ATM Keypad Shuffling And Application

Mrs ANITHA T[1], Dr SUMATHI[2], GAYATHRI C[3]
[1, 2, 3] Dept of Artificial Intelligence And Data science,
[1, 2, 3] SNS College Of Engineering

Abstract- *The address problem of shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touchscreen devices. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits. To reason about the security of Illusion PIN, we developed an algorithm which is based on human visual perception and estimates the minimum distance from which an observers unable to interpret the keypad of the user. None of the attacks was successful against our estimations. In addition, we estimated the minimum distance from which a camera is unable to capture the visual information from the keypad of the user. Based on our analysis, it seems practically almost impossible for a surveillance camera to capture the PIN of a smartphone user when IPIN is in use.*

I. INTRODUCTION

Now a day's millions of people using internet regularly and day by day they are increasing in abundant way. Today for authentication, user name and password is used basically, hence the security must provide in order to prevent hackers from accessing the data present in account of particulars. Phishing is a type of attack in which the attacker attempts to acquire the person's information such as user-id, password, pin no, etc. by showing the user to believe that he is communicating with a trustworthy person. The users would normally receive a phishing email with a link and if user clicked that link, it will take them to a fake web site which could add malicious programs into the users compute. Sometimes a phishing email can ask the users to provide their account details to carry verification purpose. So, it is necessary that the authentication should secure to protect user accounts. The common technique used for authentication is textual password technique. The vulnerabilities of this type of technique is dictionary attack, social engineering and shoulder surfing attack. A Dictionary Attack is a technique for defeating with authentication mechanism by trying to determine or generate its decryption key to enter into once account. It is such method in which there is breaking to a password protected system by systematic manner by entering every word in a dictionary as password and in Shoulder Surfing, the hacker tries to look over persons shoulder to catch password. This is an attack in which an observer try to watch the keyboard entries to learn password characters entered by the user. Shoulder surfing could be carried out in a number of ways. As the keyboard is openly displayed on the screen of computer, it makes very easy to observe the key entered by person. Shoulder surfing is possible by watching the keyboard entry from some distance or by recording complete process through CCTV camera or by taking screen shots of keys pressed by person.

II. RELATED WORKS

ATM keypad shuffling refers to the practice of rearranging the numbers on the keypad after each use, aiming to enhance security and protect users from PIN code theft. Here's a more detailed exploration of this concept and its related works:

Security Enhancement:

Objective: The primary goal is to prevent unauthorized access by making it difficult for onlookers or surveillance cameras to determine the PIN code based on the observed keystrokes.

Implementation: Various shuffling algorithms are designed to dynamically change the position of the numbers on the keypad, introducing unpredictability.

Research on Shuffling Algorithms:

Dynamic Algorithms: Studies focus on developing algorithms that change the position of numbers dynamically. For example, rearranging the keypad layout after each transaction or based on a time interval.

User Behavior Analysis: Research may explore how users adapt to dynamic shuffling and if certain algorithms are more effective in preventing PIN code inference.

User Experience and Preferences:

Human Factors: Investigating how users perceive and adapt to keypad shuffling is crucial. Research may assess the impact on usability, user acceptance, and potential frustration.

Preference Studies: Understanding which shuffling patterns or algorithms users find more intuitive or secure can influence the design of such systems.

Application in Banking and ATMs:

Integration: Research and development focus on seamlessly integrating keypad shuffling into existing ATM systems without compromising user experience.

Usability Testing: Testing the efficiency and user- friendliness of these systems in real-world scenarios to ensure they meet security objectives without causing inconvenience.

Biometric Integration:

Combined Security Measures: Exploring how keypad shuffling can complement biometric authentication methods, creating a multi-layered security approach.

Security Threats and Countermeasures:

Analysis of Attacks: Research may examine potential attacks on keypad shuffling systems, such as shoulder surfing or sophisticated methods, and propose countermeasures.

Usability vs. Security Trade-offs: Investigating the balance between enhanced security and the usability challenges introduced by dynamic keypad layouts.

Regulatory Compliance:

Standards and Regulations: Considering how keypad shuffling aligns with industry standards and regulations in the financial sector to ensure widespread adoption.

Future Developments:

Emerging Technologies: Exploring how advancements in technology, such as artificial intelligence or machine learning, can contribute to improving the security of ATM keypad shuffling.

Overall, research in ATM keypad shuffling is multidisciplinary, involving aspects of computer science, human-computer interaction, and cybersecurity to create secure and user-friendly solutions.

