ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science
Volume 9 Issue 05 May 2020, Page No. 25023-25028
ISSN: 2319-7242 DOI: 10.18535/ijecs/v9i05.4481

TOTP Based Authentication Using QR Code for Gateway Entry System

[1]Abhishek Arvind, [2]Pradyumna Mahajan, [3]Rishikesh Chalke[*]

[1,2,3]Student, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Mumbai University, Mumbai, India

Abstract:
In today's scenario, there are various ways the attackers can gain access to secure information and use it for their own benefit. In this paper, we aim to introduce a system to improve the existing gateway system by providing more security. This proposed system involves the use of Time-Based One-Time Password (TOTP) with Quick Response code (QR code). A QR code is a 2D matrix barcode where a large amount of information can be stored in a compact manner. TOTP is a temporary password that is active for a short duration of time. For every 30 seconds, a TOTP is generated. A QR code is generated which contains the TOTP. The QR code is scanned and the server checks the TOTP generated on the server-side. If this TOTP matches with the TOTP in the QR code then the user is allowed to enter. This method increases the security of the system and prevents unauthorized access.

Keywords: Authentication, Physical Security, QR Code, Shared Secret Key, TOTP.

1. Introduction

The primary objective of this paper is to introduce a secure authentication method for gateway entry system that complements the one currently in use. The proposed system will use the technological advancements, like QR code, TOTP and Biometrics with the aim of increasing the security and reducing the cost of the system. A comparison of the proposed system can be made with the existing systems used for gateway entry in order to determine its usefulness.

The existing gateway entry systems mostly use Radio Frequency Identification (RFID) [1] technology for gateway entry authentication. While RFID is widely used in the industry, it has certain limitations. For RFID, special RFID chips and RFID readers are needed to be deployed in order to transmit and read the code which increases the cost of the system. Moreover, RFID tags can also be cloned [2] and stolen as there is no way to check who is using the RFID, leading to security getting compromised.

In order to overcome these drawbacks of the existing RFID system, we are proposing a gateway entry system that uses Time-Based One-Time Password (TOTP) with Quick Response code (QR code). QR code can be generated very easily and that too at a very low cost and reduces the user effort as well. The TOTP generated is embedded in the QR code and lasts only for a short duration of time which makes it harder to copy and use. These features make it harder to penetrate into the system and provide more security while decreasing the cost.

2. Literature Review

2.1 QR Code

QR code [3] is basically a barcode consisting a matrix of dots. QR code is used for opening URLs, performing online transactions, storing data of flight tickets and many more applications which reduces user effort and makes the process much easier. The main idea behind the QR code is to create an image so that it can be scanned by a QR code scanner or a smartphone having a QR code reader application and can be translated into meaningful forms of data.

The data stored in a QR code can be alphanumeric, numeric, binary or kanji. All QR codes are square in shape and they have three squares in the top-left, top-right and bottom-left corners which are used for the positioning of the image sensor. The dots in the QR code contain the version, format, and data as well as error correction code. QR code is much more beneficial than barcode as it can be scanned in any direction rather than a particular direction and can contain significantly more data it being two-dimensional in nature [4].

2.2 TOTP

TOTP [5] is a password which is generated using an algorithm that uses the current time and a shared secret key as inputs. TOTPs expire after a short duration of time and therefore offer increased security.

There are certain parameters that need to be followed in order to establish a TOTP authentication. The parameters are as follows:

1. The user and server must know, or be able to derive the current Unix time (the number of seconds elapsed since midnight UTC of January 1, 1970) for TOTP generation.
2. The user and the server must share a secret key.
3. The algorithm must use HMAC-Based One-Time Password (HOTP) [10] as a key building block.
4. The user and the server must use the same time-step value which is 30 seconds by default.
5. There must be a unique shared secret key for each user.
6. The key must either be randomly generated or derived using key derivation algorithms.
7. The keys must be protected against unauthorised access.

After the above-mentioned parameters are established by the user and the server, both the user and the server generate a TOTP value. Further, the server verifies whether the value generated by the user matches with the TOTP value generated locally. Depending on the application, the server may allow the value generated by the user before or after the current time in order to get rid of problems caused by any clock skews, network latency or any kind of user delays.

