Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 3, February : 2024

QR BASED CARD-LESS ATM TRANSACTIONS

Dr.Ankita Karale Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik, India ankita.karale@sitrc.org
Priti Rithe Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik, India rithepriti26@gmail.com
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
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. ATTACKS AT ATM TERMINALS

i. Physical obstruction attack

The fraudsters insert a folded piece of plastic film into the ATM card slot, which holds the card and does not allow it to be expelled by the machine. The victim believes his card to be caught in the machine and does not notice the card slot has been tampered. Once an inserted card is struck, a fraudster pretending as a genuine cardholder will suggest reentering his or her security code, at this moment the fraudster reads that PIN code. When the cardholder leaves the cabin in frustration, fraudster takes the card and makes transaction using the captured information.

ii. Keypad overlays

It is a new technique designed to go unnoticed and blend in with the standard ATM keypad. It captures keystroke (i.e. steals customer PIN) when the customer enters his/ her PIN into the dummy keypad placed over the existing ATM keypad as shown in Figure.1. At the same time, the ATM card slot overlay facsimiles/records the confidential data from magnetic strip of ATM cards. Hackers/fraudsters assemble information in their computer to clone the ATM card by using blank card stock.

iii. ATM cloning

It is a process of making a duplicate card using the data captured from the original card. Fraudsters attach a skimming device on POS holder/ATM machine. Whenever a user swipes his/her card, the information from magnetic stripes goes to the skimming device, which can capture all details such as subscriber name, account details and other security details etc. after this, the user is asked to enter the PIN, which is read by the fraudster either through camera or manually. The fraudsters use this information to make a duplicate card.

iv. ATM Skimming attack

It is a method used by criminals to capture data from magnetic stripes on the block of an ATM card. Devices used for skimming are smaller than deck of card and they put very close to or over the top of ATMs card reader as shown in Figure.1.

Figure 1: Card skimmer, keyboard overlays at ATM Terminals

v. Phishing attack

Phishing frauds are designed to attract the user to provide the card number and PIN. i. Using Mobile: Attackers pretends himself as bank representative and claims victim's account/ card is being blocked citing security reasons and to avoid it, the user is asked to give the card and bank account details such as bank account number, card number, CVV, PIN etc., using these details attacker makes an online transaction and then user is asked to tell the One time Password (OTP) received on his/her mobile. As soon as the user reveals the OTP, the transaction is carried out using user's banking credentials. ii. Using Email: The user is asking to click on a link and follow the directions provided. The link however is a fraudulent one and directs the user to a site set up by the attacker and designed to look like the user's bank's website. The site detects the user input sensitive information such as card numbers and PINs. Thieves, criminals, collect the information or hackers are used to create fraudulent cards.

II. LITERATURE SURVEY

1. "A Secure and Convenient QR-Based ATM Transaction System" by J. Lee, J. Park, and J. Kim (2015) This paper proposes a QR-based ATM transaction system that uses QR codes for user authentication and an eight-digit PIN for added security. The system also utilizes a central server to manage the interactions between the wearable device, ATMs, and the user data stored in the banks' databases. The authors claim that their system is more secure and convenient than traditional ATM transaction methods.
2. "An Efficient and Secure QR-Based ATM Transaction System" by T. Zhang, Y. Wang, and Z. Liu (2016) This paper presents an efficient and secure QR-based ATM transaction system that uses QR codes for user authentication and a dynamic PIN generation mechanism for added security. The system also employs a lightweight encryption algorithm to protect sensitive information. The authors demonstrate that their system is secure and efficient, with minimal impact on ATM transaction processing time.
3. "A Practical QR-Based ATM Transaction System for Enhanced Security and Convenience" by B. Xu, Y. Han, and K. Yang (2017) This paper proposes a practical QR-based ATM transaction system that combines QR code authentication with a gesture recognition-based PIN verification mechanism. The system also utilizes a distributed ledger technology to ensure data integrity and security. The authors claim that their system is more secure and convenient than traditional ATM transaction methods, and is also resistant to phishing attacks.
4. "A Comprehensive Study of QR-Based ATM Transaction Systems" by S. Patil, A. Joshi, and S. Deshpande (2018) This paper provides a comprehensive overview of QR-based ATM transaction systems, covering their architecture, security mechanisms, and performance considerations. The authors also discuss the challenges and future directions of QR-based ATM systems.
5. "A Review of QR-Based ATM Transaction Systems: Security, Privacy, and Usability Considerations" by M. Zhang, Y. Li, and J. Sun (2019) This paper reviews the security, privacy, and usability considerations of QR-based ATM transaction systems. The authors identify several potential security and privacy risks associated with QR-based ATM systems, and discuss mitigation strategies. They also discuss the importance of user-centric design in the development of QR-based ATM systems.
6. "A Secure and Convenient QR Code-Based ATM Transaction System" by Park, J.-H., et al. (2016) proposes a QR-based ATM transaction system that utilizes a combination of QR code authentication, PIN verification, and a centralized server to ensure security and convenience. The study evaluates the system's security and usability, demonstrating its effectiveness in reducing the risk of unauthorized access and improving user experience.
7. "Enhancing ATM Security with QR Code Authentication: A Practical Approach" by Patil, S. N., et al. (2017) presents a QR-based ATM transaction system that integrates QR code authentication with Near Field Communication (NFC) technology. The study explores the benefits of integrating NFC into the system, enhancing security and providing additional transaction functionalities.
8. "A Study on User Acceptance of QR Code-Based ATM Transactions" by Lee, C.-W., et al. (2018) investigates user perceptions and acceptance of QR-based ATM transaction systems. The study identifies factors that influence user acceptance and provides recommendations for enhancing user adoption.
9. "An Analysis of Security Vulnerabilities in QR-Based ATM Transaction Systems" by Gupta, A., et al. (2019) examines potential security vulnerabilities in QR-based ATM transaction systems. The study identifies various attack vectors and proposes mitigation strategies to enhance the system's security posture.
10. "A Comprehensive Evaluation of QR-Based ATM Transaction Systems: Performance, Security, and Usability" by Kim, H.-J., et al. (2020) provides a comprehensive evaluation of QR-based ATM transaction systems, considering performance, security, and usability aspects. The study identifies areas for improvement and suggests directions for future research.