III. METHODOLOGY

3.1. PROPOSED METHODOLOGY

1. Initialization:

Generate an initial random arrangement of keypad numbers using a cryptographically secure pseudo-random number generator. Encrypt and store this initial arrangement securely on the ATM and the server.

2. Dynamic Shuffling Algorithm:

Develop a dynamic shuffling algorithm that triggers keypad rearrangement at regular intervals or based on predefined events. Ensure the algorithm is resistant to pattern analysis, making predictions difficult for potential attackers.

3. Encryption and Key Management:

Implement a robust encryption algorithm with a secure key for protecting the shuffled keypad configuration.

Employ a secure key management system to safeguard encryption keys, allowing only authorized entities access.

4. Server-Side PIN Validation:

When a user enters their PIN, the ATM encrypts the entered PIN using the current keypad arrangement and sends it securely to the server. The server decrypts the received PIN using the stored key and verifies it against the original PIN associated with the current shuffled keypad layout.

5. Secure Communication:

Establish secure communication channels between the ATM and the server using protocols like TLS to protect data during transmission. Implement measures to detect and respond to any unauthorized attempts to intercept or manipulate communication.

6. User Interface:

Display clear and concise instructions on the ATM screen explaining the shuffled keypad system and guiding users on entering their PIN. Use visual cues and prompts to ensure users understand and follow the necessary steps for PIN entry.

7. Regular Algorithm Updates:

Periodically update the shuffling algorithm and encryption methods to stay ahead of potential security threats. Conduct thorough testing before deploying updates to ensure compatibility and reliability.

8. Monitoring and Logging:

Implement a comprehensive logging system to record keypad shuffling events, PIN entries, and any suspicious activities. Regularly monitor logs for unusual patterns or security incidents, enabling prompt response to potential threats.

9. User Education and Awareness:

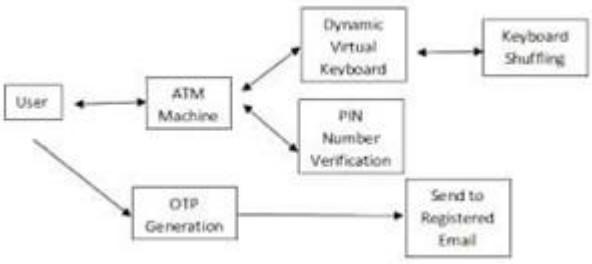
Launch educational campaigns to inform users about the security benefits of shuffled keypads. Emphasize the importance of keeping PINs confidential and explain that the changing keypad layout enhances overall security.

10. Compliance and Standards:

Ensure the proposed methodology aligns with relevant security standards and regulations. Regularly conduct security audits and assessments to verify compliance and identify areas for improvement.

By incorporating these steps into the implementation process, you can establish a robust and secure shuffled ATM keypad system that enhances overall security and mitigates the risk of PIN theft.

3.2 BLOCK DIAGRAM



3.3 ADDITIONAL METHODOLOGIES

1. Cryptographic Key Derivation:

Utilize a secure key derivation function to generate unique keys for encrypting the keypad configuration. Derive keys based on a combination of factors, such as time and transaction-specific parameters.

2. Secure Element Integration:

Integrate a secure element within the ATM to store sensitive data, including encryption keys and the current shuffled keypad configuration. This hardware-based security enhances resistance against physical attacks.

3. Biometric Authentication Integration:

Integrate biometric authentication, such as fingerprint or iris scanning, in conjunction with the shuffled keypad. This adds an additional layer of security, ensuring the user's identity is verified alongside the PIN.

4. Multi-Party Computation for Decryption:

Implement multi-party computation techniques for PIN decryption. Split the decryption process between the ATM and the server, requiring collaboration for PIN verification without exposing the full decrypted PIN at any point.

5. Behavioral Analysis:

Incorporate behavioral analysis into the system to detect anomalies in PIN entry patterns. Unusual patterns, even with a valid PIN, could trigger additional security measures or alerts.

6. Adaptive Shuffling Algorithm:

Develop an adaptive shuffling algorithm that adjusts the frequency of keypad rearrangements based on usage patterns and threat assessments. This ensures a balance between security and user convenience.

7. Secure Over-the-Air Updates:

Implement a secure mechanism for over-the-air updates to refresh the shuffling algorithm and address any vulnerabilities. This helps in maintaining a resilient security posture against evolving threats.

