QR based Card-Less ATM Transactions

Prof.(Dr)Ankita Karale
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
India
ankita.karale@sitrc.org

Saurabh Shelke
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
India
saurabhshelke28032002@gmail.com

Vinayak Gote
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
India
vinayakgote44@gmail.com

Priti Rithe
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
India
rithepriti26@gmail.com

Rushikesh Pawar
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
India
rp310799@gmail.com

Abstract
The conventional method of conducting ATM transactions using physical cards and four-digit PINs presents vulnerabilities such as card theft, PIN observation, and skimming. In response, this paper introduces a novel approach that leverages QR codes for secure and convenient ATM transactions. This system is designed for integration with smartphones and wearable devices, eliminating the need for physical ATM cards. Users generate a unique eight-digit PIN in combination with QR codes for authentication. A dedicated background server manages transactions, generating distinct eight-digit PINs for each transaction while securely linking them to the user's bank account. This approach enhances security, safeguards against observation attacks, and streamlines the transaction process. The innovative system has the potential to provide a more robust and user-friendly alternative to traditional ATM card-based transactions, with a strong focus on security and convenience. However, rigorous testing and adherence to regulatory requirements are essential to ensure its practicality and legal compliance in the banking sector.
Keywords: ATM, credit card, ATM card, security, QR code, PIN security, attacker, cyber criminal

I. INTRODUCTION

ATM transactions have become an integral part of our daily routines, offering quick access to cash and banking services. However, traditional card-based transactions come with their share of challenges. Long queues, distractions during transactions, time constraints, the need to remember PINs, the risk of others seeing your PIN, the speed of interaction, and the overall environment can all pose difficulties for card users. Moreover, as card-based systems have been in use for a while, fraudsters have become increasingly inventive in exploiting their vulnerabilities. Traditional ATM cards rely on a magnetic strip to store sensitive information, including PINs and authentication details. Unfortunately, these magnetic strips have proven vulnerable to fraudulent activities. It has become relatively easy for criminals to clone these strips using inexpensive card readers, granting them unauthorized access to users' information. While chip-based cards provide a more secure option, they still necessitate the physical presence of a card, presenting its own set of limitations.

II. LITERATURE SURVEY

Wireless Communication using Li-Fi Technology :
This paper describes the Li-Fi technology. Li-Fi stands for Light-Fidelity. Li-Fi is transmission of information through an LED light bulb by sending information through a LED light that varies in intensity faster than the human eye can follow. D-light, introduced by Harald Hass can be utilized to deliver information rates higher than 10 megabytes per second. Information can be send by varying intensity of LED light bulb such that each intensity transmits some information. Li-Fi can transfer information with data rates up to 10-50 Mbps, using which one can easily transfer Hugh amount of data in the blink of an eye. This data transfer can be done in a very secure manner as data is transmitted through light and light cannot travel through solid objects.

Development of transceiver using flashlight & camera in VLWC :
This paper describes how the bit codes are transmitted from one mobile to another using technology called as Li-Fi. Flashlight of one mobile is used for transmission of information and the information is retrieved using camera of second one. Flashlight blinks while sending information from one mobile to another. The flashlight of mobile turns on for 1 in bit code and turns off for 0 in bit code. Flashlight of mobile can provide transfer rate up to 750 bps by blinking because the intensity of flashlight cannot be changed. The camera of mobile can provide frame rate up to 60fps. Thus transfer rate is very less as compared to pure Li-Fi because of lack of hardware available in mobiles.

High sensitivity universal lifi receiver for enhance data communication :
This paper describes how the information is transferred from one computer to another using Li-Fi technology. An Arduino board can get attached to any computer by using USB cable. An LED light is attached to Arduino board at the sender side and a photo-resister is connected to Arduino board at receiver side. Then a data is first converted into respective bit codes and transmitted using LED light which is attached to Arduino board. Intensity of light is varied for transmission of information at sender side and it is received using photo-resister of receiver. Photo-resister is used to check sudden changes in intensity of light. Arduino can be used to transfer information by changing the intensity of LED. Arduino is an external module with different variants like Arduino UNO, Arduino NANO, etc. with each of them having their own unique use over the other. Arduino UNO is very cheap and provides most of the basic requirements for lots of projects.

