International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Offline Transaction System using TOTP

Shrusti Sangodkar, Claren Rodrigues, Sherwin Rodrigues, Tecwin Rodrigues, Basil Jose

Abstract- ***This paper proposes a new system which can be used to make short distance transactions Offline. The method discussed in this paper provides an in depth explanation of the project and how TOTP (Time-Based One Time Password) is used to carry out authentication which is completely offline. This idea is implemented since there is no current system which facilitates offline payments to occur. The project uses various functions such as Hashing (using SHA-1) and Audio QR to ensure security while it works offline. The project employs a QR code which encodes the user's ID, TOTP token and the amount to be transferred to the receiver. The receiver then scans the QR code and decodes the contents, authenticates the user, checks the balance, if it is sufficient then the transaction occurs successfully. This system can be used in different scenarios such as shopping, travelling, restaurants etc.***

Keywords: Audio QR; HMAC-SHA1; HOTP; Offline; OTP; TOTP; Transaction; QR-Code

I. INTRODUCTION

With the wide use of the Internet and the development of E-commerce, today almost most of the transactions occur via the Internet. Transactions are made by people on a daily basis for a wide variety of reasons such as-

- Shopping
- Travelling
- Hotels
- Booking tickets
- etc.

For a transaction to occur successfully, there must be a good and secure Internet connection, without which the transaction can fail and the user could not get the item that they desired, or even worse, might lose their money.India is a country where almost everybody faces the network problems on a daily basis, mostly while travelling in the rural areas, forests or anywhere where there isn't a proper network system. In such a case, if the user is on their devices, trying to make an important transaction, this sudden loss of the connection will definitely be dangerous. In this paper, a method for an Offline Transaction System of currency for short distant transactions is introduced. An application will be designed for the user as well as the receiver.

Revised Manuscript Received on June 08, 2020.
* Correspondence Author
Shrusti S. Sangodkar*, Student, Department of Computer Engineering, Agnel Institute of Technology and Design, Assagao, Goa, India.
Claren Dominic Rodrigues, Student, Department of Computer Engineering, Agnel Institute of Technology and Design, Assagao, Goa, India.
Sherwin Rodrigues, Student, Department of Computer Engineering, Agnel Institute of Technology and Design, Assagao, Goa, India.
Tecwin Rodrigues, Student, Department of Computer Engineering, Agnel Institute of Technology and Design, Assagao, Goa, India.
Prof. Basil Jose, Assistant Professor, Agnel institute of Technology and Design, Assagao, Goa, India.

The user will have to register on the user app or using the website. The user then connects his/her wallet with this account. This part requires the Internet. Once this is done, the user is able to make offline transactions. Whenever an offline transaction is to be made, the user will use the application to generate a QR code which will contain the User's registration ID, the amount in the wallet stored locally, the shared secret key and the TOTP generated. The receiver will scan this code and will try to validate the TOTP, check for availability of sufficient balance, deduct the amount and send an audio QR once the transaction is done successfully.

Our system is based on the use of various techniques ranging from Cryptography, QR code generation, TOTP and Audio QR.

This system can be divided into 4 parts

a. User creating an account on the app and getting registered.
b. Once the user wants to do a transaction:
   - The generation of the TOTP
   - Generation of QR
c. The receiver scans the QR for validation.
d. Generation of Audio QR(acknowledgement).

II. RELATED WORK

The algorithm used in this project is TOTP [2] which is used for the offline authentication purpose. This project also uses QR code [6] generation in order to encode the details which are then scanned and decoded.

A related project was Digital Bus Pass Using QR-Code [5] in which it makes use of databases to store the user's data. The system helps the user to get their passes online instead of waiting in long queues this saves their time. Users can deposit money into their account and also if the bus pass is expiring extend its validity.

Audio QR Codes for Voice Service Position Sharing [12] is another such project which uses Audio QR that determines exact positions of devices without the use of Internet or any high end devices. They introduce the audio-based sharing for the spoken Web. This has benefits in underdeveloped regions where textual literacy, income and data connections are low.

