IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

"Quick-Cash "
(A QR-Based Smart ATM)

Mr. Anup Sonawane[1], Mr. Harshal Mahajan[2], Mr. Rohit Hire[3], Mr. Manish Pagare[4], Mr. Krishna Kadam[5]
HOD, Department Of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Mahavir Polytechnic, Nashik, India

Abstract: *In this innovative proposal, we present a secure alternative to traditional ATM transactions, addressing vulnerabilities associated with physical card swiping. Our system leverages QR codes, seamlessly integrated into smartphones and wearable devices, eliminating the need for a physical ATM card. To enhance security, an extended eight-digit PIN is employed, generated by a dedicated background server for each transaction. This server not only oversees transactions but also links them to the user's bank account in real-time. By utilizing QR codes and an advanced PIN system, our solution mitigates risks associated with shoulder surfing, replay attacks, and ATM card skimming, providing users with a robust and secure means of conducting ATM transactions.*

Keywords: ATM, credit card, ATM card, security, QR code, PIN security, attacker, cyber criminal's

I. INTRODUCTION

Amidst the concerns surrounding COVID-19, a promising solution emerges for secure ATM transactions. The fear of physical contact with ATM surfaces is alleviated as users can now withdraw cash by simply scanning a QR code displayed on the machine's screen with their mobile phones, eliminating the need to touch any surfaces. This innovation not only enhances hygiene but also addresses security issues associated with traditional ATM cards, where PIN entry is vulnerable to peeping attacks. By embracing QR code technology, we ensure a secure and touch-free transaction experience, safeguarding user data from potential leaks and other security threats.

II. RESEARCH METHODOLOGY

1. Project Scope and Goals: The projects study techniques is intended to provide through knowledge of integrated ATM machines. The major goal is to create an Smart/Card-less/QR-Based ATM which is easy to use. The goal are to create a seamless integration of those component in order to give consumer a better ATM experience.

2. System Architecture and Design: Here web server acts as an interface between the Android application and ATM. In the centralized database, we have stored all the user's credentials; the user needs to install the Android app on his/her smart device. First, the user needs to register their information in the bank website. Once the registration is successful, then the bank will provide the account number and OTP password to the registered user. In the Android app, then the registered user need to enter the account number and OTP password. User authentication is done on the server side, once the server finds the authorized user, and then the user is allowed to set the new password. In the Centralized Database, we have stored the credential information. Now the user interacts with the ATM. Then the authentication process is done on the server side, then user information is displayed in the ATM, now the user can do transaction /withdraw. When the user leaves the ATM, the new QR code is generated using Dynamic Token Generator.

3. Data Collection and Preparation: For the project on QR-based card-less ATM transactions, data collection involves gathering information on current ATM transaction systems, security vulnerabilities, and user behaviours related to ATM usage. This may include studying existing ATM protocols, security mechanisms, and fraud incidents. Additionally, data on QR code technology, encryption methods, and mobile device usage patterns are collected. Data preparation involves organizing and structuring the collected information for analysis and implementation. This includes categorizing security threats, identifying common user behaviours and understanding technological

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

requirements for QR code authentication. Furthermore, data preparation involves designing algorithms for PIN generation, transaction identification, and server-client communication. Overall, data collection and preparation lay the foundation for developing a secure and efficient QR-based card-less ATM system.

4. Website Design: Our focus in building the website for the QR-based cardless ATM transaction project is to create a platform that not only informs but also empowers users. We will provide a clear and detailed explanation of how the system works highlighting its security features and advantages compared to traditional ATM networks. Our website has easy-to-follow instructions, questions and tutorials to ensure users feel confident setting up and using the system. With a user-friendly and well-designed interface, website navigation will be seamless on all devices. We will include visuals such as photos and videos to increase understanding, ensure users feel educated and empowered to adopt these new solutions with confidence.

III. PAGE STYLE DESIGN OF THE PROPOSED SYSTEM

Architecture of the System:

The web page fashion layout will reflect the system's architecture, emphasizing the seamless integration of various additives inclusive of the server, ATM machines, Android utility, and bank database. Clear delineation of each element's position and interaction in the machine may be illustrated via visual hierarchy and layout corporation.