Environment monitoring system based on wireless networking using open source hardware :
This paper illustrates the working principle and applications of an Arduino board. Arduino board can be used as a tool for study and research works. Arduino board can provide a quick tool in development of VLSI test bench especially of sensors. Main advantages are fast processing and easy interface. Arduino board is a micro-controller that can be programmed easily using C or C++ language in the Arduino IDE. Arduino board is integrated by different types of sensors. It is more convenient to use.

Modified RSA cryptography system based on offline storage and prime number :
This paper illustrates the working and benefits of modified RSA algorithm. The modified RSA algorithm is used for providing security for the data by using encryption and decryption techniques. The first public key algorithm provides security for transfer and saving of data over the system. Modified RSA algorithm is faster than traditional RSA algorithm. The modified RSA algorithm works with 3 prime numbers to make a modulus n which is obscure to decomposable by third party personal. The database system is used to deliver the key parameters for modified RSA algorithm. Modified RSA algorithm is more efficient than old RSA algorithm. The large prime no. relies upon three factors it is hard to break the large prime no. into three as compare in existing RSA algorithm. It take the index value corresponding to Encryption & Decryption from the database table and exchange at the time of encryption and decryption instead of unique key Encryption & Decryption in this way modified RSA algorithm is more efficient than RSA algorithm.

LI-FI the path to a new way of communication, IEEE :
This paper illustrates the wireless data transmission by the use of light for data transmission called as visible light communication. The data is transmitted by changing the intensity of light. Light waves have wider electromagnetic spectrum range as compared to radio waves. As the electromagnetic spectrum becomes continuously overcrowded due to increasing usage of Wi-Fi. To overcome this Li-Fi provides vaster electromagnetic spectrum. It is faster, safer, greener, better and heathier future for wireless communication system.

Automated Teller Machine :
This paper illustrates benefits and challenges of the ATM system. ATM cards are used for transaction of money from one bank account to another bank account. Most of the people now more often use Cashless money for their transactions. ATM cards are also used to withdraw money from the ATM machine. Some frauds can take place during transaction with ATM machine like card cloning, pin pad overlay, spy camera, etc. ATM cards users are increasing. Security in ATM card is lacking due to frauds like card cloning, pin pad overlay, spy camera, etc.

Double authentication in ATM machine to prevent fake ATM machine fraud :
This paper illustrates the use of ATM card transaction over traditional cash transaction in an ATM (Automated Teller Machine). Most of the people now more often uses Cashless money for their transactions. Cashless money includes ATM card transactions, online transactions, etc. ATM cards can be used for withdrawal of money from a bank account or transaction of money from one bank account to another. ATM cards are provided to authorize users by the bank with each of them having their own pin code for verification of user identity at the time of money transaction. Some frauds can take place during transaction with ATM machine like card cloning, pin pad overlay, spy camera; etc. ATM cards are very useful for transactions as compared to traditional cash oriented transactions. ATM cards are easy to carry and use. Because of this the use of ATM system has rapidly increased in past few years which also lead to increase in

ATM frauds. An ATM fraud brings distrust among ATM users as their contract with bank gets violated.

Data Encryption and Decryption Using RSA Algorithm in a Network Environment :
This paper describes the design of ATM system that improves the authentication of user while using ATM system. RSA (Rivest-Shamir-Aldeman) algorithm is used for encryption and decryption in ATM system for user authentication. Information is encrypted at sender side using public key provided to the sender and it is decrypted at receiver end using private key provided to the receiver. It is high speed encryption-decryption algorithm with 56 or 128 bit key lengths. An incorrect private key still decrypts the information but in different form other than original information. RSA algorithm is widely used as it provides better encryption in less time as compared to other algorithms. If private key is not known then encrypted form of RSA algorithm can only be cracked by using brute force or by systematic guessing, both of which are infeasible.