8. HSM (Hardware Security Module) Integration: Integrate HSMs to manage cryptographic operations securely. HSMs provide a dedicated and tamper-resistant environment for critical security functions, such as PIN encryption and decryption.

9. Dynamic PIN Length Variation:

Introduce occasional variations in PIN length dynamically. This adds an extra layer of complexity, making it harder for attackers to deduce the PIN length even if they observe multiple entries.

10. Continuous Security Testing:

Conduct regular penetration testing and security assessments to identify vulnerabilities and weaknesses in the system. This proactive approach helps in addressing potential security threats before they can be exploited.

11. User-Friendly Interface Design:

Design an intuitive and user-friendly interface that ensures a smooth experience for users despite the shuffled keypad. Provide feedback and guidance to users during PIN entry to enhance clarity.

12. Regulatory Compliance and Privacy:

Ensure compliance with data protection regulations and privacy standards. Implement measures to protect user data and adhere to legal requirements regarding the storage and processing of sensitive information.

By incorporating these additional elements into the methodology, the ATM keypad system becomes more resilient against various security threats and offers a higher level of protection for user PINs and sensitive data.

3.4 REQUIREMENTS

Hardware:

Keypad Interface:

- Select a keypad with individual keys and a matrix layout. Each key should have a unique identifier.
- Interface the keypad with the microcontroller using a suitable communication protocol (e.g., GPIO pins).

Microcontroller/Processor:

- Choose a microcontroller or processor with sufficient processing power and security features.
- Implement code on the microcontroller to read input from the keypad, shuffle the keys, and communicate with the ATM software.

Display:

- If your ATM has a display, ensure it supports the display of the shuffled keypad layout.
- Integrate the display with the microcontroller to update the visual representation of the shuffled keypad.

Secure Enclosure:

- Design a secure enclosure to house the keypad, microcontroller, and other components.
- Implement physical security measures to prevent unauthorized access or tampering.

Software:

Algorithm for Shuffling:

Develop a robust algorithm to shuffle the keypad layout securely. Consider cryptographic techniques to enhance security.Ensure the algorithm is efficient and does not introduce delays in the user interface.

User Interface (UI):

Modify the ATM software to incorporate the shuffled keypad layout. Design a clear and intuitive visual representation on the screen to guide users through the shuffled layout.

Input Handling:

Adjust the software to interpret the shuffled keypad input correctly. Map the shuffled key presses back to the original layout for processing transactions.

Security Measures:

Implement encryption for communication between the microcontroller and other components. Employ secure coding practices to prevent software vulnerabilities.

Regularly update and patch the software to address any discovered security issues.

Testing:

Usability Testing:

Conduct usability testing with actual users to ensure the shuffled keypad is user-friendly and does not hinder the transaction process.

Security Testing:

Perform thorough security testing, including penetration testing, to identify and address vulnerabilities. Regularly update security protocols based on emerging threats and industry best practices. Ensure compliance with relevant standards and regulations, such as those set by financial institutions and security standards like PCI DSS. Regularly review and update the implementation to address evolving security challenges.

3.5. SOFTWARE IMPLEMENTATION

Security Monitoring:

Implement continuous security monitoring features to detect and respond to any suspicious activities. Set up alerts for multiple incorrect PIN attempts, unusual patterns, or potential tampering.

Remote Updates:

Develop a secure mechanism for remotely updating the keypad shuffling algorithm and software. Ensure that updates can be deployed efficiently without compromising security.

User Education:

Provide clear instructions to users about the shuffled keypad system to avoid confusion. Educate users on the importance of keeping their PIN confidential and not sharing it.

Fallback Mechanism:

Establish a secure fallback mechanism in case of technical issues or emergencies. Ensure that users can still access their accounts through alternative authentication methods if needed.

Collaboration with Hardware:

Coordinate with the hardware components of the ATM to seamlessly integrate the shuffled keypad. Ensure compatibility and synchronization between the software and hardware components.

Regulatory Compliance:

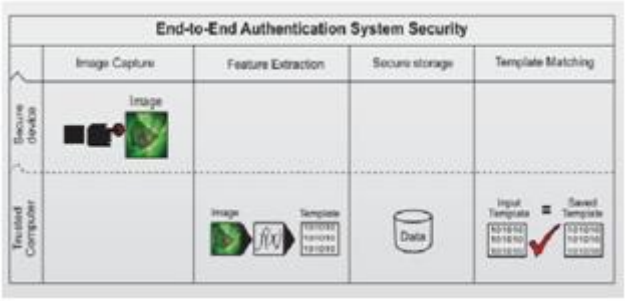
Stay updated with relevant regulations and standards related to ATM security. Regularly assess and update the software to meet changing compliance requirements.

