INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 02, February 2024, pp : 250-253

e-ISSN : 2583-1062

Impact Factor : 5.725

SOPHISTICATED AUTHENTICATION USING INDIRECT PIN ENTRY

M. Vishnu[1], V. Vigneshwaran[2], S. Krishna[3], Mrs. R. Kohila[4]

[1,2,3]Student, Department of CSE (Cyber Security) Muthayammal Engineering College, India.

[4]Assistant Professor M.E., Department of CSE (Cyber Security) Muthayammal Engineering College, India.

ABSTRACT

In the realm of secure PIN entry methods, traditional direct input mechanisms have been prevalent but prone to vulnerabilities such as shoulder surfing and brute force attacks. To address these concerns, indirect PIN entry methods have emerged, offering enhanced security through challenges presented to users. However, existing indirect methods often demand significant cognitive effort, rendering them impractical for a wide range of users. In this paper, we propose an innovative approach to indirect PIN entry leveraging QR code technology, aimed at enhancing accessibility and usability while maintaining robust security. Our method involves the generation of challenges in QR code format, which users can effortlessly scan using a dedicated mobile application.

We present the design and implementation of an ATM Simulator Web Application, developed using Flutter for the front-end and PHP for the back-end, as a proof of concept for our proposed method. Furthermore, we detail the challenge generation process, wherein original PINs are mapped to shuffled keys, and users are tasked with rearranging a keypad according to the challenge's instructions. Evaluation of our method demonstrates its efficacy in enhancing security while significantly reducing the cognitive burden on users. Through this work, we aim to contribute to the advancement of secure PIN entry methods, paving the way for more accessible and user-friendly authentication solutions in various domains.

Keywords: Indirect PIN Entry, One Time PIN, Shoulder Surfing.

1. INTRODUCTION

Background and Motivation:

PIN (Personal Identification Number) entry methods play a crucial role in secure authentication systems across various domains such as banking, e-commerce, and access control systems. Traditional direct PIN entry methods, while widely used, are susceptible to security vulnerabilities such as shoulder surfing and brute force attacks.

Overview of Indirect PIN Entry Methods:

Indirect PIN entry methods have emerged as a solution to enhance security in authentication processes. These methods often involve challenge-response mechanisms, which present challenges to users to verify their identity. However, existing indirect methods have limitations, including high cognitive load and usability issues.

Proposal and Objectives:

To address the limitations of existing indirect PIN entry methods, we propose an innovative approach leveraging QR code technology. The primary objectives of our research are to enhance accessibility, usability, and security in PIN entry processes. Our proposed solution utilizes a Flutter-based mobile application for QR code scanning and a PHP-based backend server.

2. SYSTEM ARCHITECTURE

Overview:

The system architecture of our proposed indirect PIN entry method leveraging QR code technology comprises three main components: the mobile application, the backend server and the front-end ATM Simulator. This section provides an overview of the architectural design and interaction between these components.

Atm Simulator:

The ATM simulator is responsible for replicating an ATM like user interface along with user management utilities for admins and virtual ATM Cards. The users can insert their virtual ATM Card and the simulator communicates with backend server for authentication and further utilities. It allows users to authenticate, enquire balance and also withdraw virtual money.

Backend Server:

The backend server is responsible for generating challenges, validating user responses, and facilitating communication between the simulator application and the authentication database.

Developed using PHP, the backend server handles HTTP requests from the mobile application, processes challenge generation requests, and stores user authentication data securely.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 02, February 2024, pp : 250-253

e-ISSN : 2583-1062

Impact Factor : 5.725

Upon receiving a request from the simulator application to generate a challenge, the backend server generates a unique challenge sends it back to the simulator.

The backend server also generates the solution for the challenge as well to match it against the user submitted solution.

Mobile Application:

The mobile application serves as a helper to solve the challenge more quickly. Initially the users should setup the application with their original PIN once. After that the application will directly open at the QR Scanning page where it scans the QR in the simulator screen and gives user the solution.

