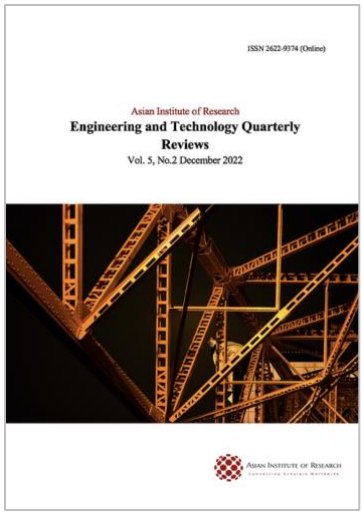

Engineering and Technology Quarterly Reviews

Maragathavalli, P., Aishwarya, Devi. V., Sharmila, J., & Nekkanti Bhavitha. (2023), A Novel Approach for UPI Seamless Transaction with Colour Code System by CASS Using Cloud Computing. In: *Engineering and Technology Quarterly Reviews,* Vol.6, No.1, 79-91.

ISSN 2622-9374

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Engineering and Technology Quarterly Reviews* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Engineering and Technology, including (but not limited to) Civil Engineering, Informatics Engineering, Environmental Engineering, Mechanical Engineering, Industrial Engineering, Marine Engineering, Electrical Engineering, Architectural Engineering, Geological Engineering, Mining Engineering, Bioelectronics, Robotics and Automation, Software Engineering, and Technology. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Engineering and Technology Quarterly Reviews* aims to facilitate scholarly work on recent theoretical and practical aspects of Education.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Engineering and Technology Quarterly Reviews
Vol.6, No.1, 2023: 79-91
ISSN 2622-9374

A Novel Approach for UPI Seamless Transaction with Colour Code System by CASS Using Cloud Computing

P. Maragathavalli[1], Aishwarya Devi V.[2], Sharmila J.[3], Nekkanti Bhavitha[4]

[1] Professor Information Technology, Puducherry Technological University Puducherry, India.
Email: marapriya@ptuniv.edu.in
[2] B. Tech Student Information Technology, Puducherry Technological University Puducherry, India.
Email: aishwaryadevivelmurugan@pec.edu
[3] B. Tech Student Information Technology, Puducherry Technological University Puducherry, India.
Email: jsharmi2002@pec.edu
[4] B. Tech Student Information Technology, Puducherry Technological University Puducherry, India
Email: bhavithachowdary127@pec.edu

Abstract
The rise of mobile payment applications like UPI has revolutionized the way transactions are carried out. However, with this convenience comes the risk of security breaches. One of the most common forms of attack is direct observation through shoulder surfing, where adversaries can notice the PIN entry during a transaction. To counteract this issue, a solution based on Covert Attentional Shoulder Surfing (CASS) has been proposed. This system is intended to provide high-level security to users during transactions, making it an excellent option for commercial and personal transactions. The proposed system provides various features that benefit users in the seamless transaction process. Overall, the proposed system is a reliable and secure option for mobile payment users, addressing the significant concerns of shoulder surfing and fraud detection. Compared to the existing system, our system has a 98 % accuracy rate, a high level of responsiveness. These improvements indicate that our system is more efficient and effective than the previous system.

Keywords: Advanced Behavior Analysis, Covert Attentional Shoulder Surfing (CASS), Mobile-Based Applications, Online Transactions, Platform-as-a-Service (PaaS), PIN Entry, Platform Independence, Shoulder Surfing, Unified Payment Interface (UPI).

1. Introduction

The Unified Payments Interface (UPI) is a mobile application that enables online transactions, offering a user-friendly and dependable platform. However, despite its advantages, UPI is without security concerns. One such issue is that the use of a personal identification number (PIN) during transactions can be observed by nearby

individuals, resulting in a potential direct observation attack through shoulder surfing. To address this issue, a solution has been proposed involving the implementation of Covert Attentional Shoulder Surfing, which offers high-level security. This approach was developed after recognizing the limitations of previous methods, which failed to address the aforementioned security pitfall. The proposed system provides various features that benefit users in the seamless transaction process. One such feature is Behaviour Analysis using Long Short-Term Memory (LSTM) where user input data is captured and analyzed to detect any behavioural anomalies that may indicate fraudulent activity. Another critical feature of this system is CASS, which aims to prevent shoulder surfing attacks. By hiding the user's PIN input from potential observers, CASS adds an additional layer of security to mobile transactions. Furthermore, the system is platform-independent, allowing users to connect to the mobile transaction applications from any platform

