International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-9, Issue-12, 2022 Regular Edition E-ISSN: 2349-7084

Online Banking Using QR Authentication

Kranthi Kiran[1], Rakesh[2], D Saidulu[3]

[1,2] *UG Student, Department of Information Technology, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.*

[3]*Associate Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India*

Email ID: kranthikiran2255@gmail.com[1], rakeshkorakoppu999@gmail.com[2], fly2.sai@gmail.com[3]

Corresponding author : ***D Saidulu***

Available online at: http://www.ijcert.org

Received: 28/10/2022, Revised: 21/11/2022, Accepted: 24/12/2022, Published: 30/12/2022

Abstract:. Every year, thousands of users face issues with scammers and lose their money. Most of them are because of cracked UPI pins, and some are because of OTP sharing. Cyber fraud is increasing exponentially as a high-speed infrastructure is developed. This is causing insecure transactions for various payments done through different payment gateways. QR (Quick Response) code is versatile and is used in various fields, such as online banking, managing attendance, and for security applications. It is a 2-D matrix bar code where the information is stored in both horizontal and vertical dimensions. Here we would like to improve the security channel by adding QR generation while making transactions, which helps prevent fraud and loss of personal information.

Keywords: UPI, Cyber frauds, Payment Gateways, Quick Response (QR) Generation, Bar Code.

---

1. Introduction

It is amazing to see technology reaching new heights. With the rapid advancement of technology, there is a significant amount of risk that should be avoided. Considering the factors of banking, which have kept on changing in recent decades, it is important to upgrade the security level for online banking to be secure. The One-Time Password (OTP) is a revolutionary and very useful change in the field of online banking. It comes with a great security feature where the user will get the new password as text every time he tries to make a new transaction. Yet because of the present scammers, the OTPs have been found out and the transactions have become insecure. It became insecure because the scammers called the customers, asked for OTPs, and made unauthorized transactions. Even though there have been a lot of advertisements and knowledge sharing across various fields, it is still happening in various parts of the world, and the number of text OTPs has greatly increased. Users sometimes cannot categorize the OTPs in the fast-moving world. So the introduction of QR codes as an OTP for online banking will be helpful and will lessen the risks of insecurity in payment infrastructure because QR codes are machine-readable but not human-readable.

The motivation of the paper is In the existing systems, using just the OTPs in text for the transactions has resulted in so many cybercrimes in various parts of the world. The primary cause of the majority of cybercrimes is the sharing of OTPs. Scammers take advantage of people's lack of awareness, focusing primarily on the illiterate and elderly. The issue here is that the customers who are sharing the OTPs are doing so only because they can read and understand the OTP as it is in text format.

So our paper suggests the use of QR codes for OTPs instead of text OTPs. As the QR code is machine-readable, even if a hacker or scammer tries to steal the money, the customer or user cannot share the OTP because it is in QR format. The transaction process will be similar to the existing process except that the text "OTP" is replaced by the OTP hidden in the QR code.

The remaining paper is organized as follows: Section 2 represents a literature review; Section 3 presents a proposed model; Section 4 presents a result analysis; and Section 5 presents concussion.

2. Literature Review

In this paper [11], Mobile money applications are thriving due to the ease and convenience they bring to people, where they offer to transfer money between people's bank accounts or cards with a few taps on a smartphone, either through mobile banking or mobile payment services. However, gaining user adoption of mobile banking and payments is hampered by customers' lack of trust in the security of the services, which makes sense given that whenever people grant service access to their debit or credit cards or bank accounts, they open the door to identity theft, fraudulent transactions, and stolen money. Add to that the fact that people and developers are already ignoring the security aspect of applications. This paper consists of two parts: first, an intensive security analysis of a selection of different mobile banking and mobile payment applications on the Android platform, where 80% of the selected applications were found not to follow the best security measures. And second, a thorough step-by-step Android security testing guide in the form of this paper to ease the process of security testing any Android application to be used by developers, ethical hackers, and anyone interested in testing the security of any application.

