International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

THREE LAYERED SECURITY FOR BANKING

Tanvi Gangawane[1], Jemin Patel[2], Sambhav Thole[3]

[1]*Tanvi Gangawane, Dept of Information and Technology, Atharva College Of Engineering, Maharashtra, India*
[2]*Jemin Patel, Dept of Information and Technology, Atharva College Of Engineering, Maharashtra, India*
[3]*Sambhav Thole, Dept of Information and Technology, Atharva College Of Engineering, Maharashtra, India*

Abstract - *Layered Security is one method of security to protect the user's resources and data. one layered security consists the usage of login creditionals like username and password. It is the most commonly used system of authentication but it comes with a number of security risks such as stealing the secure and private information and keylogging attack. To overcome this issue we have enhanced the level of security by adding two more layers of security i.e authentication using QR code and OTP based authentication.*

***Key Words*: IMEI number, OTP, QR code, three layered security.**

1. INTRODUCTION

QR code is two dimensional matrix barcode which stores the data in that dimension. Data is presented as square dots with specific pattern in both horizontal as well as vertical dimension. Specific QR scanner can read those patterns and retrieves the stored data. In our approach, second layer is Authentication using QR code. For this, smartphone is used as QR scanner. Instead of executing the entire authentication process on personal computer, the part of authentication is moved to the smartphone. This part of authentication enhances security greatly and offers protection against attack such as malware and keylogging attacks. User plays his/her role in visual authentication which boosts both the security of our system and reassuring to the user that they plays role in the process of authentication. It is not degrade the usability.

1.1 NEED

A keylogger is a software designed to capture all of a user's keyboard strokes, and then make use of them to impersonate a user in financial transactions. keylogger attacks are generally used in login procedures where username and password can stole by user's keyboard strokes or moves.so there is need for authentication system which not only takes username and password but also acquire for another verification step. mostly user's are insecure about their own account in many domain as bank ,healthcare, institutes. so the secure and trustworthy authentication system is needed for people or user.

1.2 APPLICATION AND SCOPE

Our protocols are generic and can be applied to many domains in authentication system. For example, ATM (Automated Teller Machine), personal computer. Furthermore, our design does not require an explicit channel between the bank and the smartphone, which is desirable in many domains.

SCOPE

Besides the security of an authentication protocol, both usability and deployability are equally important and critical for the acceptance of any protocol in modern computing settings. The authentication protocols which we used are generic and can be applied to many types of authentication. It gives better user experience.

2. LITERATURE SURVEY

QR i.e. "Quick Response" code is a 2D matrix code that is designed by keeping two points under consideration, i.e. it must store large amount of data as compared to 1D barcodes and it must be decoded at high speed using any handheld device like phones. QR code provides high data storage capacity, fast scanning, omnidirectional readability, and many other advantages including, error- correction (so that damaged code can also be read successfully) and different type of versions. Different varieties of QR code symbols like logo QR code, encrypted QR code, iQR Code are also available so that user can choose among them according to their need. Now these days, a QR code is applied in different application streams related to marketing, security, academics etc. and gain popularity at a really high pace. Day by day more people are getting aware of this technology and use it accordingly.[1]

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. 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 requirement.[2]

Presence system is one of the important components in the lecture process and student attendance recap is one of the elements in various aspects of lecture assessment. Presence has been carried out by signing students. The use of telecommunications technology which is now growing rapidly is the smart phone where one of the operating systems used in smart phones is the Android operating system, Android provides an open platform for users to create their own applications that have been used if various

mobile devices. In addition to the development of communication technology, there is also a Quick Response Code or QR Code that has the meaning of a code that can convey information quickly with a quick response. QR Code can not only store horizontal information such as barcodes but can also store information vertically. This study aims to build a presence system using an Android operating system. [3]