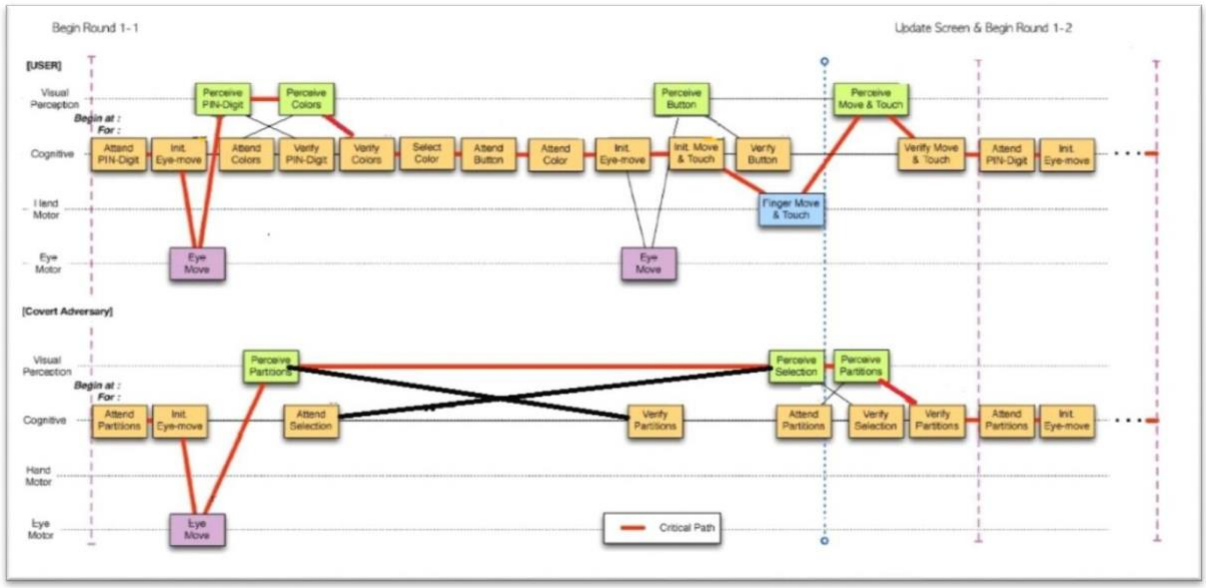

Figure 1: General Architecture of CASS

2. Motivation of the Proposed System

The motivation of our proposed system is to ensure that the user is aware of the insecure attacks by

- Providing a hassle-free e-payment transaction experience to users, which will reduce the time and effort required to complete online transactions.
- Enable a highly secure online transactions, using a color code PIN authentication system, that does not require users to remember complex passwords.
- Offer a more user-friendly experience by using color palette instead of numbers for entering PIN, which will make the system more accessible to users.
- Enhance security by blocking user accounts after three failed attempts, which will protect user’s data and prevent unauthorized access.
- Ensuring accessibility for the users irrespective of the platforms they use.

3. Literature Survey

Y. Zhou, B. Hu, Y. Zhang and W. Cai conducted a study on the implementation of cryptographic algorithms in dynamic QRcode payment systems and its performance, which was published in IEEE Access. However, their research revealed that the QR code payment system does not offer a high level of security and is costly to implement. As a result, this finding raises concerns about the security and cost-effectiveness of QR code-based payment systems.

The study conducted by Andriotis, Kirby, and Takasu in the International Journal of Information Security (2022) proposed adynamic graphical password scheme called Bu-Dash, which utilizes the Covert Attentional Shoulder Surfing technique. However, the research revealed that the proposed system did not provide any validation mechanism for ensuring the correct formation and input of Bu-Dash passwords. As a result, invalid entries could not be identified.

Kim, SI., Kim, SH conducted a study on an e-commerce payment model utilizing blockchain technology, which has the potential to provide secure transactions. However, the use of a public distributed transaction ledger system in the blockchain may increase the risk of disclosing personal identification data. Additionally, the process can be time-consuming, affecting the user's experience.

Hajek, P., Abedin, M.Z. & Sivarajah's research titled "Fraud Detection in Mobile Payment Systems using an XGBoost-basedFramework" employs a powerful Machine Learning technique to detect fraudulent activity in mobile payment transactions. However, the study only focuses on identifying the fraudulent transactions and does not propose any remedial measures to prevent future fraudulent activity.

4. Limitations of the Existing System

Online payments are susceptible to security breaches as there is no way to authenticate the authorized person, and biometrics can also result in false authentication. Without proper security measures, important financial information and data can be easily hacked by fraudsters. The current system only detects fraudulent activities after an attempted theft, making it ineffective in preventing financial information from being stolen. A more proactive approach is needed to detect and prevent fraud beforeit occurs, rather than just detecting it after the fact.

5. Proposed System

The proposed system is designed to provide a secure and convenient means of conducting commercial and personal transactions. Our solution incorporates advanced features, including behaviour analysis, Covert Attentional Shoulder Surfing (CASS), and platform independence using Platform-as-a-Service (PaaS), cloud computing technique.

5.1 Advanced Behaviour Analysis

The first feature of our proposed system is behaviour analysis. The system captures gesture data to understand the way users interact with their mobile devices. This data is stored and analyzed, and if any mismatch is found with the behavioural characteristics, fraudulency is detected, and an alert message is automatically sent. This feature can be particularly useful during commercial transactions where fraudulent activities are a concern.

5.2 Covert Attentional Shoulder Surfing (CASS)

The second feature of our proposed system is Covert Attentional Shoulder Surfing (CASS). This feature is designed to prevent direct observation attacks by intruders when a user enters a PIN. CASS plays a vital role in preventing shoulder surfing attacks and can be particularly useful during personal transactions such as person-to-person payments (P2P).