According to this paper [12], mobile phones have become an inseparable companion for many users, serving far more than simply as communication tools. In developing countries, the number of mobile phone users outnumbers the number of bank account holders. Besides, the low banking service penetration and, therefore, the massive migrant communities are another issue in utilizing mobile phones for payment functions. Therefore, mobile payment might achieve the success it's targeting simply and far quicker than in developed countries. There are lots of variables associated with mobile payments. During this paper, the varied models used for mobile payments are briefly mentioned. Then, the paper can propose a state of affairs for mobile payment that tackles each consideration of the method, namely: speed of group action and security, without complicating the method or making it undesirable to users.

The author of this paper [13] explains the implementation details of the online banking authentication system. Security is an important consideration for online banking applications, which may be enforced by various web technologies. While implementing an on-line banking system, secure information transfer is accomplished through the use of https information transfer and information encryption techniques for secure storage of sensitive information. We intend to use the concept of QR-codes with robot applications to eliminate the threat of phishing and to validate user identity. The QR-code, which can be scanned by the user's mobile device, overcomes the shortcomings of an old countersign-based mostly system. We can improve security by utilizing only once the countersign (OTP) that is hidden within the QR code.

In this paper [14], financial tasks are being engaged in the internet field as a high-speed internet infrastructure is developed and people are informed. However, the existing internet banking system was exposed to the danger of hacking. Beyond stealing a user's ID and password, personal information has recently been leaked via a high-level method such as phishing or pharming. Seeing that most of the examples that happened in domestic financial agencies were caused by the appropriation of ID or passwords belonging to others, a safe user confirmation system becomes much more essential. In this paper, we propose a new online banking authentication system. This authentication system used mobile OTP in conjunction with a QR-code, a 2D barcode variant.

In this paper [15], with the rapid advancement of technology, the QR Code has a wide range of applications. A QR Code is a second matrix Universal Product Code that stores data in both horizontal and vertical dimensions. QR Code will hold a bigger quantity of information in a smaller area, perform reliable error correction at a higher speed, and have a quicker latency. The increasing use of sensible phones among all age groups made accessing QR Codes easier by providing end-user content along with net links, personal details, etc. QR Code is flexible and is employed in various analysis fields like online banking, group action management, health care, facilitating visually impaired folks, and security applications like totally different styles of cryptography and steganography. Secure authentication is achieved using victimization data-hiding algorithms and the embedded QR Code. This paper focuses on the security aspects handled by QR Code in various applications and more directly addresses the secure transportation of information via SQRC, which has real-time applications such as vehicle and identity verification.

3. Proposed Model

We propose a new authentication system for online banking which can provide greater security and convenience by using QR-code .The importance of security and ease of use is like two side of a coin. It cannot be provided considering that show up on one side. Therefore, we should always seek for safety devices to meet all ease and security of electronic financial services. We are using QR Code . It is a matrix code developed and released primarily to be a symbol that is easily interpreted by scanner equipment. It contains information in both vertical and horizontal directions, whereas a 1D barcode has only one direction of data (usually the vertical one) [1].QR Code also has error correction capability. Data can be restored even when some parts of the code are distorted or damaged. Compared to a 1D Barcode, a QR Code can hold greater volume of information: 7,089 characters for numeric only, 4,296 characters for alphanumeric data, 2, 953 bytes of binary (8 bits) And 1,817 characters of Japanese Kanji/Kana symbols. B. Usage without a machine, it’s impossible for a human to manually decode QR Codes . We attach a QR code for online transaction.[1].It provides security by ensuring that user cannot use same password again and again [2].It also offers other characteristics like anonymity, portability, extensibility and enable to keep information safe or from being leak [4].There are two approaches for generating an OTP:

Figure 1. Sample QR Code

1. Time based OTP- In these OTP changes at frequent interval of time.
2. Event based OTP- In these OTP will be generated by pressing a button on the OTP device or token.

4. Implementation

Implementation in this is quite similar to text OTP system. We are just trying to replace the text with a more secure system i.e, QR code [5].The OTP will be hidden in the QR code and can't be revealed until it is scanned. OTPs will be secure because they are in machine readable format. QR code se will be received by the user and then can be scanned for making a payment successful.