3. PROPOSED SYSTEM FOR PROJECT

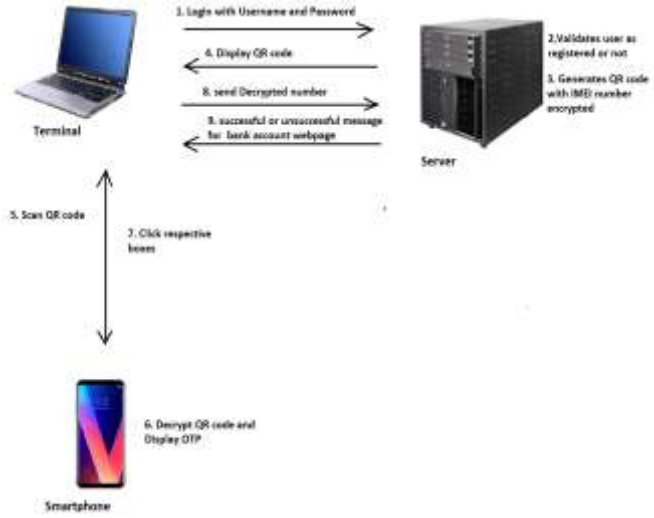

Fig -1: Proposed System

1. Terminal

A user's terminal i.e desktop computer or laptop. The user log in with username and password by using terminal. When server generates QR code, then the QR code displays on terminal. OTP dialog box displays on terminal. OTP submits to server by using terminal. on successful login the bank account webpage opens on terminal.

2. Server

Server is the system entity which performs back-end operations by interacting with the terminal. Server generates QR code and sends to terminal. On successful QR visual login server sends OTP to smartphone. server-sent-OTP submits to server from terminal. Sever checks for successful or unsuccessful authentication.

3. Smartphone:

Smartphone scans QR code which is displayed on terminal. On sucessful QR code visual login, smartphone receives OTP from server.

4. METHODOLOGY

In our approach terminal, server and smartphone each has important role. On terminal, user log in with username and password. The login creditionals sends to server. Server receives the creditionals and checks in database for registered user. Once the user is found as registered in online banking account, then server starts to fetch IMEI number related to that particular user and encrypts it into QR code using QR generator. IMEI number encrypted into QR code using encryption key. New formed QR code sends to terminal. Where smartphone is camera equipped in it . the application with QR scanner is in smartphone. Smartphone has IMEI number same as registered user encrypted IMEI number. That's why smartphone application scanner decrypts pattern hidden in QR code. QR code get scanned by smartphone i.e Visual login of QR code.

Once QR code decrypts, the message of successful visual login sends to server. Server generates 3D OTP i.e three layered of security. Server sends OTP to smartphone. Internet connection should be moderate for procedure. User use this OTP on terminal. On successful OTP verification, server will give user access to his bank account web page.

4.1 ALGORITHM USED

Encrk(□): an encryption algorithm which takes a key k and a message M from set M and outputs a cipher-text C in the set C.

Decrk(□): a decryption algorithm which takes a ciphertext C in C and a key k, and outputs a plain-text (or message) M in the set M.

Sign(□): a signature generation algorithm which takes a private key SK and a message M from the set M, and outputs a signature.

Verf(□): a signature verification algorithm which takes a public key PK and a signed message (M, _), and returns valid or invalid.

QREnc(□): a QR encoding algorithm which takes a string S in S and outputs a QR code

QRDec(□): a QR decoding algorithm which takes a QR code and returns a string S in S.

RSA Algorithm: RSA is the algorithm used by modern computers to encrypt and decrypt messages. This is also called public key cryptography.

5. RESULT AND ANALYSIS

For User Login

Fig -2: User Login

Once the user completes registration process for bank account the user can log in to his/her system with username and password anytime.

Fig -3: QR code generation

After successful user login, QR code will display on user's terminal. This QR code will get scanned by smartphone with scanner in it.

5.1 COMPARATIVE ANALYSIS

Schemes	Security Parameters				Category
	Security from Throttle guessing	Security from keylogging attack	Security from Phishing	Security from Theft	
Last Pass	✓	×	✓	✓	Password Manager
URRSA	×	✓	✓	×	Proxy based
Google 2 step verification	✓	×	✓	×	Phone based
Fingerprint	✓	×	×	✓	Biometric
Three layer security system	✓	✓	✓	×	**QR based Authenticati on**

Table-1: Comparative Analysis based on security

6. CONCLUSION

Our work provides extra security with the normal method of on-line authentication of banking which incorporates username and password. However, by adding QR code authentication the safety measures for banking is secure. At the end, with one time password authentication which completes fulfilment for user login for his/her bank account.

REFERENCES

[1] Sumit Tiwari, "An Introduction To QR Code Technology," in International Conference on Information Technology,2016

[2] Chirag Patil, Umesh Naik, Pallavi Vartak, "Online Session Security System using QR code,OTP and IMEI," in Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-3, 2017

[9] Sonawane Shamal, Khandave Monika, Nemade Neha, "Secure Authentication for Online Banking Using QR Code,"in International Journal of Emerging Technology and Advanced Engineering,2016