5.3 Platform Independent

Moreover, our proposed system is platform-independent, which means it can be used by all users who possess a bank account. The system provides various features for Unified Payment Interface (UPI) users to benefit them with seamless transactions. By supporting all mobile platforms, our proposed system facilitates most users to easily connect with mobile transaction applications from any platform.

In summary, our proposed system offers a versatile and secure means of conducting commercial and personal transactions. With advanced features such as behavior analysis using CASS, the system provides enhanced securityagainst fraudulent activity. Additionally, its platform-independent architecture ensures accessibility and ease of use, making it an ideal solution for a wide range of users, including UPI users.

6. Modules Description

6.1 Colour code PIN authentication

Here the variant method of PIN entry is used by which security is enhanced. Instead of standard PIN numbers, the color code with multi-touch technology is used to enter the PIN in public places. The multi-touch technology uses four standard colors for the PIN entry purposes. The colors used are standard with the reputation of colors in the keypad.

6.2 Submodules

6.2.1 Registration and Login Phase

In the registration phase the user can able to enter their respective bank details for the registration process. In the login phase user can able to login only if their login credentials exist in the database.

6.2.2 PIN Entry

The improved method displays a set of ten digits, $A = \{0, \cdots, 9\}$, on the regular numeric keypad with two split colors. The user will be provided with four colors and will have to select any one colour corresponding to the number displayed.

6.2.3 Account Summary

In this phase user can view the current bank account details and get notified.

6.2.4 Transaction Details

In this phase user can view all the money transaction details. And also the user can view the particular date or month of bank statement report.

6.3 Notification enablement

If the PIN entered by the user is incorrect more than three times the account of the respective user will be blocked . The notification will be sent if the entered color is invalid.

6.4 Unusual Online Payment Detection

6.5 E-commerce Integration

To prevent fraudulent transactions and ensure security, it is crucial to have proper authorization when handling large amounts of money. One method used to confirm the legitimacy of a large transaction is through the accessing cloud data. These classifiers analyze the transaction history of the user and calculate the mean and mode of previous transactions, which helps to establish a range of expected transaction amounts. By using this approach, the system can determine whether the current transaction falls within the expected range, providing an additional layer of security and reducing the risk of unauthorized transactions. This helps to protect both the user and the financial institution from potential losses due to fraudulent activity.

The e-commerce website has been interlinked with the color code PIN authentication system. This proposed system can be integrated and used by the individuals as well as the organisations in order to make the secured online transactions. It is also developed in such a way the users will not face any kind of difficulties in accessing the site which is provided with our enhanced platform independent approach. This colour code authentication system can be integrated with any type of applications like E-commerce