III. METHODOLOGY

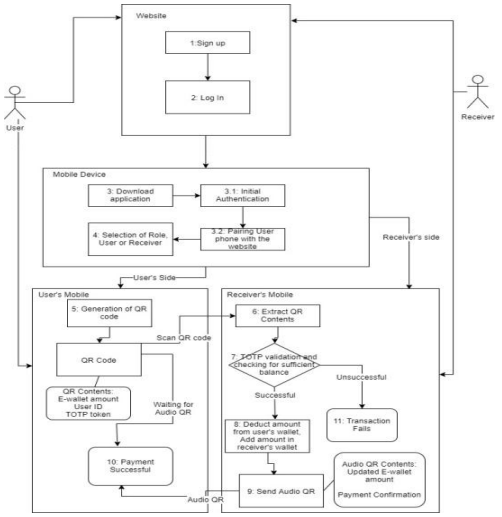

Figure 3.1: Project Flow

The Figure 3.1 shows the overall flow of how the project will be. The flow of the project can be divided into 3 blocks, the first block shows the registration process of the user and the receiver, the second block shows downloading of the application and selecting a the role of the user or the receiver. The third block explains the Transaction process that will take place between the user and the receiver.

1. Account Registration

The user has to create an account on the website before accessing the application. While creating the account, the user has to use his/her phone number or email ID and a valid password, along with necessary details such as first name and last name. The user will also have to link his/her existing E-Wallet to this account, if not, then the user should fist create an E-Wallet and then try to register to this Website. After the registration is successful, the user will get a confirmation, confirming their registration and the user is now able to download the application and access all the feature it offers.

Similarly the receiver has to register on the website connecting his/her E-Wallet and other necessary details. They must then specify the occupation for which the transaction process is to be used.

2. Log In

Once the user/receiver creates an account, they must log into their account, in order to complete the confirmation of their email account and E-Wallet. This step is crucial for security reasons.

3. Downloading the Application

The user as well as the receiver will have to download the application on their mobile devices. There should be sufficient amount of memory present on their devices.

3.1 Initial Authentication

Once the download is complete, they should log into their respective accounts using the correct username and password. If the password and usernames are registered on the website then the login will be successful

3.2 Pairing User Phone with Website

The user must then click on the generate QR option on the website, while initially registering on the application. This is done so that the user will get his/her shared secret key. The website will then generate the QR code containing the shared secret key and other necessary details such as the user ID and Wallet ID. Once the user scans the QR with his/her device, then the user will be successfully able to use the application.

Figure 3.2 QR Code

4. Selection of Roles

Then they should choose the appropriate role, i.e., whether they are the user or the receiver.

On choosing the user role, the user will be able to generate a QR code whenever he/she wants to do a transaction. On choosing the receiver role, the receiver will be able to scan the QR code generated by the user.

5. Generation of QR Code

Once the user clicks on "Generate QR"[6] option on the application, a QR code containing the user's ID, Local wallet balance and the TOTP token[9], is generated.

- User's ID: The User's ID is a unique value given to the user during registration. This value is an important element while creating the QR code because it guarantees the credibility of the user.
- Local Wallet Balance: The user has to use a local wallet which stores the amount present in the original E-Wallet when the user is connected to the Internet. The local wallet balance needs to be updated within 24 hours, without which the account of the user will be blocked. The account can then be recovered once the user connects back to the Internet. This ensures consistency of the data in the wallets.
- TOTP token: The TOTP[9] token is generated using two parameters, the shared secret key, K and the Unix or the epoch time of the instance when the user is generating the QR code. TOTP ensures that the QR is valid only for a certain amount of time after which it will be invalid.

6. QR Code Extraction

The receiver scans the QR code and uses extraction methods to extract the information encoded within the QR code. If the scanning is done correctly, then the receiver will obtain the three parameters, the user ID, the TOTP token and the E-Wallet balance of the user.

7. Validation

The most important part in this whole offline transaction process is validation, without which the transaction is bound to fail as well as various security and credibility concerns of the whole project arises.

Retrieval Number: E9795069520/2020©BEIESP
DOI: 10.35940/ijeat.E9795.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

As soon as the QR code is scanned, the receiver must validate that the user is in fact using a valid account to make transactions and also that his/her wallet has sufficient balance available to pay.