Visible Light Communication using a Digital Camera and an LED Flashlight :
This paper illustrates the optimal communication through visible light using LED flashlight as a sender and a digital camera as the receiver. The data can be transferred by blinking of LED flashlight. The LED flashlight turns on for transmission of bit '1' and turns off for transmission of bit '0'. The camera on receiver side receives the signal by observing the presence of the light spot on an intervening surface and converts it back to the binary signal. Due to light transmission the image can be clear using camera as receiver side and LED as sender side.

III. EXISTING SYSTEM

The current system relies on physical elements, namely magnetic cards, which are swiped at an ATM to verify and confirm a user's identity. This verification is done through a four-digit PIN, a secret code known only to the user and the bank. However, there are vulnerabilities in this system. Since the credit card is a physical object, it can be easily stolen. Moreover, the four-digit PIN, while offering a layer of security, has a limited number of combinations, making it susceptible to guessing. If an attacker gains access to the user's ATM PIN, it puts the user's bank account at risk. These PINs can be obtained through various means, such as someone watching over the user's shoulder (shoulder surfing), using card-skimming devices, replaying previous

IV. PROPOSED SYSTEM

Our system aims to enhance the security and simplicity of ATM transactions. To achieve this, we employ QR codes for user authentication and an eight-digit PIN for added security. The server acts as a central coordinator, managing the interactions between the wearable device, ATMs, and the user data stored in the banks' databases. This approach ensures a more secure and straightforward process for ATM transactions.

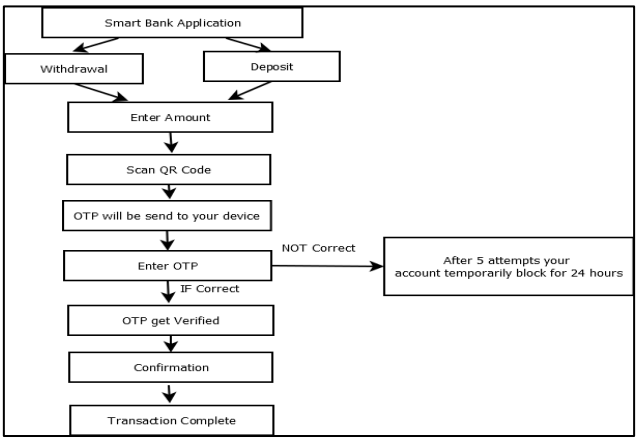

Fig. System Flow

A. SERVER:

The server plays a crucial role in ensuring secure ATM transactions. It verifies both the user and the ATM. When a transaction is initiated, the server generates a unique transaction ID upon receiving a request from the client. This ID is created using a SHA-512 hashing algorithm, and one of its components is the timestamp of when the transaction began, making it truly one-of-a-kind. This unique transaction ID is recorded in the database and shared with the client to create the ATM QR code. When an Android device scans this transaction ID, the system links the transaction in the QR code to the user who scanned it. This means the transaction is now associated with a specific user. The server then receives the transaction details from the user's Android app. To add an extra layer of security, a PIN template is generated and sent to the Android app. This template includes eight or more digits, with four of them reserved for the user's personal ATM PIN. The others are randomly generated and placed within the template. When the user enters this PIN template, along with their private ATM PIN, into the terminal, an authentication request is sent to the server. The server responds by sending the transaction details to the client, enabling actions like money withdrawal or checking the account balance. Importantly, the transaction ID is promptly marked as "used" in the server, either immediately after the transaction is completed or after a certain period to prevent misuse by potential attackers. This process ensures both security and a smooth user experience in ATM transactions.