7. Detailed Design Diagram of Colour Code Pin Authentication System

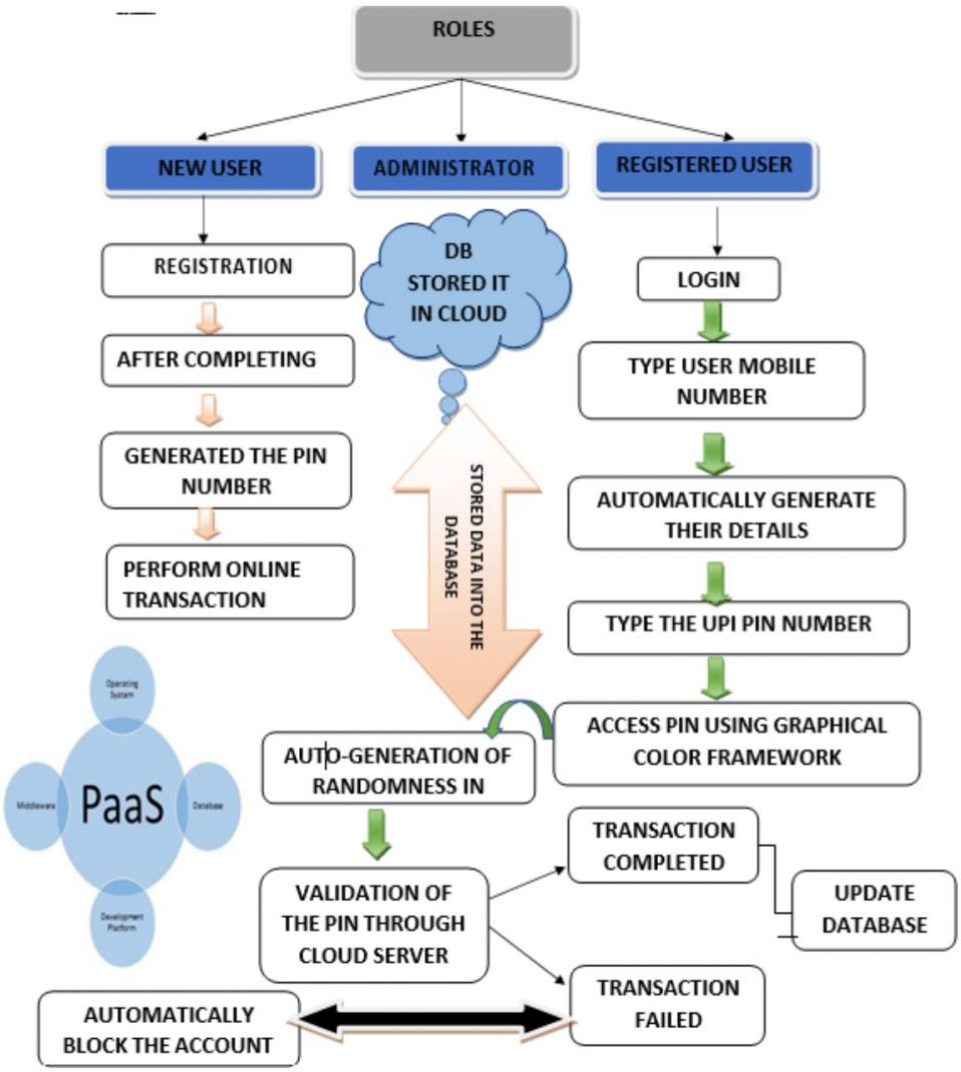

Figure 2: Detailed Design diagram of a proposed system

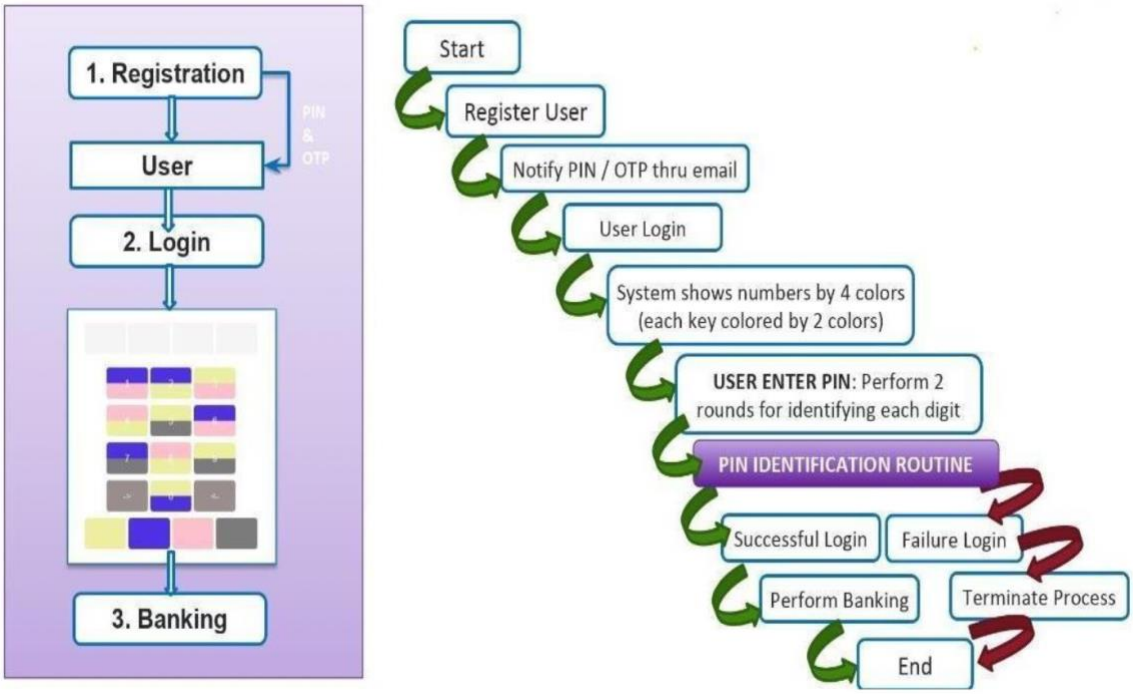

Figure 3: Work flow diagram of Color Code PIN Authentication System

8. Results

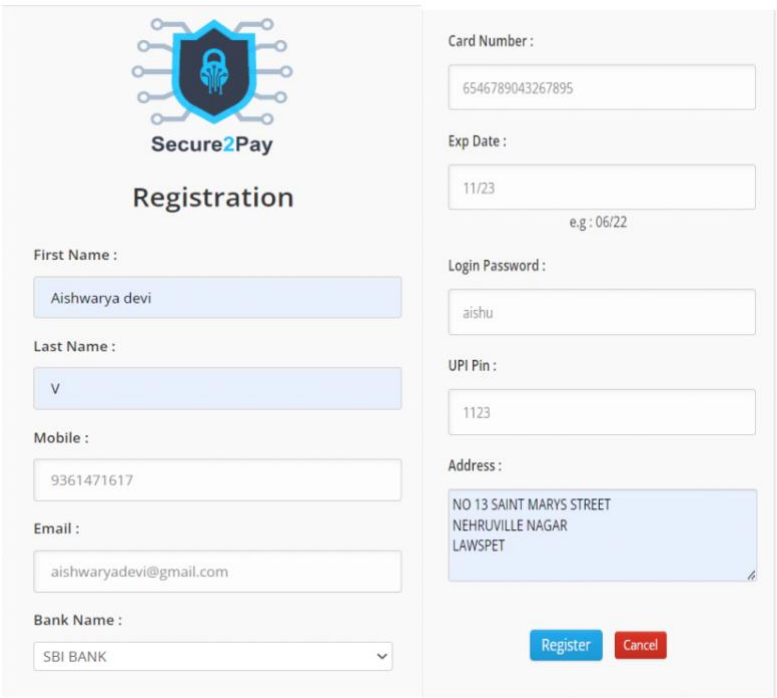

Figure 4: Registration phase