2.3 Shared Secret Key

Shared secret key [6] is a key that is known only to the parties involved in secure communication. It can be any piece of data, a password, a big number, an array of randomly chosen bytes or a passphrase.

There are two ways of using the shared secret key:

1. The secret key can be shared beforehand between the involved parties. In this case, it is known as a pre-shared key.
2. The secret key can be created during the communication between the parties using some kind of key-agreement protocol. This communication is secure.

There are various uses of this shared secret key. It can be used for authentication between the two parties using various methods like the challenge-response method. It can also be further given to a key derivation function which will, in turn, produce one or more keys that can be used for encryption of messages.

3. Related Works

In this section, we have discussed the related works on One-Time Password (OTP) based authentication systems.

Choudhary et al. [3] proposed an online banking system involving the use of OTP and QR code for payment transaction. In this system, a QR code is generated along with a secret key which is shared by the client and the server and is used to generate an OTP which is embedded in the QR code. This QR code is then scanned and the OTP is verified in order to complete the transaction. So, for each session a new OTP will be generated, thus providing more security.

Uymatiao et al. [6] proposed a multi-factor authentication cryptosystem for the web, based on the established cryptographic standards and web-based protocols. The system they have proposed also makes use of TOTP algorithms for the offline generation of one-time passwords. It establishes a login protected Transport Layer Security (TLS) tunnel and the seed is exchanged through it. The seed exchanged is stored locally. The system authenticates through the correctness of the seed for the verification of the one-time password. This ensures multi-factor authentication resulting in increased security.

4. Working

There are six steps involved in the working process: registration, verification, login, TOTP generation, QR code scanning and entry.

4.1 Registration

The app would ask the user to register using their authorised email ID and password which will be used for login. This is expected to be done over a secure connection using a protocol like TLS [7].

TLS establishes a secure connection with symmetric cryptography which is used for encryption of the data to be transmitted. Shared secrets which are both secure and reliable are used for this process. It authenticates the identity of the communicating parties with public key cryptography. Message authentication code is used for preventing undetected loss or alteration of data while transmitting it.

4.2 Verification

On successful registration, a verification email is sent to the authorised email ID. After verification, login rights are granted to the user.

4.3 Login

In the login step, the user is able to login only if the account is verified. On first login, a shared secret key is generated. The shared secret key is a random alphanumeric string which is stored under the authorised email in the server and a copy is sent to the app. The user is also asked to setup a biometric authentication so as to prevent unauthorised access of the app.

4.4 TOTP Generation

The shared secret key is now used to generate TOTPs. This is done using the HMAC-SHA1 [8] algorithm. HMAC-SHA1 is a Hash-based Message Authentication Code which uses SHA1 as the hashing algorithm. It is used to hash a message using a secret key. The secret key would be the shared secret key received from the server and the message to be hashed would be the counter value that is required for OTP algorithms. In case of TOTP, the counter value would be based on the number of 30-second time increments that have taken place since the Unix Epoch. The HMAC-SHA1 function can be given as:

$$\text{SHA1 (outer pad + SHA1 (inner pad + counter))}, \quad (1)$$

Where inner and outer pads are formed from the secret key and can be given as:

$$\text{Inner pad} = (\text{secret key}) \oplus \text{0x36} \qquad (2)$$

$$\text{Outer pad} = (\text{secret key}) \oplus \text{0x5C} \qquad (3)$$

The hash generated from the HMAC-SHA1 function is used to form TOTPs which are 6-digit numbers ranging from 000000 to 999999. These TOTPs are embedded in the QR codes which are used in the next step.

4.5 QR Code Scanning

In this step, the QR code is scanned using a QR code reader. The QR code contains the TOTP and the user ID. This TOTP is compared with the TOTP generated in the server.

4.6 Entry

This is the final step of the working process in which, if both the TOTPs match, then entry is granted to the user, or else entry is denied.

The following two figures illustrate the working of the gateway entry system.

- Figure 1 represents the login or registration phase.
- Figure 2 represents the TOTP generation and QR code scanning phase.