Design of the User Interface:

The user interface will prioritize simplicity and readability, with intuitive navigation to facilitate clean get entry to transaction functionalities. Visual factors which include icons, buttons, and menus could be designed with consistency and coherence to beautify usability and navigation performance.

Emphasis can be positioned on guiding customers through every step of the transaction method, from beginning a transaction to authentication and confirmation.

Security Procedures:

Security may be a paramount attention within the page style layout, with visible cues and indicators to reassure users of the device's protection measures. Encryption symbols, authentication activates, and other security signs will be prominently displayed to instil self-belief in customers concerning the security of their transactions. Clear commands and activates might be supplied to manual users on exceptional practices for ensuring the security of their non-public facts and transactions.

Design for Responsiveness:

The web page fashion design may be responsive, making sure most advantageous viewing and interplay reports across diverse gadgets and screen sizes. Flexible layouts and adaptive layout elements may be hired to accommodate unique viewport sizes and tool orientations seamlessly. User interface additives will dynamically alter to offer an finest person revel in, whether accessed from a phone, pill, or desktop.

Mechanism of User feedback method:

The proposal will include methods for providing user feedback, such as contact forms, feedback buttons, or survey touchpoints, to gather user insights and process any information or information troublesome solutions. Feedback channels within the user interface will be easily accessible, encouraging users to provide input or report any problems they encounter while interacting with the system

Documentation and Training:

A page layout will include detailed documentation and training materials to help users understand and use the system effectively. User guides, tutorials, quizzes and tutorial videos are readily available to provide users with the information and support they need to navigate the system with confidence.

A clear call to action will motivate users to obtain documentation and training materials, ensuring that they have access to the resources they need to optimize their experience with the system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