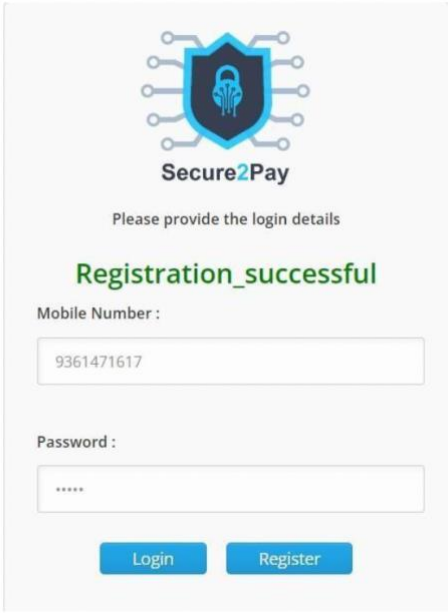

Figure 5: Secured Login phase after successful registration

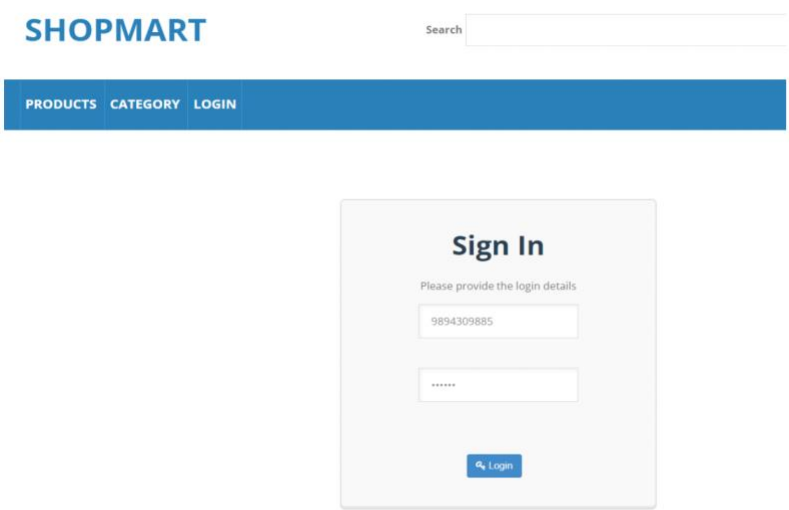

Figure 6: Login Phase for E-commerce website

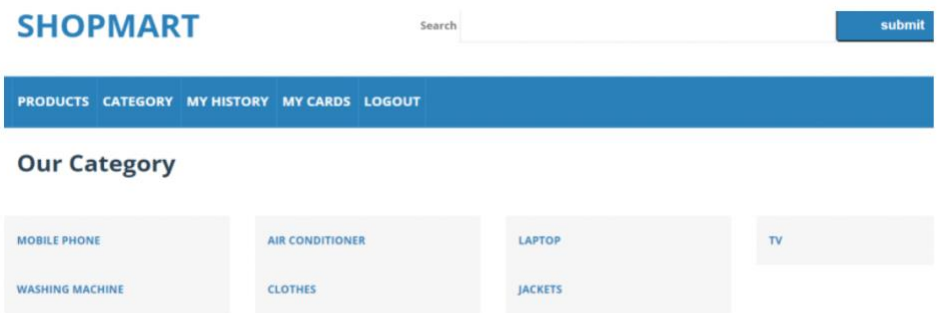

Figure 7: List of product categories in the site

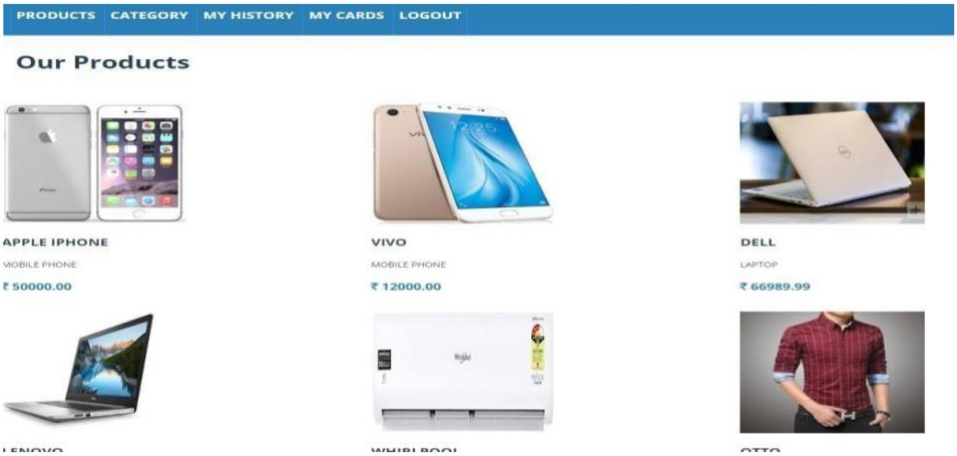

Figure 8: List of Products with price.