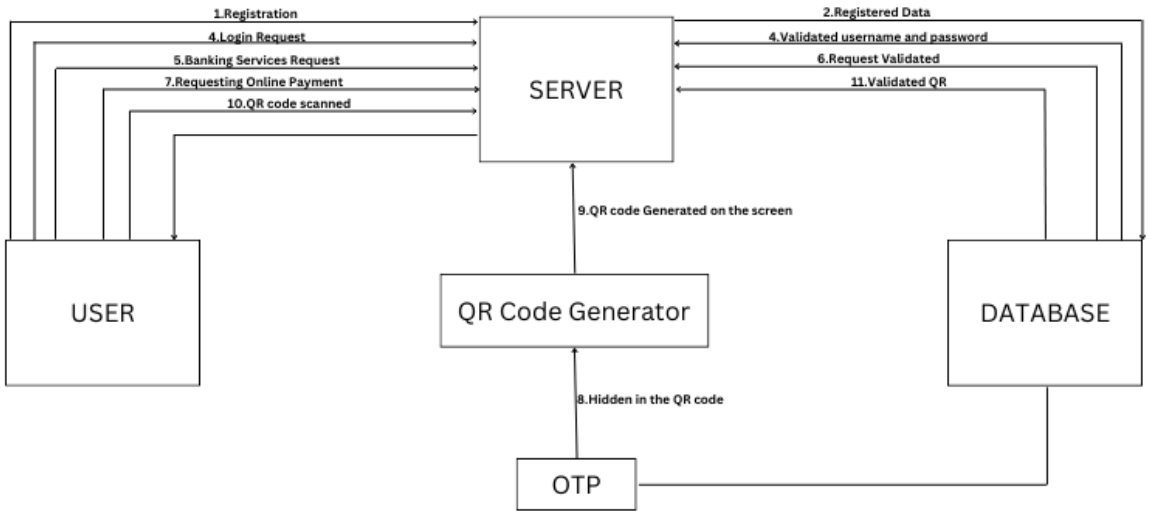

Figure 2. Architecture Design

Working of System:

Our system consists of 4 phases:

1. Initial Phase
2. QR Code Generation Phase
3. Validation Phase
4. Payment Authentication Phase

- Initial Phase: Here the data of user is stored into the database for verification of login details in further process.
- QR code Generation Phase : When the payment is requested by the user then the QR code will be generated and will be sent to the user and will be used as OTP
- Validation Phase : When the OTP is scanned by the user, the server will validate the OTP with the database and sends the acknowledgement.
- Payment Authentication Phase : If the OTP is matched the payment will be successful else it will be redirected to the second phase.

5. Security Analysis

The QR code generation helps in increasing the security of the payment then the existing system by decreasing the chances of getting attacked by the scammers [6].

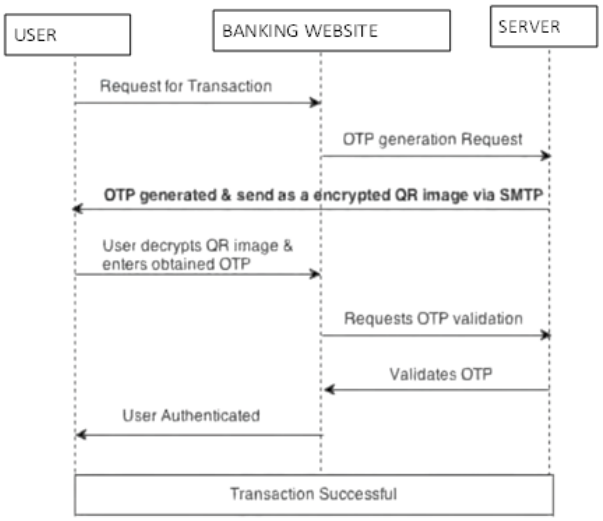

Figure 3. Sequence Diagram for Authentication System

OTPs are transmitted in the form of an image which makes it complex for intruder to detect the presence of secured information [6].OTP is send to the concerned user through an email message. Banking users can conveniently access their email accounts and obtain the QR code containing the encrypted OTP [7].Usage of AES algorithm for encrypting one time password further enhances the security of the system [8].Proposed scheme has higher degree of complexity than all existing systems and clearly the time required to crack the scheme will be more than the useful lifetime of OTPs [9].OTPs are generated for a session and have a short lifetime. It's not possible to use the OTP after their expiry [10].Popularity of QR codes makes the method user friendly.