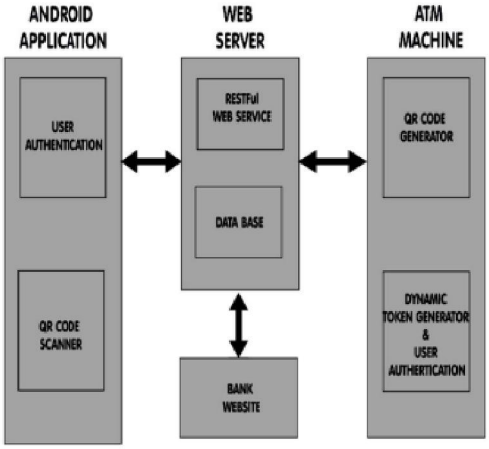


Fig 1: Architecture Diagram

Figure 2. User Authentication

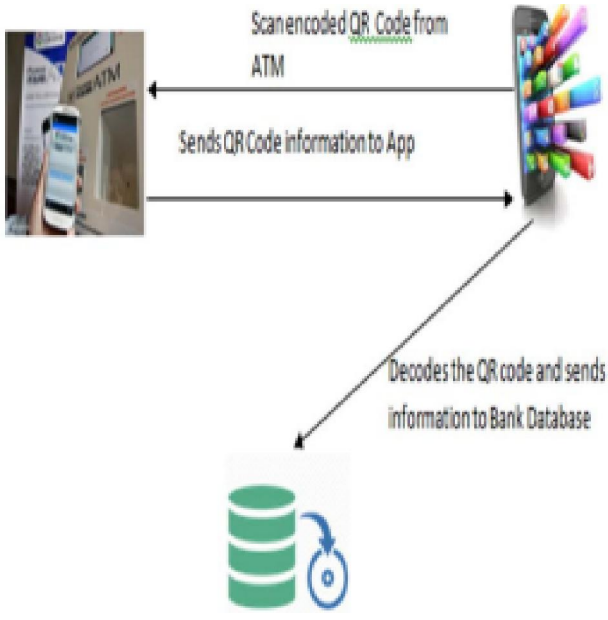


Figure 3. QR Code Scanner

DOI: 10.48175/IJARSCT-15528

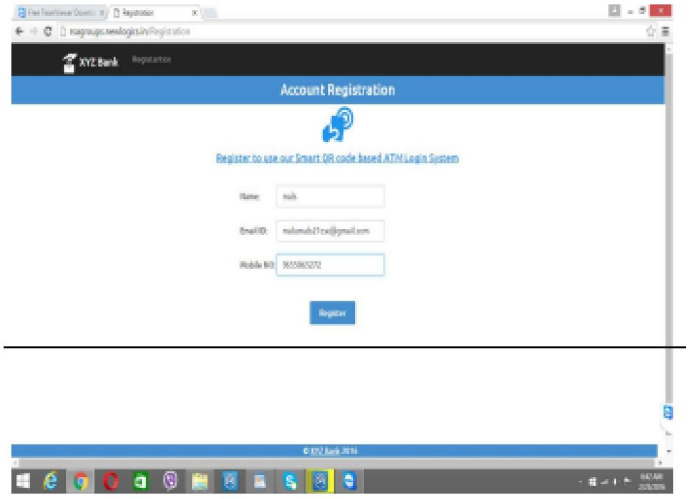
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

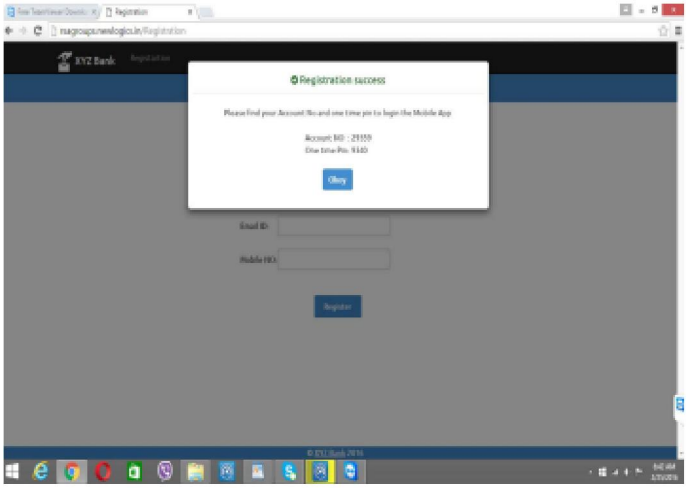
Figure 4. Web Service Module

Figure 5. Database design module

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

V. SCREENSHOTS





IV. CONCLUSION

In this paper, I have proposed a system in which from ATM the amount can be taken without using Smart cards like debit/credit card and PIN. In the QR code, the machine information is encrypted and stored. The information in the QR

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

code can be scanned by a mobile device using our mobile application which decrypts the encoded information in the QR code and sends the information to the server and transactions can be done once it identifies the validate user. Thus, we conclude that by using our system, the user can do transactions in ATM without cards as well as waiting time in ATM is also decreased. Nowadays, mainstream authentication systems of ATM have high risk. Since these systems do not have resistance to peeping attack. Finger vein authentication system and authentication system using one-time passwords have a vulnerability. For these reasons, we proposed the system without risk of peeping attacks. However, this technology displays privacy information such as payment and payees. It may be able to be read by unauthorized users. Therefore, the transfer information displayed on ATM. Illegal users are unable to find out the confidential information including the user's privacy.

ACKNOWLEDGMENT

We extend our heartfelt gratitude to Mr. Anup Sonawane, HOD & Lecturers in the Department of Information Technology, for his invaluable guidance and constant support throughout our research project. Mr. Anup Sonawane great expertise and intense knowledge were important to the project's success. Hisperceptiveguidance steered us through various challenges and significantly contributed to the project's successful completion. Their support, dedication, and valuable contributions greatly enriched our research endeavours, promote an environment of teamwork and innovation. We acknowledge and appreciate the contributions of all individuals involved, whose collective efforts have made this project possible. Their commitment to excellence and collaborative spirit have been instrumental in advancing our research objectives. Once again, we extend our heartfelt thanks to Mr. Anup Sonawane and our peers for their invaluable support and contributions throughout this research endeavour.

REFERENCES

[1] SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices. Rasib Khan, RagibHasan, and Jin fang XuSECRETLab, Department of Computer and Information Sciences.
[2] "Secure mobile-based financial transactions," S. N. White , Feb 2013, US Patent 8,374,916
[3] "Understanding credit card frauds," T. P. Bhatla, V. Prabhu, and A. Dua Cards business review, vol. 1, no. 6, 2003.
[4] "Cloning credit cards: A combined pre-play and downgrade attack on emv contactless." M. Roland and J. Langer, in Proceedings of The 7th USENIX Workshop on Offensive Technologies, 2013.
[5] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993.