B. ATM Machine:

When an ATM transaction is initiated, the ATM generates a request ID, which is a unique identifier for that transaction. This request ID, along with the ATM's identification and the current time, is sent to the server. The server uses this information to create a transaction ID, which is a one-of-a-kind code. This transaction ID is then sent back to the user's

device, where it's transformed into a QR code. This QR code serves as a secure link between the ATM and the user's device, such as an Android phone, making it a convenient way to proceed with the transaction. The user's Android device scans the QR code generated by the server, initiating the connection between the ATM and the user. To ensure security, the ATM client verifies the entered PIN template, which adds an extra layer of protection. Once the PIN template is confirmed, the user can complete the transaction seamlessly, whether it's a cash withdrawal or checking their account balance. Behind the scenes, the bank manages user details on a central server, which includes information like the user's bank account number and debit card details. Notably, these details are linked to the user's email address, simplifying the login process on Android devices. The bank's central server also keeps records of ATM locations and provides real-time monitoring of the ATMs' status. This server is closely connected to the bank's database, which houses the actual account information, ensuring the entire system operates efficiently and securely. This comprehensive approach not only enhances the security of ATM transactions but also makes them more user-friendly.

D. Android Application:

The Android application plays a central role in facilitating user interactions with the system. To get started, users need to log in to the app. This application includes two key features: a QR code generator and a QR code scanner. When a user arrives at an ATM, they scan the QR code displayed on the ATM screen using the app. This action links the transaction to the user, creating a secure connection. The app then displays a PIN template, which is a visual representation of the user's unique PIN requirements. Users enter transaction details and specify the amount they wish to withdraw. Subsequently, the app generates a new QR code that needs to be scanned by the ATM for transaction confirmation. To ensure the highest level of security, a final verification step is required. This involves entering the user's PIN within the PIN template into the ATM client. Only when this authentication process is successful can cash be withdrawn from the ATM. This multi-step procedure enhances the security of ATM transactions and ensures that only authorized users can access their funds.

V. System Protocol

The interactions and messages exchanged between the user, the ATM, and the server are explained in the following steps:
Step 1: The user enters the ATM with their mobile device and initiates the transaction by touching the ATM screen.

Step 2: A transaction request is sent to the server, along with essential parameters like the ATM's location and a request ID generated by the ATM.
Step 3: The server responds by generating a transaction ID and a PIN template, which are then sent back to the ATM client.
Step 4: The ATM, utilizing the provided transaction ID, generates a QR code for the transaction.
Step 5: The generated QR code is scanned by the user's Android device.
Step 6: The server establishes a link between the transaction ID and the user who scanned the QR code.
Step 7: An OTP (One-Time Password) is sent to the user's device, and the user enters this OTP.
Step 8: The entered OTP is verified for accuracy.
Step 9: After successful OTP verification, the user receives confirmation of the withdrawal.
Step 10: With the authentication process complete, the user can proceed to withdraw the desired amount from the ATM.

VI. Conclusion

The system is purposefully engineered to be highly resilient against various types of attacks, including card-skimming, observation attacks, replay attacks, and relay attacks. By utilizing a combination of technologies and security measures, this system offers a level of efficiency and security that surpasses traditional ATM systems. In this system, malpractices and fraudulent activities are significantly mitigated, making it a robust and secure solution for ATM transactions.

VII. Future Scope

Modifications and new features can be added to this project. A biometric authentication be used instead of one QR scanning.

Acknowledgment

- First and foremost, we wish to record our sincere gratitude to the Management of this college and our Respected Principal **Prof. (Dr) M. M. Patil.**
- Our sincere thanks to **Prof. (Dr) Ankita V. Karale**, Head, Department of Computer, Sandip Institute of Technology and Research Centre, Nashik.
- We express our sincere gratitude to our Guide, **Prof. Akhilesh Sharma** for guiding us in the investigations of this project and in carrying out experimental work.