7.1 TOTP Validation

Once the receiver decodes the QR code, they will try to first validate the user based on the token value which was generated using the TOTP algorithm [9]. After decoding the QR code, the receiver has the user's token, the user's pay balance of the local wallet and the user's registration ID. The receiver tries to generate the same token using the epoch time and the shared secret key. There might be a time gap while doing this, so the time is given a compensation of ±5 seconds at the least. Once the receiver gets the user's token, the tokens are compared, if they match, the transaction is a valid transaction, else the transaction is invalid.

7.2 User Balance validation

There must be sufficient amount of balance available in the user's local wallet, without which the transaction will surely fail. This is done when the QR code is decoded. The balance in the wallet is a part of the QR code. So if the amount of money in the wallet is less than the amount to be paid, then the transaction fails.

8. Updating the Wallet Balance

Once the validation is successful, the amount will be added in the local wallet of the receiver and will be deducted from the local wallet of the user.

9. Audio QR Generation

An audio QR [12] will be generated on the receiver's device. The audio QR will contain the amount that is to be deducted for the user's E-wallet.

10. Audio QR as Acknowledgement

An audio QR [12] is sent to the user as an acknowledgement if the transaction is successful, which also contains the amount to be deducted from the user's local wallet. Using this information the local wallet amount is deducted.

11. Failure of a Transaction

In case the transaction fails, which may be due to invalid TOTP or insufficient balance in the Wallet, the Audio QR will not be generated and the user will have to try again by generating a new QR code[6], or by updating the balance in his/her wallet if there is a network connection available.

IV. RESULT

The transaction process takes about minimum 10 seconds to maximum 15 seconds to be completed successfully. The following images are the screenshots of the application being used to do a transaction.

Figure 4.1 shows how the user generates the QR code on their device. The QR code is generated offline. *Figure 4.2* shows how the receiver is able to choose an option to scan the QR generated by the user. *Figure 4.3* demonstrates how the receiver scans the QR code from the user. Finally, *Figure 4.4* shows the receiver entering the amount to be paid by the user. After clicking on the confirm button, the transaction is successful and a message is displayed on the screen.

Figure 4.1: User clicks on pay now and a QR code will be generated containing the TOTP token, E-Wallet(Local) Balance and the user ID

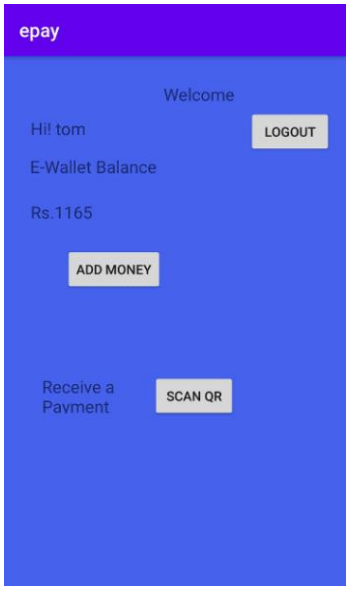

Figure 4.2: Receiver clicks scan QR to Open Scanner

Figure 4.3: Receiver scans the user's QR code

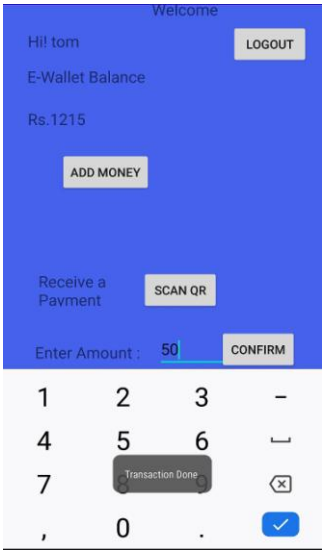

Figure 4.4: Receiver enters the amount to be paid and the money gets added in their wallet

V. CONCLUSION

In conclusion, the Offline Transaction System, with the help of TOTP can be used to make payments without the existence of a network and can be made more secure using the concept of TOTP.

The project emphasizes on the various network issues faced while processing an online transaction and aims at minimizing the transaction failures by introducing an Offline transaction system. Using the concept of TOTP is considered much better than the HOTP [3] because it uses a unique time stamp along with a shared secret key. This enhances the security in the transaction process. Audio QR is used to give an acknowledgment because it doesn't require a network to be established before transferring any data across two devices.

