International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Two Way Authentication for Banking Systems

Nupur Shinkar[1], Sanket Sonje[2], Shubham Kamble[3], Pranav Pardeshi[4], Prof. Pooja Dhule[5]

[1,2,3,4](Student, Department of Computer Engineering, MMCOE, Pune, India)
[5](Department of Computer Engineering, MMCOE, Pune, India)

Abstract - *This effort also provides an innovative protection method for validity using the QR code. Which uses two-way authentication by entering passwords and mobile phones that act as logos for authentication. The QR code is very safe because all information that is stored and sent is encrypted. Our smartphone is used to scan the QR code. Scan results generate a string, the mixing number of IMEI telephone numbers that are registered by the user, and any number where any number is generated by random number function. If the network is available on the smartphone, then the string is inserted automatically into the registration page and opens the home page of the bank. Otherwise, a 6-digit Password is created, which must have entered the login page manually and the home page of the bank is enabled for operation. The goal is to establish validation methods using two-factor authentication: Trusted devices (mobile phones) that will print the QR code and act as a user-sign and password.*

Key Words: *Quick Response Code, OTP, Advanced Encryption Standard, IMEI number, Encryption*.

1. INTRODUCTION

Now, almost every day we can do online (banking, shopping, communication), and in this work, our job is that while doing this online, our information is not broken. Of course, methods of cracking security code have become more and more difficult. These powerful systems allow users to work smoothly on the computer. This job is based on the two-way validation system. This QR code provides security. QR code is a quick response code. The system currently has security techniques, such as passwords, user names, fingerprints, and face recognition. But with these techniques, security does not exist until the signal, so there is a need to develop such a secure security system. The QR code is a matrix that contains an array of square poles that is organized in a full squared model. Different sizes of character sizes are provided with four error correction levels. The unit size is measured by the user to allow the creation of a token by many methods. There are two parts in this system. In the input code section, the code is changed to the QR code. In studying and coding, this data is then done after correcting the error code, the final message is structured. Another part is the decoding section. This section decodes the QR code and displays the data contained in the QR code.

2. LITERATURE REVIEW

How to encode QR image was explained by S. Istyaq and his colleagues [3]. It says that nowadays, the world is moving further than the imagination of the persons, progressively, new era in expertise comes which create giant impact on people. Now the discovery of the computer took place, most of the work is accomplished by the computer. In order to guard the vital resource of the public, it is important to make the alteration in previous technology or generate a new one. Level of security such as textual password, biometric etc. is executed. But there are disadvantage i.e. textual password is easy to summon up. Therefore, by using diagrammatical method, we can give the best alternative to the passwords as done in this paper. They offered a system based on the diagrammatical method that uses QR code and the basic procedure is confidential in the levels of encryption in QR code.

Article provides a software response verification system called Snap2Pass which is discovered by Ben Dodson and his mates [8]. This application is comfortable to use, provides security, and does not require a browser. QR system code, a small two dimensional image that encodes digital data. When logged into the server site, it sends the browser on the computer to the encrypted QR code. Users scan QR code with their mobile phone camera, resulting in cryptographic responses sent to the server. A web server has installed a browser on the computer. Their research has shown that Snap2Pass authentication is easier to learn and faster than challenge response systems. From this article we came to know about scanning application for QR code.

Today numerous people are performing online financial transaction. This transaction wants to be secure. There are numerous attacks exist behind this. Phishing is one type of attack. For noticing this attack, several anti-phishing mechanisms are used. In this process, assume that cheater sends out thousands of phishing mails with a link to the forged website. Sufferers click links in email trusting it is genuine. They enter personal information on that false website. Cheater gathers the stolen data and login into accurate website. This is a whole process of phishing. S. Khairnar in his project [2] propose an innovative scheme for online fraud transaction prevention using extended visual cryptography and QR codes. One time password is used for phishing website recognition. The system

provides security for online users and detecting the phishing websites.

Mobile payment is nowadays potentially hazardous. Mobile devices are still unsafe and need more attention in safe areas. This document by T. Purnomo and colleague [1] provides us a mutual verification system between the customer and the dealer using the QR code. QR Code is widely used in current technology. Secure data transmission can be done via QR code. It may contain more material than the old one. This security system is supported by the Public Key Infrastructure (PKI).Using this Public Key Infrastructure will keep the key distribution secure, ensure sender and recipient as a genuine user and guarantee that the data information is confidential. This security system is also strengthened with the addition of QR Code as media of payment. We used this paper for encryption of QR Code using public key infrastructure.