Figure 9: Displaying the details of the specific product

Figure 10: Adding the product to the cart

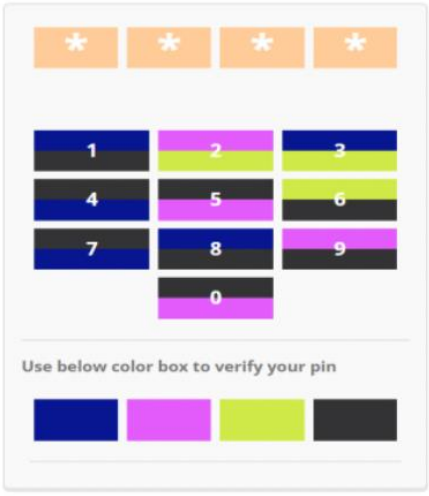

Figure 11: Proceeding to the payment portal

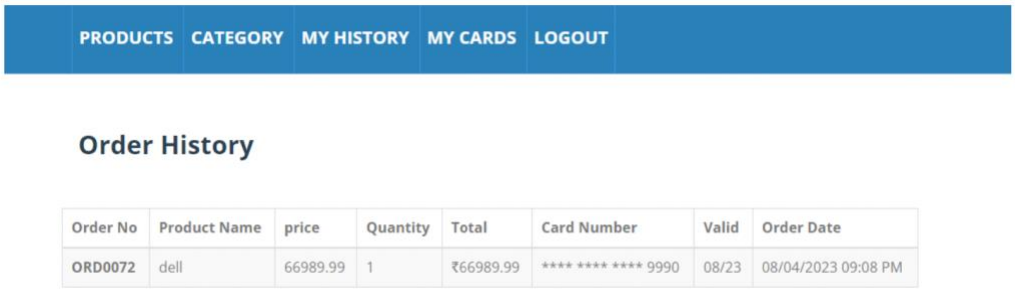

Figure 12: Displaying the history of orders in the site

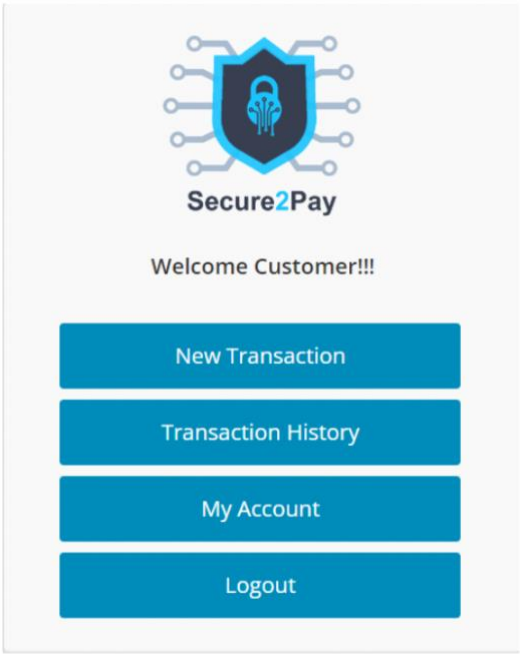

Figure 13: Dashboard for the end users for person to person transaction

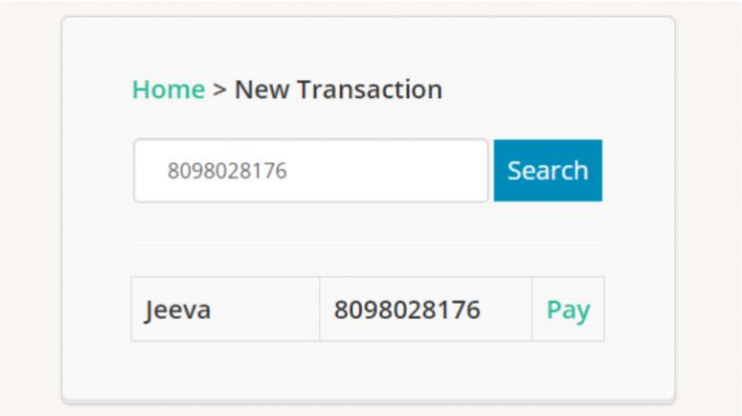

Figure 14: Entering the mobile number of the receiver

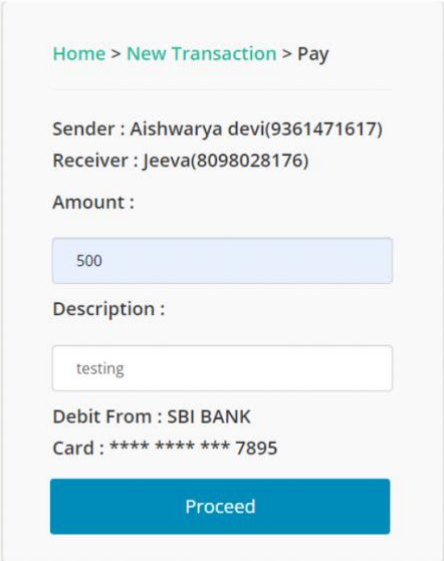

Figure 15: Entering the amount to be sent to the receiver

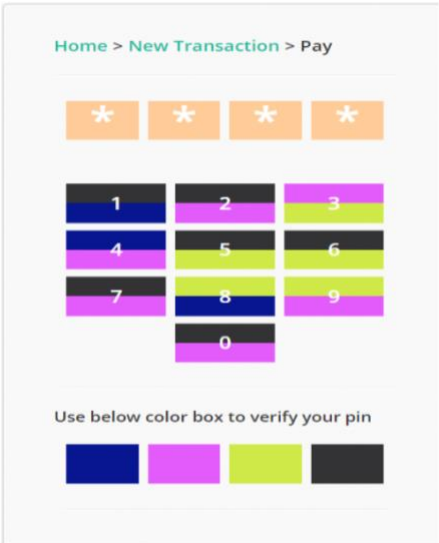

Figure 16: Colour palette PIN entry

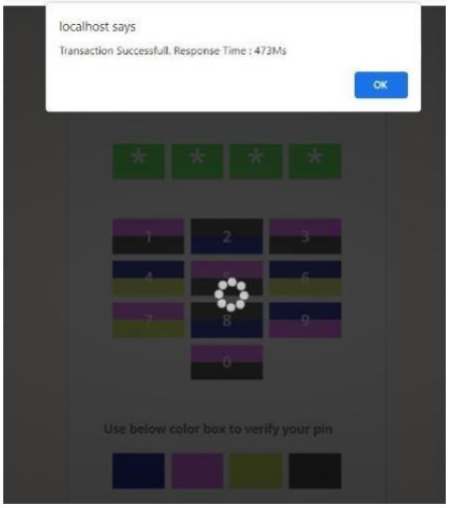

Figure 17: Notification of successful payment

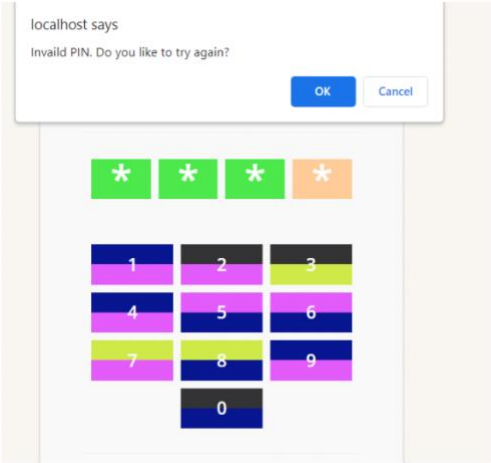

Figure 18: Notification of Invalid PIN

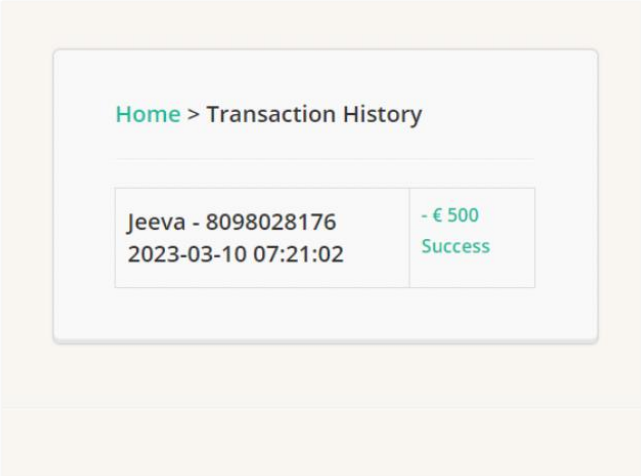

Figure 19: Transaction history

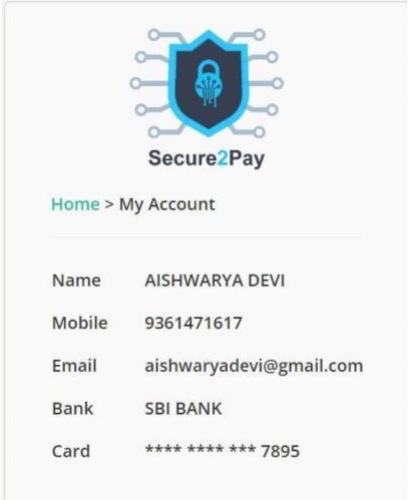

Figure 20: To view the account summary

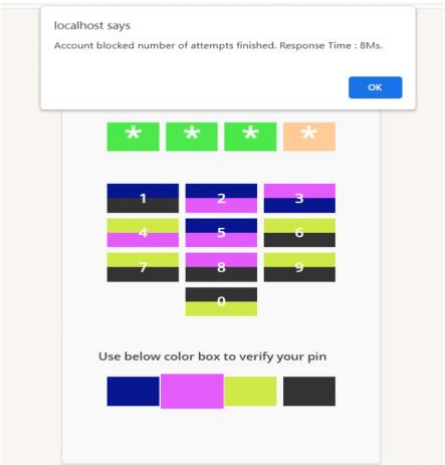

Figure 21: Notification for the blocked account

9. Result Analysis and Discussion

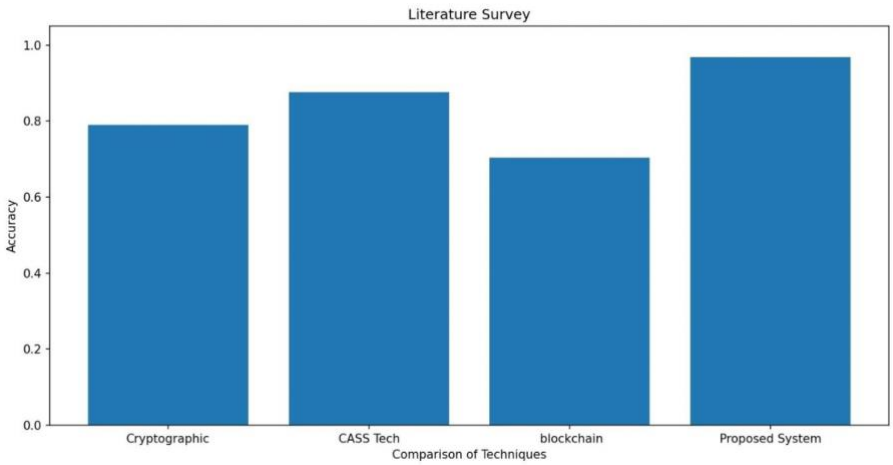

Figure 22: Result Analysis of Existing System with the Proposed System

As the Graph shows, there are various concerns regarding the security, cost-effectiveness, and user experience of current online payment systems. The following graph summarizes the findings of the studies mentioned:

The graph shows that the use of QR code-based payment systems is not highly secure and may be costly to implement, according to the study conducted by Zhou et al. The proposed graphical password scheme by Andriotis et al. did not provide a validation mechanism for correct input, and the blockchain-based e-commerce payment model studied by Kim and Kim may have privacy risks and could lead to a poor user experience due to the time-consuming process.

On the other hand, Hajek et al. showed that using machine learning techniques such as XGBoost can be effective in detecting fraudulent activity in mobile payment transactions. However, their study did not propose any remedial measures to prevent future fraudulent activity.

Overall, the graph highlights the need for more secure and user-friendly online payment systems, while also emphasizing the importance of addressing privacy concerns and providing comprehensive fraud prevention measures. Our Proposed System has more accuracy and less time latency and has a more security Concern than the existing Systems.

10. Conclusion

Our method is very efficient one and helps in seamless onboarding for the users. It has enhanced security features. Covert Attentional Shoulder Surfing (CASS) was the major technique that contribute for the most secured transactions. Our solution is also platform independent hence benefiting various users to access our UPI. This has been supported by an automatic fraud detector and recognizes the unauthorized user thereby, sending analert message to the bank as well as to the user. Hereby, we suggest that our solution of UPI is the most secured one as compared to the other applications and helps in seamless onboarding.

Acknowledgment

We are deeply indebted to Dr. P. Maragathavalli, Professor, Department of Information Technology, Puducherry Technological University, Puducherry, for her valuable guidance throughout the project work.