Encryption for Communication:

Employ strong encryption protocols for communication between the ATM and the banking network. Protect sensitive data during the transmission process.

Response Plan for Security Incidents:

Develop a comprehensive response plan for security incidents, including a protocol for handling potential breaches. Define roles and responsibilities for incident response to minimize the impact on users and the financial institution. These additional points address ongoing security considerations, user awareness, and proactive measures to maintain a secure and reliable ATM system with keypad shuffling implemented in the software.



IV. RESULT AND DISCUSSIONS

Results and Discussion:

Effectiveness: Evaluate the success of ATM keypad shuffling in preventing PIN theft. Analyze any reported incidents of unauthorized access before and after implementation.

User Experience: Assess user feedback regarding the convenience and ease of use. Consider whether the shuffling mechanism causes confusion or inconvenience for customers.

Adoption Challenges: Discuss any challenges faced during the implementation phase, such as technical issues, costs, or resistance from users.

Security Assessments: Conduct regular security assessments to identify vulnerabilities and ensure that keypad shuffling remains an effective deterrent against evolving threats.

Comparative Analysis: Compare the security effectiveness of keypad shuffling with alternative security measures, weighing the strengths and weaknesses of each approach.

security threats will be essential in maintaining the project's effectiveness. In summary, the "ATM Keypad Shuffling" project represents a proactive approach to enhancing ATM security and user satisfaction, with the potential for further evolution and innovation to meet the changing needs of ATM users and the evolving landscape of security threats.

V. CONCLUSION

In this paper, the "ATM Keypad Shuffling" project aims to address a critical security concern while enhancing the user experience at ATMs. By implementing a dynamic keypad shuffling system, the project seeks to mitigate the risk of PIN code theft through various means, such as hidden cameras, skimming devices, and shoulder surfing. The project's primary objective is to strike a balance between security and user-friendliness, ultimately providing a secure and convenient ATM experience for all users. Through the design thinking process, the project can take into account user empathy, needs, and feedback to develop a solution that aligns with their expectations. The project's scope encompasses the design and implementation of the dynamic keypad system, user he project's scope encompasses the design and implementation of the dynamic keypad system, user experience considerations, security enhancements, and compliance with relevant regulations. While certain elements are excluded, such as changes to physical ATM hardware and legal aspects, the scope provides a clear framework for project execution. Looking into the future, the project offers opportunities for ongoing improvement and innovation, including advanced security features, global adoption, user education, and integration with emerging technologies like AI and blockchain. Continuous user feedback and adaptation to evolving

REFERENCES

[1] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 553–567.

[2] M. Harbach, A. De Luca, and S. Egelman, “The anatomy of smartphone unlocking,” in Proceedings of the 34th Annual ACM Conference on Human Factors in Computing Systems, CHI, 2016.

[3] J. Bonneau, S. Preibusch, and R. Anderson, “A birthday present every eleven wallets? the security of customer-chosen banking pins,” in Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012, vol. 7397, pp. 25–40.

[4] R. Anderson, “Why cryptosystems fail,” in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993, pp. 215– 227.

[5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens.” WOOT, vol. 10, pp. 1–7, 2010.

[6] A. Oliva, A. Torralba, and P. G. Schyns, “Hybrid images,” ACM Transactions on Graphics (TOG), vol. 25, no. 3, pp. 527–532, 2006.

[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, “Multi-touch authentication on tabletops,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010, pp. 1093–1102

[8] L.-W. Chan, T.-T. Hu, J.-Y . Lin, Y.-P. Hung, and J. Hsu, “On top of tabletop: A virtualtouch paneldisplay,” in Horizontal Interactive Human Computer Systems, 2008. TABLETOP 2008. 3rd IEEE International Workshop on. IEEE, 2008, pp. 169–176.

[9] W. Matusik, C. Forlines, and H. Pfister, “Multiview user interfaces with an automultiscopic display,” in Proceedings of the working conference on Advanced visual interfaces. ACM, 2008, pp. 363–366.

[10] C. Harrison and S. E. Hudson, “A new angle on cheap lcds: making positive use of optical distortion,” in Proceedings of the 24th annual ACM symposium on User interface software and technology. ACM, 2011, pp. 537–540.