code. All four sides of the QR code are surrounded by the quite zone border. QR code consists of function patterns and encoding regions. The localization of QR code gets help from finder patterns of its most marked feature. Obtain the approximate region of QRcode, and implement coarse positioning for QR image according to the finder patterns. According to located QR code obtain the version number determine the size of QR code. Data and error correction code words ensures that the QR code will be read successfully if some portion of it is damaged.

3.2 Banking System:

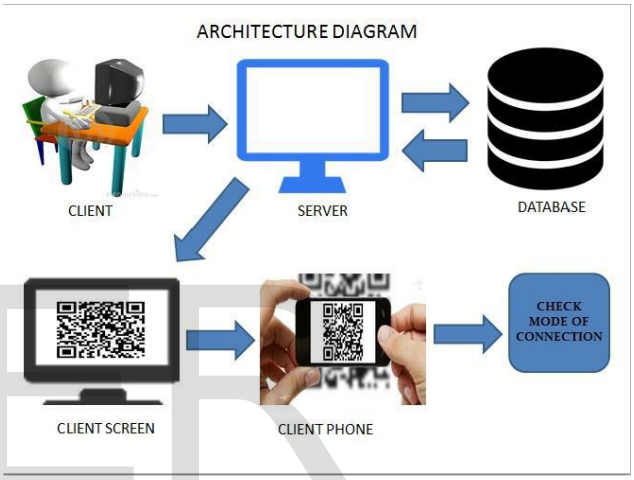

Fig. 2: Banking system architechture

The figure 3 shows the architecture of banking system. The client must first create a bank account in the bank. During the creation of bank account, personal details along with the phone number and the corresponding IMEI number is registered. Bank Employee then stores the mobile number and its corresponding IMEI number in the customer database along with other details. The bank sends a user id and password to the customer. This id and password is used by the customer to login into the bank website. The password can be changed by the user after the initial login. The client when relogins the system with the username and new password generated by the client, 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's machine. The client then scans the QR code with the mobile with the help of Random no + IMEI no which will be stored in the system database. It is then said to check the mode of connection.

3.2.1 Online mode:

As shown, in this First IMEI number and random number are encrypted using the public key. This encrypted string generates the QR code using the QR code generation function which is present in java. Now this QR code image is display on the client machine. User scans this QR code using mobile phone. After scanning, in online mode means net is available on phone the generated string (IMEI number and random number) automatically gets entered into the login page. After successful login the home page of the bank

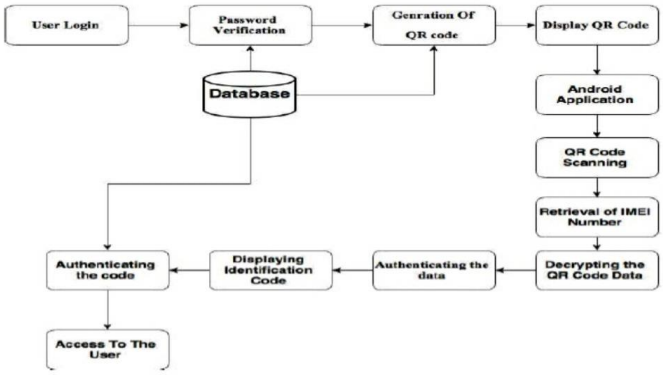

Fig. 3: Online Authentication system

gets open.

Hence in this system there is no need to remember the password. The server decrypts the string using the user public key and verifies that a row exists in the transactions table with our random number and then accordingly updates the row of transaction table. Subsequently the server checks that the IMEI is correct or not from the database. If the login is successful the transaction row is deleted. It means every time the generated QR code image is different. Now the PHP session is created and when user logs off and the session is destroyed.