Interaction Flow:

The interaction flow between the mobile application, simulator and the backend server are as follows:

1. Insert a virtual card in the simulator and the we wait for the challenge from the server.
2. Users can either solve the challenge by themselves by performing the calculations in their mind itself or they can quick open the helper application which've provided using which they can scan the QR in the simulator screen to obtain the solution to the challenge.
3. The mobile application extracts the challenge information from the QR code and calculates the solution based on the PIN the user had initially set up.
4. User resolves the challenge and submits the response to the backend server for verification.
5. The backend server verifies the user's response and grants access to the user's account if successful.
6. On Success the Users will have options to check their Account Balance and also withdraw virtual money if they have sufficient balance.
7. These two basic features were provided to make proof of concept for that the user has been authenticated.
8. Once done the virtual card can be removed form the simulator and the simulator goes to the initial state.

3. DESIGN AND IMPLEMENTATION

System Design:

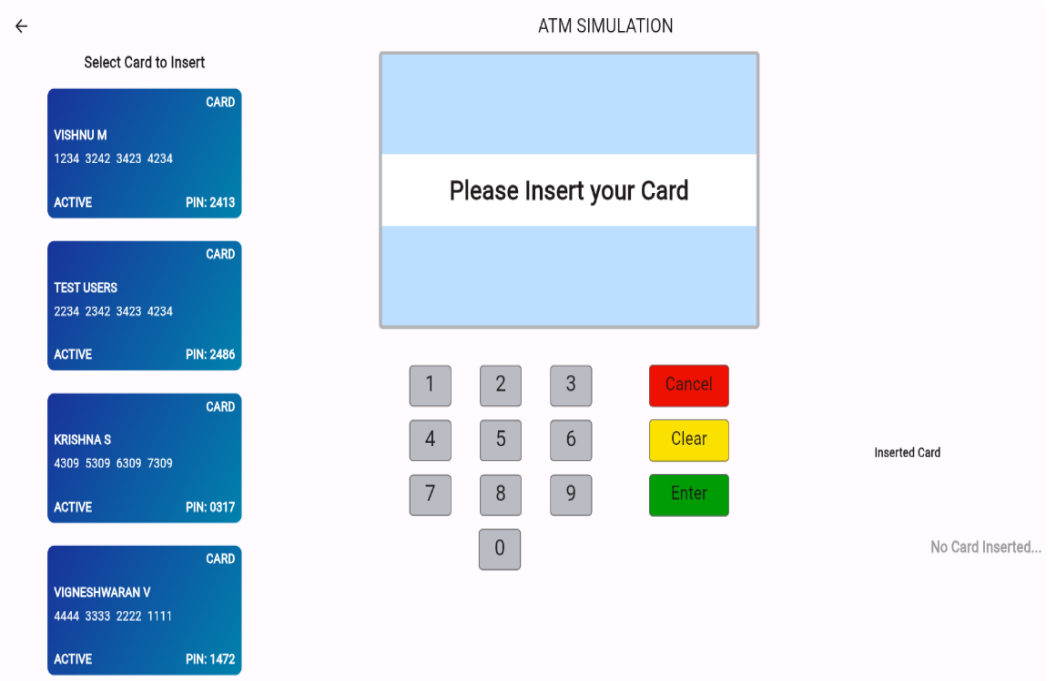
The design of our indirect PIN entry system leveraging QR code technology involves several key components, including the mobile application interface, challenge generation algorithm, and backend server architecture.

The system is designed to ensure security, usability, and compatibility with existing authentication processes, while leveraging QR code technology to streamline the PIN entry process.

The Simulator Design:

The simulator is designed using the Flutter framework and deployed as a web application which communicates to the backend PHP server for all it's operations. The simulator is designed in a way that it replicates an ATM Machine with Keypad, Virtual Cards etc..