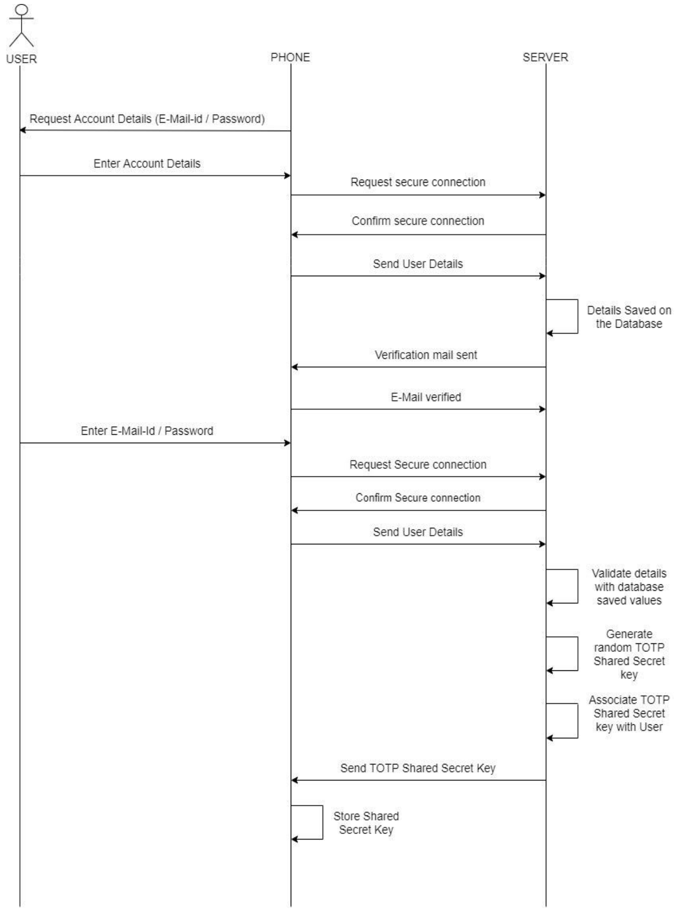

USER
PHONE
SERVER
Request Account Details (E-Mail-id / Password)
Enter Account Details
Request secure connection
Confirm secure connection
Send User Details
Details Saved on the Database
Verification mail sent
E-Mail verified
Enter E-Mail-Id / Password
Request Secure connection
Confirm Secure connection
Send User Details
Validate details with database saved values
Generate random TOTP Shared Secret key
Associate TOTP Shared Secret key with User
Send TOTP Shared Secret Key
Store Shared Secret Key

Figure 1: Login or Registration Phase

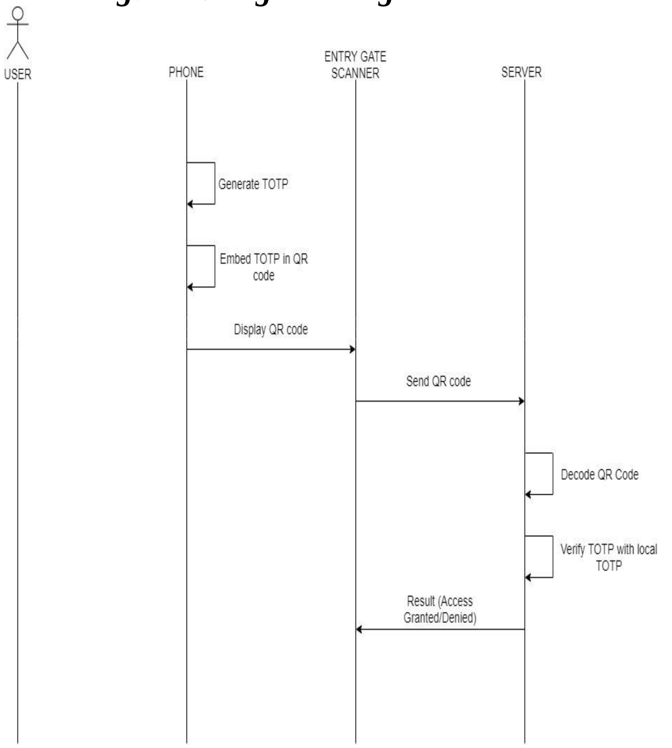


Figure 2: Totp Generation and Qr Code Scanning Phase

5. Implementation

The implementation of the gateway entry system can be explained as follows:

- Figure 3 depicts the login or registration page. Here, the user is required to enter the authorised email ID and password in order to login. First time users need to register in order to proceed.
- Figure 4 depicts the email verification page. After registration, a verification email is sent to the authorised email ID. Upon verification, the user is allowed to login.
- Figure 5 depicts the QR code scanning page. Once login is done, the shared secret key is sent to the user and also stored in the app. This key is used to generate the TOTP which is embedded in the QR code. The QR code is then scanned using a QR code scanner. This TOTP is then compared with the TOTP generated in the server.
- Figure 6 depicts whether the user is granted entry or not. If both the TOTPs match, then the user is allowed to enter, otherwise entry is not allowed.

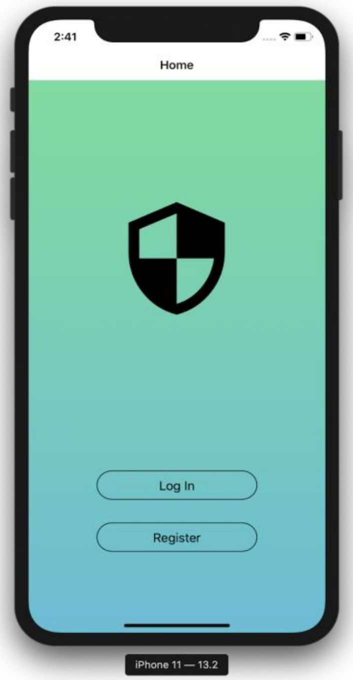
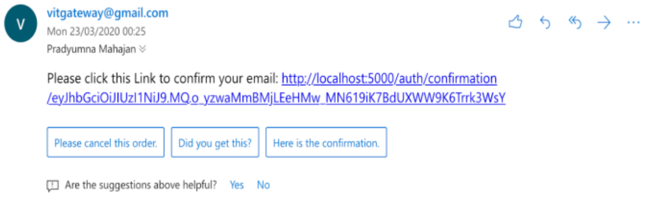


Figure 3: Login or Registration Page



vitgateway@gmail.com

Mon 23/03/2020 00:25

Pradyumna Mahajan

Please click this Link to confirm your email: http://localhost:5000/auth/confirmation /eyJhbGciOiJIUzI1NiJ9.MQ.o_yzwaMmBMjLEeHMw_MN619iK7BdUXWW9K6Trrk3WsY

V
Please cancel this order.
Did you get this?
Here is the confirmation.
Are the suggestions above helpful?
Yes
No

Figure 4: Email Verification Page

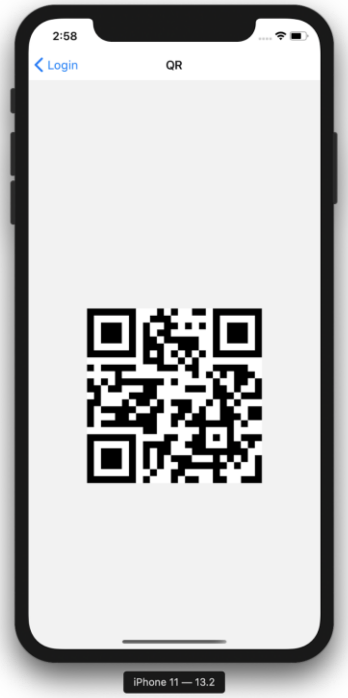


Figure 5: QR Code Scanning Page

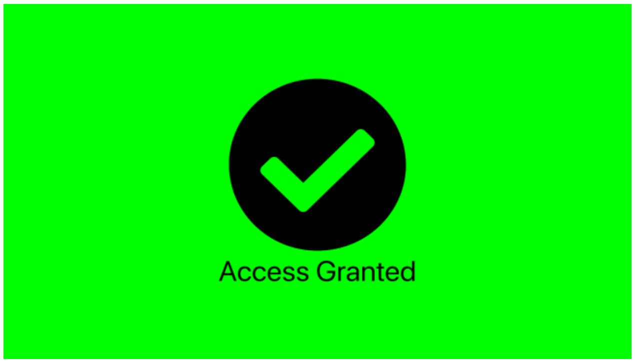


Figure 6: Entry Page

6. Analysis

Comparison of this physical gateway entry system can be done with two other systems:

1. Security Personnel based authentication system
2. RFID based authentication system

The proposed system is better than having Security Personnel as:

- It does not require a person to be always present; a turnstile can be used instead.
- It is cheaper and reliable.
- Forging identification is not possible as the passwords change every thirty seconds.

There are two types of RFID systems. One is Contact-less smart cards which use high frequency RF technology (13.56 MHz) and the other is Proximity badges which uses low frequency RF technology (125 kHz) [9].

The proposed system is better than Contact-less smart cards and Proximity badges because:

- No specialized equipment such as RFID tags or RFID readers are required. A smartphone with a camera can take the place of a RFID reader.
- Unlike RFID tags, if the smartphone is stolen/gets lost, it cannot be used to enter secure premises as a password is required to open the app.

The proposed system is better than Proximity badges also because:

- In proximity badges, the distance between the badge and reader needs to be 3 inches or less for reliable badge reads.
- Proximity badges are susceptible to high levels of electromagnetic fields which can lead to the destruction of the badges.
- Reader placement (on metal vs wood) can have an adverse effect on the “read” distance between the badge and the reader in case of proximity badges.

7. Conclusion

TOTP based authentication using QR code for gateway entry system was built in order to provide more security at a cheaper rate. Unlike the RFID based system, in which the RFID tags can be stolen and used and the devices used increases the cost of the system, TOTP authentication using QR code not only increases the security at a lower cost, but also reduces the user effort.

We hope that our approach of using TOTP based authentication will help to further improve and focus on the domain of security, introducing new methodologies to prevent attacks on the systems which is very much required today.

8. Acknowledgment

The authors would like to thank Dr. Dilip Motwani and the entire faculty of Department of Computer Engineering, Vidyalankar Institute of Technology, for their valuable support and guidance and to all those who helped in the completion of this research project.

9. References

[1.] D. Mehendale and R. Masurekar, "A Comparative Study of Different Technologies for Electronic Toll Collection System," IJIRCCE, vol. 4, Issue 2, February 2016, pp 1532-1538.

[2.] T. Kasper, I. von Maurich, D. Oswald and C. Paar, "Cloning Cryptographic RFID Cards for 25$."

[3.] A Choudhary, S. Rajak, A. Shinde, S. Warkhade, Prof. F.S. Ghodichor, "Online Banking System using Mobile OTP with QR-code," IJARCCE, vol. 6, Issue 4, April 2017, pp 657-661.

[4.] Jose Rouillard, "Contextual QR Codes", Proceedidngs of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI 2008), Athens, Greece, July 27-August 1, 2008.

[5.] D. M'Raihi, S. Machani, M. Pei, J. Rydell, "Totp: Time-based one-time password algorithm," Internet Engineering Task Force, RFC:6238,2011. [Online]. Available: http://tools.ietf.org/html/rfc6238

[6.] M. L. T. Uymatiao, W. E. S. Yu, "Time-based OTP Authentication via Secure Tunnel (TOAST): A Mobile TOTP Scheme Using TLS Seed Exchange and Encrypted Offline Keystore," IEEE, 2014, pp 225–229.

[7.] T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force, RFC: 5246, 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[8.] H. Krawczyk, M. Bellare, R. Canetti, "Hmac: Keyed- hashing for message authentication," Internet Engineering Task Force, RFC: 2104, 1997. [Online]. Available: http://tools.ietf.org/html/rfc2104

[9.] Pearson R. "Electronic security systems: A manager's guide to evaluating and selecting system solutions," Elsevier, Apr 1 2011.

[10.] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O.Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," Internet Engineering Task Force, RFC:4226,2005.[Online].Available: https://tools.ietf.org/html/rfc4226