3.2.2 Offline mode:

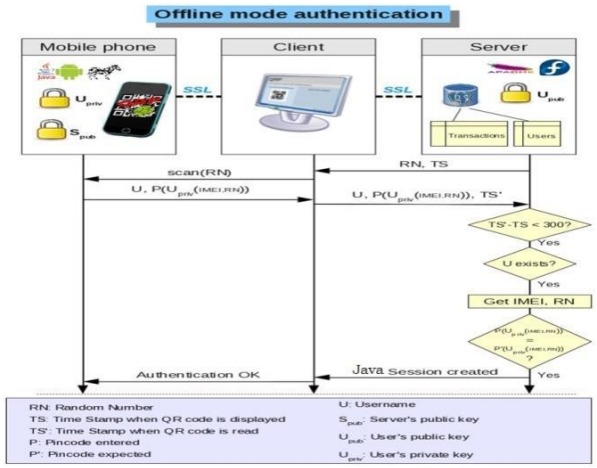

Fig. 4: Offline Authentication System

In this if the phone detects that the Internet cannot be accessed within specified time period then, using pin code generation algorithm, a unique six-digit number is generated from the encrypted string (IMEI number and random number). Fig.5: Offline Mode of Authentication User has to enter this pin code on login page manually with respect to username. For entering the pincode, the keypad is available on screen. So, there is no need to enter the pin code using systems keypad. This system provides more security at this point. After entering the pin code server verify the IMEI number of user which is stored in the database. If the IMEI number is present then user is valid and then homepage of bank is gets open. The timestamp is also checked. If the random number is generated before the 10 minutes ago then session is destroyed. Hence the user is not able to login.

4 SOFTWARE REQUIREMENTS

4.1 RealTime Database:

A real time database is used due to its performance and scalability. Apart from this, the database will process a lot of data because of the number of clients that perform transactions. Database is used for authentication of IMEI number and client's information and data storage.

4.2 Android Application:

The Android app contains mostly two layouts one for login options and second page contains the scanner camera to scan the QR code. The app must be downloaded on every client's android phone with a camera permission access.

4.3 Website:

The website of the bank contains registration page with information about the IMEI number of the user to be entered which will get stored into the database so the next time user gets online for net banking, he/she will be authenticated with the data stored in database. The website will mostly be used to show the authentication process and transaction options like withdrawal and deposit.

5 LIMITATIONS

The system proposed is mainly developed to add a security level to protect the user's personal information, but with some limitations. This iternet technology has some limitations which are listed below.

1) User need to have strong internet connection and a phone with a camera.

2) Application of the bank needs to be installed

3) User needs to log on both on the app and in the website while transacting which will take just few seconds.

6 CONCLUSIONS

This system uses AES algorithm to encrypt the (IMEI number combined with Random digit) string hidden behind the QR code. The algorithm is light weight and used by industry standards for application softwares to protect the information of the users which is of utmost concern in the netbanking era. Hence, to improve the security of authentication process by adding an additional layer, we are using qr code mechanism for verifying the otp and hence the user.

ACKNOWLEDGEMENT

The authors wish to thank Prof.Jaya Jeswani, Dept. of Information Technology, Xavier Institute of Engineering for her unending support and guidance for this project.

REFERENCES

[1] Snehal Kalbhor, Ashwini Mangulkar, Mrs. Snehal Kulkarni "Android App for Local Railway Ticketing Using GPS Validation".
International Journal of Emerging Trends in Science and Technology, IJETST-Volume 01, Issue- 01, March-2014, Pages 71-74.

[2] Fu-HauHsu, Min-HaoWu, Shiuh-JengWANG, "Dual-watermarking by QR-code Applications in Image Processin".9th International Conference
on Ubiquitous Intelligence and Autonomic and Trusted Computing, DOI 10.1109,2012, Pages 638-643.

[3] Mrs.Shanta Sondur, Ms. Tanushree Bhattacharjee "QR-Decoder and Mobile Payment System for Feature Phone", VESIT, International Technological Conference(I-TechCON)-Jan. 03 – 04(2014), Pages 13-15.

[4] SomdipDey, B. JoyshreeNath and C. AsokeNath "A New Technique to Hide Encrypted Data in QR Codes" Institute of Information Systems Argentinierstrasse -2009.

[5] Dr. A. P. Adsul, Gayatri Kumbhar, Vrunda Chincholkar, Yogesh Kamble, Anuja Bankar "Automated Exam Process using QR Code Technology" International Journal of Application or Innovation in Engineering & Management, (IJAIEM)-ISSN 2319-4847, Vol.3, Issue 4, April- 2014, Pages-296-298.

[6] Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica S. Lam "Secure, Consumer-Friendly Web Authentication and Payments with a Phone", International Journal of Applied Engineering Research, ISSN 0973-4562, Vol. 8, No. 17 (2013).