Initial Interface:



www.ijprems.com
editor@ijprems.com

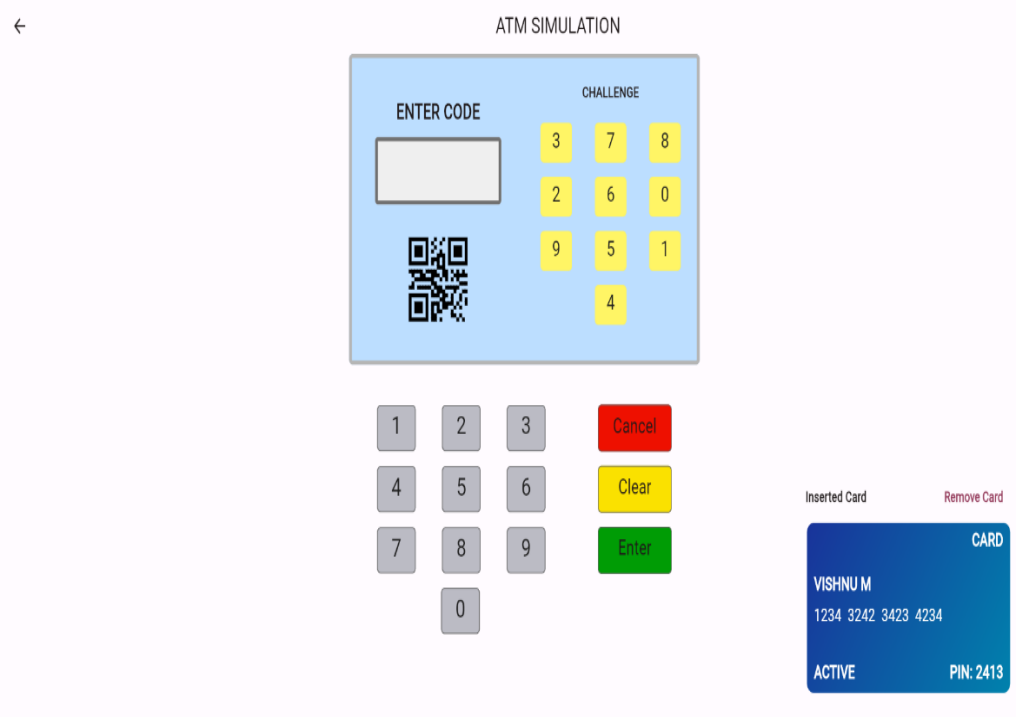
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 02, February 2024, pp : 250-253

e-ISSN : 2583-1062

Impact Factor : 5.725

After Inserting the Card:

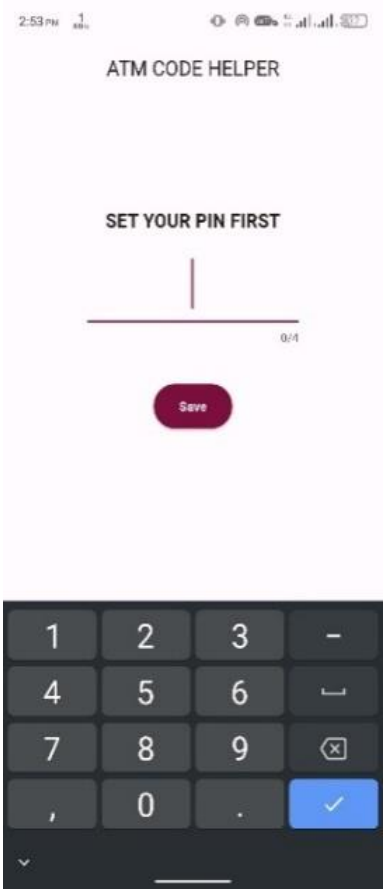


Here the QR Code as Well as the challenge keypad will be displayed on the screen so that the users can choose their way of solving according to their convenience.

Mobile Application Design:

The mobile application is designed using the Flutter framework, which enables cross-platform development for both iOS and Android devices. The application interface is designed to be intuitive and user-friendly.