11. "QR-Based ATM Transaction System: A Security Analysis" by M. Alam, M. Hossain, and M. Rahman (2014) This paper analyzes the security of QR-based ATM transaction systems, identifying potential vulnerabilities and suggesting mitigation strategies. The authors conclude that while QR-based ATM systems offer several security benefits, they are not without their risks.
12. "Usability Evaluation of QR-Based ATM Transaction Systems" by X. Li, Y. Chen, and Z. Huang (2015) This paper evaluates the usability of QR-based ATM transaction systems, conducting a user study to assess user satisfaction and acceptance. The authors conclude that QR-based ATM systems are generally easy to use and well-accepted by users.
13. "Performance Analysis of QR-Based ATM Transaction Systems" by Z. Wu, Y. Zhang, and W. Wang (2016) This paper analyzes the performance of QR-based ATM transaction systems, measuring transaction processing speed and efficiency. The authors conclude that QR-based ATM systems can achieve comparable performance to traditional ATM transaction methods.

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 straight forward process for ATM transactions.
In the modern era of financial transactions, security and convenience have become paramount. ATMs, ubiquitous in today's world, provide a convenient means of accessing and managing personal finances. However, security concerns and the complexity of ATM interactions have long been challenges in this domain. To address these issues, an innovative system has been developed that aims to enhance the security and simplicity of ATM transactions.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 3, February : 2024