References

Andriotis, P., Kirby, M. & Takasu, A. Bu-Dash: a universal and dynamic graphical password scheme (extended version). Int. J. Information. Security. (2022). https://doi.org/10.1007/s10207-022-00642-2

Hajek, P., Abedin, M.Z. & Sivarajah, U. Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework. Information System Front (2022). https://doi.org/10.1007/s10796-022-10346-6

http://www.inderscience.com/storage/f112312849571016.pdf

http://www.inderscience.com/storage/f431712891151062.pdf

https://colorswall.com/palette/100916

https://gist.github.com/Njengah/415fa17bd93d5520b263434a7ee3f314

https://www.npci.org.in/what-we-do/upi/product-overview

https://github.com/topics/color-palette?l=python

K. K. Lakshmi, H. Gupta and J. Ranjan, "UPI Based Mobile Banking Applications – Security Analysis and Enhancements," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 1-6, doi: 10.1109/AICAI.2019.8701396.

Kim, SI., Kim, SH. E-commerce payment model using blockchain. Journal of Ambient Intelligence and Humanized Computing 13, 1673–1685 2022). https://doi.org/10.1007/s12652-020-02519-5

S. Fugkeaw, "Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain," in IEEE Access, vol. 10, pp. 49028-49039, 2022, doi: 10.1109/ACCESS.2022.3172973.

Y. Madwanna, M. Khadse and B. R. Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, pp. 150-154, doi: 10.1109/ICSCCC51823.2021.9478078.

Y. Zhou, B. Hu, Y. Zhang and W. Cai, "Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance," in IEEE Access, vol. 9, pp. 122362- 122372, 2021, doi: 10.1109/ACCESS.2021.3108189.