Initial Setup



Initially the Users will have to setup the application with their original password.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

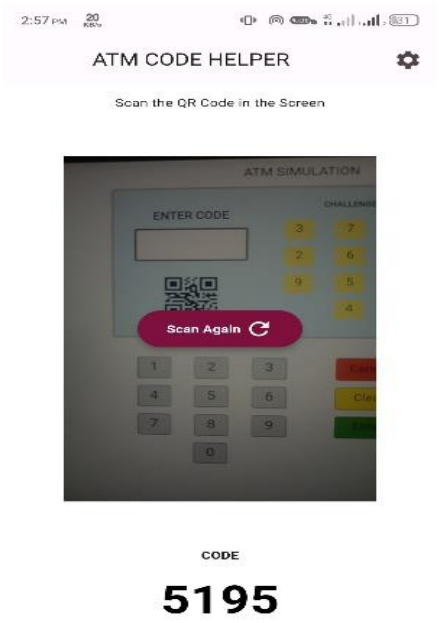
www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 02, February 2024, pp : 250-253

e-ISSN : 2583-1062

Impact Factor : 5.725

Post QR Code Scanning



Then the users will be able to scan the QR Code and the Solution will be displayed in the Screen itself which the user can enter in the simulator to get authenticated.

Challenge Generation Algorithm:

The Challenge Generation Algorithm is quite simple.

Steps:

1. Create an array which has all numbers from 0-9.
2. [1,2,3,4,5,6,7,8,9,0]
3. PHP has a build-in method called shuffle which shuffles an array in a random order.
4. Now send this shuffled array as a challenge to the client i.e the simulator application

5. CONCLUSION

The proposed QR based problem solving method enables all kind of people to get used to the Indirect PIN Entry methods without needing to have knowledge about how the system works. Although Indirect PIN Entry method has already been proposed it has not been implemented widely because of it's limitations such as the user should be able to solve the challenge in mind, the user should be educated and it takes a lot of time than the direct PIN entry methods. We addressed all these three limitations by leveraging the QR code technology.

6. REFERENCES

[1] FARID BINBESHR, LIP YEE POR, M. L. MAT KIAH, A. A. ZAIDAN and MUHAMMAD IMAM, "Secure PIN-Entry Method Using One-Time PIN (OTP)". In 2023 IEEE pp. 10.1109/ACCESS.2023.3243114 January 2023.

[2] Kabir, M. Monjirul, Nasimul Hasan, Md Khalid Hassan Tahmid, Tanjil Ahmed Ovi, and Victor Stany Rozario. "Enhancing smartphone lock security using vibration enabled randomly positioned numbers." In Proceedings of the International Conference on Computing Advancements, pp. 1-7. 2020.

[3] SM, Hari Krishna, Gautam Pradyumna, B. Aishwarya, and Chinmaya Gayathri. "Development of personal identification number authorization algorithm using real-time eye tracking & dynamic keypad generation." In 2021 6th International Conference for Convergence in Technology (I2CT), pp. 1-6. IEEE, 2021.

[4] Guerar, Meriem, Mauro Migliardi, Francesco Palmieri, Luca Verderame, and Alessio Merlo. "Securing PIN-based authentication in smartwatches with just two gestures." Concurrency and Computation: Practice and Experience 32, no. 18 (2020): e5549.

[5] Das, Indrajit, Ria Das, Shalini Singh, Amogh Banerjee, Md Golam Mohiuddin, and Avirup Chowdhury. "Design and implementation of eye pupil movement based PIN authentication system." In 2020 IEEE VLSI DEVICE CIRCUIT AND SYSTEM (VLSI DCS), pp. 1-6. IEEE, 2020.

[6] Jain, Shreyans, Shristi Dabola, Shikhar Binjola, and Rajni Jindal. "AlignPIN: Indirect PIN selection for protection against repeated shoulder surfing." In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 594-599. IEEE, 2021.