Figure 4. Scanning QR Code

6. Results

Once the QR code is generated, we need to scan the QR for proceeding into the payment. If the hidden OTP in QR and the original OTP is matched, payment will be successful. The QR code should be scanned in the given time interval

Figure 5. Payment authentication

7. Conclusion

This paper concludes that using QR codes for banking authentication will protect users from scammers. As the use of QR codes expands across industries, they will become more user-friendly and faster than existing systems. The highly secured banking field can be made more secure by using QR. This system does not require any technical pre-requisite, which makes it user-friendly. The future enhancement of this research is that the mobile camera and banking server integration will be securely made, and in further updates the security layers will be improved to the next level, which will help the user with a scam-free payment environment. We can also create an application that will assist users in monitoring QR codes and deleting them as needed so that they can keep track of recent scans.

References

[1] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005.
[2] Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking", NSPW"07, North Conway, NH, USA, Sep. 18-21, 2007.
[3] Sang-Il Cho, hoonjae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.
[4] Amandeep Choudhary, Shweta Rajan, Akshata Shinde, Siddeshwar Warkhade, Prof. F.S. Ghodichor, "Online Banking System using Mobile-OTP with QR-code", IJARCCE, vol.6, 4 April, 2017.
[5] ISO/IEC 18004:2000 – Information Technology – Automatic Identification and Data Capture Techniques – BarCode Symbology – QR Code, 2000.
[6] Abhas Tandon, Rahul Sharma, Sankalp Sodhiya, P.M.Durai Raj Vincent, "QR code based secure OTP distribution scheme for Authentication in Net-Banking", International Journal of Engineering and Technology,5(3):2502-2505, June, 2013.
[7] Qiu-xia Wang; Tie Xu; Pei-zhou Wu, "Application research of the AES encryption algorithm on the engine anti-theft system," Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on, vol., no., pp.25,29, 10-12 July 2011.
[8] J. S. Tan, "QR code," Synthesis Journal, Section 3, pp. 59-78, 2008.
[9] 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.
[10] Jose Rouillard, "Contextual QR Codes", Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-August 1, 2008.
[11] Bwalya, M., & Chembe, C. (2020, February 21). A Security Framework for Mobile Application Systems: Case of Android Applications. Zambia ICT Journal, 3(2), 31–43. https://doi.org/10.33260/zictjournal.v3i2.84
[12] Saurabh Shinde, Amar Bhegade, Anita Salve, & Chitra Bhosale, Prof. Shalaka Deore. (2015, December 17). Mobile based Anti-Phishing System using Secure QR Code. *International Journal of Engineering Research And*, *V4*(12). https://doi.org/10.17577/ijertv4is120289

[13] P.S.V, D., P, D., & SK, D. (2020, January 25). An Enhanced Mutual Authentication Scheme using One-Time Passwords with Images. *International Journal of Computer Trends and Technology*, *68*(1), 45–51. https://doi.org/10.14445/22312803/ijctt-v68i1p111

[14] Choudhary, A., Rajak, S., Shinde, A., Warkhade, S., & F.S., P. G. (2017, April 30). Online Banking System using Mobile-OTP with QR-code. *IJARCCE*, *6*(4), 657–661. https://doi.org/10.17148/ijarcce.2017.64125

[15] Amoah, G. A., & J.B., H. A. (2022, October 20). QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing). *International Journal of Computer Applications*, *184*(33), 34–39. https://doi.org/10.5120/ijca2022922425