References

1. 2021 7th International Conference on Information Management (ICIM) | 978-1-6654-4380-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICIM52229.2021.9417129

2. “Secure Card-less ATM Transactions”: University of Gothenburg. December 21, 2020 at 13:51:26 UTC from IEEE Xplore

3. "Achieving Privacy and Security using QR Code using Encryption Technique in ATM" 978-1-5090-4799-4/16 $31.00 © 2016 IEEE DOI 10.1109/ICRTCCM.2017.36

4. Ruslan, Gusti Made Karmawan, Suharjito, Yudi Fernandoand, and Anderes Gui, (2019), "QR Code Payment in Indonesia and Its Application on Mobile Banking" in FGIC 2nd Conference on Governance and Integrity 2019, KnE Social Sciences, pages 551–568. DOI 10.18502/kss.v3i22.5073

5. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions Circuits Systems. Video Technology, Vol. 14, No. 1, pp. 4–20, 2004.

6. Y. Feng and P. Yuen, "Protecting face biometric data on a smartcard with Reed–Solomon code," in Proc. CVPR Workshop Privacy Res.Vis., 2006.

7. Y. Lee, K. Park, S. Lee, K. Bae, and J. Kim, "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", IEEE Transactions On Systems, Man, And Cybernetics— Part B: Cybernetics, Vol. 38, No. 5, 2008, pp. 1304-1313.

8. Abhinav Muley, Vivek Kute, "Prospective solution to bank card system Using fingerprint", Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) [5] Anshuman Mohanty, Pranav Giria, Saptaswa Pal, Vishruthi K Acharya, "NFC Featured Triple Tier ATM Protection", 978-1-5386-5657- 0/18/$31.00 c 2019 IEEE

9. Sweedle Machado, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar, Priya Chaudhari, "Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System" 978-1-5386-5257-2/18/$31.00 ©2019 IEEE

10. Prachi More, Shubham Chandugade, Shaikh Mohammad Shafi Rafiq, Prof. Priya Pise, "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud", 2019 International Conference On Advances in Communication and Computing Technology (ICACCT) Amrutvahini College of Engineering, Sangamner, Ahmednagar, India. Feb 8-9, 2019

11. Ariana Tulus Purnomo, Yudi Satria Gondokaryono, Chang-Soo Kim, Ilkyeun Ra, "A Study on QR Code and Fingerprint Sequence for Securing Mobile Payment System", International Conference on Future Information & Communication Engineering, pp. 33-35, 2016.

12. Ariana Tulus Purnomo, Vincentius Timothy1, Yudi Satria Gondokaryono, Chang-Soo Kim, "An Approach in Mobile Payment Security using QR Code and ID-Based Encryption through Public Key Infrastructure (PKI)", Conference on Information Security and Cryptography, 2016.

13. Ariana Tulus Purnomo, Yudi Satria Gondokaryono, Chang-Soo Kim, Ilkyeun Ra, "The Combining Method of Fingerprint and QR Code as Mutual Authentication for Mobile Payment", SERSC Korea Information and Communications Society Journal of Information and Communication Convergence Engineering, 2016.

14. William Stallings, "Cryptography and Network Security", Pearson, United States of America.

15. Kinjal H. Pandya and Hiren J. Galiyawala, "A Survey on QR Codes: in Context of Research and Application", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue. 3, March 2014.

16. Somdip Dey, "SD-EQR: A New Technique to Use QR Codes in Cryptography", International Journal of Information Technology and Computer Science, IJITCS, May/June 2012.

17. International standard ISO/IEC 18004, "Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbology QR Code", Reference number? ISO/IEC 18004:2000(E), First edition 2000-06-15.

18. QR Code's features and standards, http://www.qrcode.com/en/about/version.html, accessed on 25 August 2016.

19. SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices. Rasib Khan, Ragib Hasan, and Jinfang Xu SECRETLab, Department of Computer and Information Sciences.

20. M. Imran and A. M. Hussaan, "Adaptive & dynamic interfaces for automated teller machines using clusters," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-6, doi: 10.1109/ICOMET.2018.8346346.