The scope of this project is to create a system which is capable of doing an offline transaction. The project aims at storing a local wallet on the user's device, generating the QR code[6] using this and various other factors such as time, shared secret key and identity to make the transaction secure, scanning the QR code, Validation of QR code, Deduction of amount in the wallet, generating an acknowledgment using the Audio QR[12]. Further development could be done to improve the encoding and the security or the system. QR code scanning process can be eliminated by introducing a better alternative. This system can facilitate a contactless payment. This will ensure that no viruses of infectious disease will be spread via paper money.

REFERENCES

1. https://www.mobilefish.com/download/iota/iota_part34.pdf
2. D. M'Raihi, S. Machani, M. Pei and J. Rydell, TOTP: Time-based One-time Password Algorithm, http://tools.ietf.org/html/
3. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, Gemplus, O.Rane, RFC4226, HOTP: An HMAC-Based One-Time Password Algorithm,http://tools.ietf.org/html/.
4. Sukhjeet Kaur , QR code Security and Solution, Department of Computer Science and Engineering, Adesh Institute of Technology, Volume 7 Issue No.4.
5. Snehal Banale ,Prajakta Dudhade , Rajshree Pal, Sayali Patil and
6. Prof.Sneha Jagtap, Digital Bus Pass Using QR Code, Department of Computer Engineering, APCOER, India, Volume 06, Issue 05, May 2017, ISSN: 2278 -7798.
7. Phaisarn Sutheebanjard, Wichian Premchaiswadi, QR code Encoding, https://www.researchgate.net/publication/251987247
8. Jennifer Pearson, Simon Robinson, Nitendra Rajput, Matt Jones and Amit Nanavati, Audio QR Codes for Voice Service Position Sharing, FIT Lab, Swansea University, SA2 8PP, UK, IBM India Research Lab, Vasant Kunj, New Delhi, 110070, India.
9. Sangeeta Singh, QR Code Analysis, M.Tech, Department of Computer Science and Applications, KUK, Haryana, India,Volume 6, Issue 5, May 2016 ISSN: 2277 128X.
10. Wikipedia , Time-based One-time Password Algorithm, http://en.wikipedia.org/wiki/-based_One-time_Password_
11. https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology
12. https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm
13. Jennifer Pearson, Simon Robinson, Nitendra Rajput, Matt Jones, Amit Nanavati; Audio QR Codes for Voice Service Position Sharing; FIT Lab, Swansea University, SA2 8PP, UK and IBM India Research Lab

AUTHORS PROFILE

Shrusti S. Sangodkar is pursuing her Bachelor of Computer Engineering at Agnel Institute of Technology and Design, Assagao-Goa. Her interests include WEB DESIGNING, ETHICAL HACKING, BIG DATA ANALYTICS and DATABASE MANAGEMENT. The projects she has worked on till date include developing a website for Ration card services and Game Development(Pong) using HTML canvas and JavaScript. She has also worked on Bolt IoT, App development and Computer Networking. She is also a member of the IET(Institution of Engineering and Technology).

Claren Dominic Rodrigues is currently pursuing his from Agnel Institute Of Technology And Design Assagao, Goa. He has attended workshops on web development and Robotics. He has also worked with IOT's, Game development using UNITY software, Firebase and AI. He has done mini projects on web development that is CRIME RECORD MANAGEMENT SYSTEM and LIBRARY MANAGEMENT SYSTEM. He had also done mini projects using BOLT IoT to solve the day-to-days problems, such as a Temperature monitoring

Sherwin Rodrigues is a student within the Computer Engineering program at Agnel Institute of Technology and Design. He will graduate with a Bachelor's degree in Computer Engineering in 2020. His research interests include Cloud Computing, Network Security and mobile payments. He has also worked and developed IoT devices, some of which are air quality monitoring system and temperature logging system.

Tecwin Rodrigues is a student within the Computer Engineering program at Agnel Institute of Technology and Design. He will graduate with a Bachelor's degree in Computer Engineering in 2020. His research interests include Web Development, Big Data Analytics and Cloud computing. He has also worked and developed small website like weather forecasting website

Prof. Basil Jose has completed BE in Information Technology & ME in Computer Science & Engineering from Goa College of Engineering. Currently working as Assistant Professor at Agnel institute of Technology and Design. Has 6 international publications & 2 national publications. Life member of Indian Society of Technical Education.