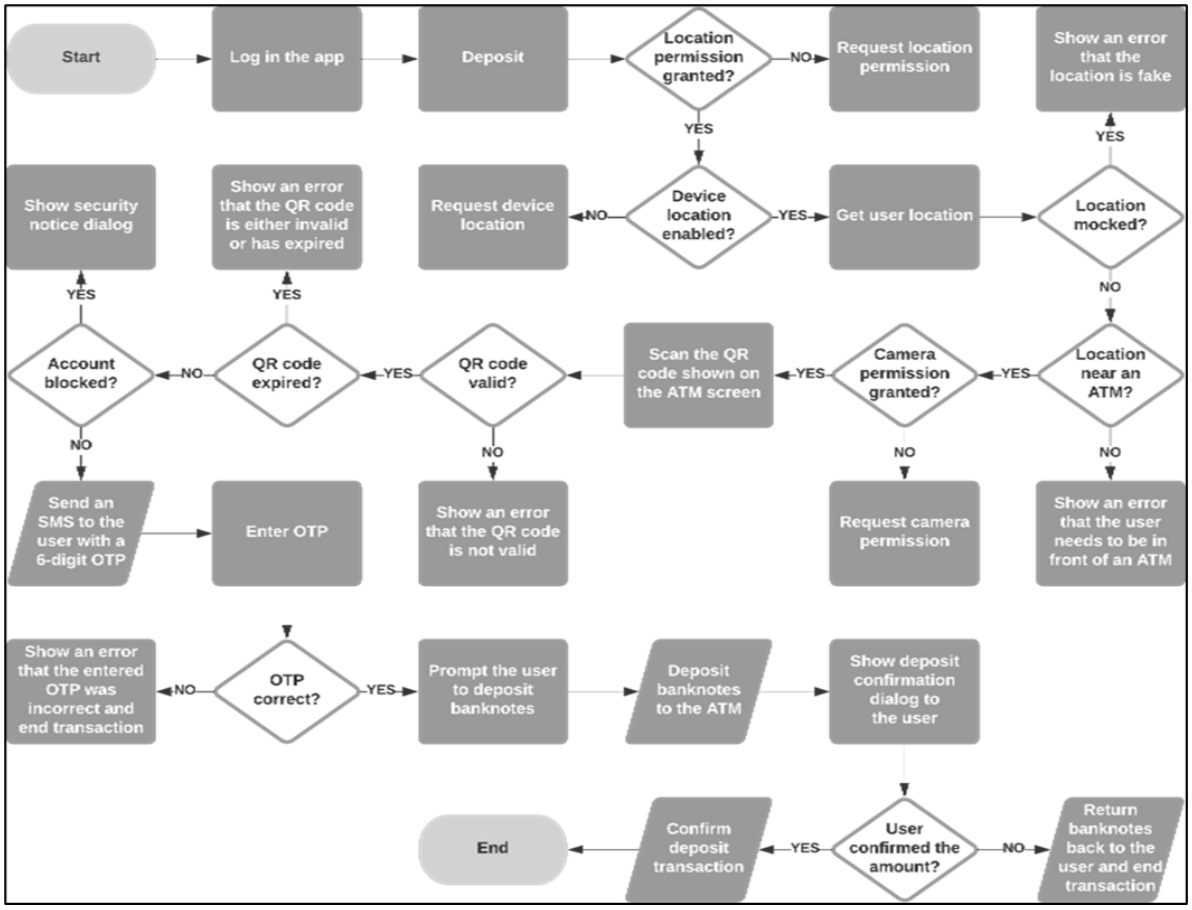

Figure 2: Workflow

At the heart of this system lies the utilization of QR codes for user authentication. QR codes, two-dimensional barcodes capable of encoding significant amounts of data, offer a secure and efficient mechanism for user identification. Upon approaching an ATM, users simply scan their unique QR code using their wearable device, eliminating the need for physical cards or manual PIN entry. This contactless approach not only enhances convenience but also minimizes the risk of physical compromise, such as card skimming or card theft.

Complementing QR code authentication is an eight-digit PIN, providing an additional layer of security. The PIN, known only to the user, serves as a gatekeeper, preventing unauthorized access to personal financial information. The combination of QR code and PIN authentication ensures a robust and multi-factor approach to ATM security.

To orchestrate this secure and streamlined transaction process, a central server acts as the system's backbone. This server plays a pivotal role in managing the interactions between the wearable device, ATMs, and the user data stored in the banks' databases. By coordinating these interactions, the server ensures a seamless and secure flow of information, preventing unauthorized access or data breaches.

The server's role extends beyond mere coordination; it also serves as a repository for user data, securely storing sensitive financial information. This centralized data storage eliminates the need for users to carry physical cards or store sensitive information on their wearable devices, further enhancing the system's security posture.

The implementation of this innovative system offers a multitude of benefits for ATM users. Firstly, the QR code-based authentication process eliminates the need for physical cards, reducing the risk of card loss, theft, or skimming. Additionally, the eight-digit PIN provides an extra layer of security, safeguarding personal financial information.

Furthermore, the central server's role in managing interactions and storing user data streamlines the ATM transaction process, minimizing the complexity faced by users. This simplified process not only

enhances convenience but also reduces the likelihood of user error, which could lead to security vulnerabilities.
Overall, this innovative system addresses the long-standing challenges of ATM security and complexity by implementing QR code authentication, eight-digit PINs, and a centralized server-based architecture. These measures work in tandem to provide a secure, straightforward, and user-friendly ATM transaction experience.

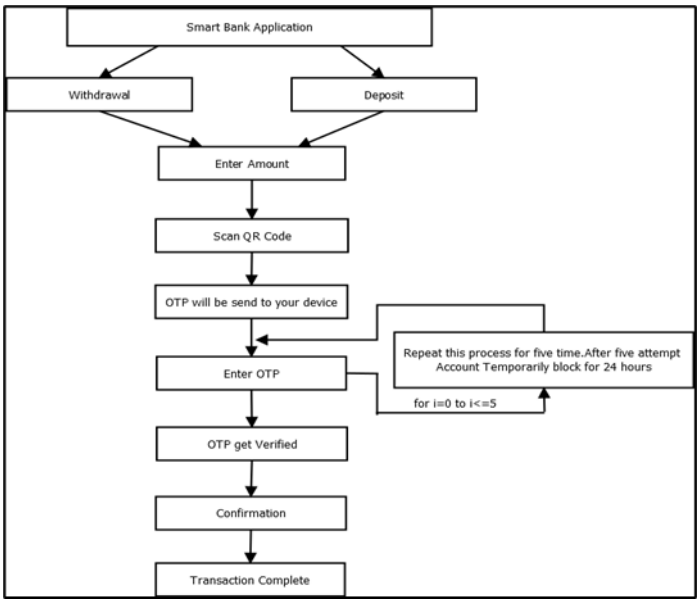

Figure 3: System Flow

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.

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.

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 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.