Security is the greatest challenging feature in the internet and network applications. Internet and networks applications are rising very recklessly, so the position and the value of the exchanged data above the internet or additional media types are growing. Therefore the hunt for the finest solution to bid the essential guard against the data stalkers' attacks along with providing these services in time is one of the extreme motivating subjects in the security linked communities. Cryptography is the one of the important categories of computer security that alters information from its normal form into an unreadable form. The two important characteristics that recognize and distinguish one encryption algorithm from another are its skill to protect the secured data against attacks and its speed and effectiveness in doing so. Jawahar Thakur, Nagesh Kumar [7] provides us an AES algorithm details. Later main concern here is the presentation of algorithms in altered settings; the accessible judgment takes into attention the behavior and the performance of the algorithm when diverse data loads are used. The comparison is made in between aes, des and blowfish, we extract the information related to the AEs algorithm from this paper.

3. PROPOSED METHODOLOGY

The philosophy behind the development of the system using the Internet model is that it will allow software developers to take advantage of the previous generation of the system. An important step in developing this system is to start with the introduction of a weak core module and, then, to the needs of the software to improve the system. Using existing systems, developers can identify system failures and develop development by providing new system functions. In each case, the design changes are executed and the new functionality of the system is implemented. This procedure continues until the main goal of ensuring the best security is done. Development includes the steps, steps, alerts, and checklists that provide a system that replaces the existing OTP build system. The QR Code Authentication System allows the operator to enter the password if the operator is verified and the code string is displayed on the screen as a QR code. The user gets authentication if the encrypted string is equal to the IMEI number in the Database.

Figure I. QR- code

Earlier of the QR code there was some primitive authentication methods such as username and password, barcode, fingerprints, face recognition. Security is suffered because username and password are challenged with phishing and difficulty. The barcode limit is up to 20 digits, so complex passwords cannot be generated through barcode. Damaged and broken barcode does not really provide security. Tools and technologies used for fingerprint identification and face recognition are not economically efficient and are beyond specific issues. So to overcome any lack of existing system, the QR code is advised.

QR code is a quick response. It was founded by Denso-Wave, a subsidiary of Japanese car company Toyota in 1994. It can hold up to 4296, which means it can create a modern password. Because it's a two-dimensional bar code, it can be read in any way.

First of all, the user will enter the registration section and submit details such as username, password and IMEI phone number. When the data is verified it will be saved in the database. Data in database server will generate private keys and public keys and save them on the server. From now on, the user will continue to download the software and install it on the phone. When users first use the application, public files and private files are produced and stored in the internal storage of the mobile phone. When registering, if the user does not enter all the values, such as username, password, IMEI number, phone number, and email address, the registration procedure will not be executed. Validation is the most important part of the registration process. If authentication fails, the user will not be able to log in.

4. CONCLUSION & FUTURE SCOPE

This job offers more security with an online banking certificate method. With the username and password. Instead, by creating a QR code, the bank security process

has been improved. Two realistic factors are measured in this system. Using this QR code increases the security during the entry of a specific bank. Depending on the accuracy, only the user can complete the transaction. In the future, you can add voice commands to web apps and Android applications. The scheme of the system of people with visual impairment, where each person will be able to hear the code after scanning the QR code. People with such weaknesses can do it using the text-to-speech feature of the web app.

5. ACKNOWLEDGEMENT

We would like to express our gratitude to Prof. Pooja Dhule, Department of Computer, MMCOE, Pune for her continued support in our project work.

REFERENCES:

[1] T. Purnomo, Y. S. Gondokaryono and C. Kim, "Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure," 2016 6th International Conference on System Engineering and Technology (ICSET), Bandung, 2016, pp. 194-198. doi: 10.1109/ICSEngT.2016.784964

[2] S. Khairnar and R. Kharat, "Online fraud transaction prevention system using extended visual cryptography and QR code," 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, 2016, pp. 1-4. doi: 10.1109/ICCUBEA.2016.7860061

[3] S. Istyaq and M. S. Umar, "Encoding passwords using QR image for authentication," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2016, pp. 818-823. doi: 10.1109/NGCT.2016.7877523

[4] 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

[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] SomdipDey, B. JoyshreeNath and C. AsokeNath "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security" Institute of Information Systems Argentinierstrasse -2009.

[7] Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis " International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011).

[8] Ben Dodson, Debangsu Sengupta, Dan Boneh, Monica S. Lam "secure, consumer-friendly web authentication and payments with a phone",10.1007/978-3-642-29336-8_2

[9] Snehal.Kalbhor,Ashwini.Mangulkar,Mrs.SnehalKulkarni"Android App for Local Railway Ticketing Using GPS Validation".International Journal of Emerging Trends in Science and Tech.,IJETST-Vol-01,Issue-01,Mar-2014,Pages71-74.