

# Enhancing Card Transaction's Security Through Cyber Security

Sudershan Manasvi Malhar<sup>1</sup>, Vasundhara Rao<sup>2</sup>, SVS Harshitha<sup>3</sup>,  
Swetha Mukka<sup>4</sup>, Sai Varshan<sup>5</sup>

<sup>1,2,3,4,5</sup>Student, Department of Information Technology, BV Raju Institute of Technology, Telangana, India

## Abstract

This paper highlights the security issues associated with credit cards and underscores the crucial role of encryption in mitigating the risk of credit or debit card data theft. Credit card encryption encompasses safeguarding the card itself, securing the terminal used for card scanning, and ensuring the protection of card information during transmission between the terminal and a backend computer system. The encryption mechanism is specifically engineered to validate and limit access to card security features. In our project, we developed a web application using VS Code, employing HTML for the frontend and PHP for the backend, and implemented AES encryption as a robust security measure.

**Keywords:** Encryption, AES, HTML, PHP, VS Code

## 1. Introduction

The authors of this paper recognize the importance of the Security concerns and the sensitive information linked with the credit cards and other payment systems. Since, covid usage of credit cards have increased promoting cash less transactions. Hence, the situation has led users to be vulnerable for any possible cyber-attacks.

To overcome this challenge, the authors proposed have proposed an extra layer of encryption to increase the security of current credit card transaction payment system. This layer is not only increasing the security but also decreases the hackers from tracking the user's personal information. Online transactions are leaving behind other means of transactions like Cash on delivery and usage of liquid cash in every nook and corner of the world. Everyone is preferring to make online transactions in an easy and secure manner. A cardholder obtains a credit or debit card from an issuing bank, uses the account to pay for goods or services. When a customer wants to make his/her payment through credit/debit card, initially the e-Commerce website will ask for the card details like Name of the card holder, validity and CVV. Once the details are validated, we receive an OTP from Bank server to make the transaction for the purchasing goods. Credit card encryption is a security measure used to prevent the likelihood of credit or debit card fraud transactions. But there are few chances of losing OTPs or confidential data easily by the hackers. Effortless bypassing of our OTP has become a common phenomenon in current world.

The application was tested with a sample group of customers to evaluate its performance and effectiveness. The results showed that the application significantly increases the security and improved customer satisfaction.

The application developed using VSCode platform and the front-end is developed by using languages HTML, CSS and Back-end is developed by using language php. Database has been supported by MySQL(xampp) The application has proven to be effective in increasing security and customers satisfaction.

This application is developed using powerful cyber security algorithm known as AES. AES stands for Advanced Encryption Standard. It is a symmetric encryption algorithm. This algorithm uses a 128-bit data block and may use three different key sizes 128, 196, 256 bits. The 128-bit data block is divided into 16 bytes and are mapped into a 4 x 4 array called state. It is an iterative algorithm. The total number of rounds  $N_r$  is dependent on key Length  $N$ .

## 2. Implementation

The central focus of this paper's web application primarily revolves around the concept of encryption. Encryption, in any context, plays a pivotal role in enhancing user security and attaining more satisfactory outcomes.

### Encryption

The procedure of encoding confidential information through encryption algorithms to prevent unauthorized access is employed in this process. In this encryption process, a combination of the AES (Advanced Encryption Standard) Algorithm and RSA is utilized to conceal data, effectively thwarting intrusive attacks. As AES encryption is applied, only the recipient with knowledge of the encryption key shared between sender and receiver can decrypt and access the data. In summary, encryption enhances data integrity and fosters trust among consumers.

The design of the user interface primarily emphasizes simplicity and user-friendliness, enabling customers to effortlessly upload their questions, provide answers only they know, make payments, and obtain their OTPs with minimal effort. The intuitive design ensures that customers can swiftly and efficiently complete these tasks without requiring extensive training or technical expertise.

## 3. Experimental Work

The web application discussed in this paper underwent a comprehensive testing phase involving a sample group of customers. The test results demonstrated that the application effectively enhanced the security of customer's sensitive information, reducing their vulnerability, and consequently leading to improved customer satisfaction and increased revenue for the printing service provider.

This heightened efficiency and enhanced customer satisfaction translated directly into boosted revenue for the banking service provider as well. The testing results underscored the application's remarkable effectiveness in generating additional income for the provider, establishing it as a valuable addition to their service portfolio.

The authors of this paper developed the web application using VS Code and a variety of web development languages, with the overarching goal of enhancing data integrity. The project's core idea is to enhance the customer experience in security-related scenarios. To achieve this, the authors introduced an additional layer of security, featuring a specific dialog box allowing users to provide a question as a means to verify their identity. This supplementary layer adds significant security, as the questions and answers can be personal and known only to the user. This enhancement leaves customers more satisfied and reassured, knowing that the application is more secure and their money is well-protected.

In a broader context, the inclusion of an OTP (One-Time Password) in credit card transactions permits users to add an extra layer of security. However, it's essential to note that if an attacker gains access to the user's mobile number, they can potentially intercept the OTP, jeopardizing the user's funds and financial security.

### The steps involved in this process are:

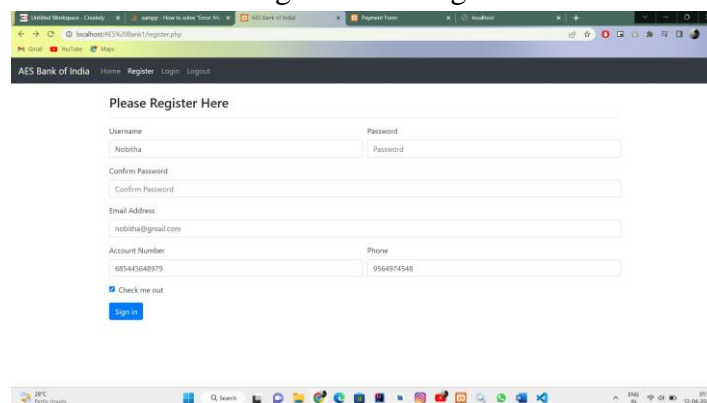
- Users are required to register their identity on the AES Bank of India's server by providing the necessary information.
- Subsequently, the customer proceeds with the checkout process and opts to make a payment using either a credit or debit card by submitting their card details.
- The card details are shared with the website or any other platforms responsible for processing the transaction. These platforms securely transmit the card details, along with transaction information, to their payment gateway.
- The payment gateway, in turn, securely transfers this transaction information to the payment processor employed by the merchant's acquiring bank.
- The payment processor then forwards the transaction information to the card association.
- The card association passes on the transaction information to the customer's issuing bank. The issuing bank checks for adequate funds to complete the transaction and performs fraud checks to ensure the transaction's legitimacy.
- To ascertain the legitimacy of the transaction, the service provider's servers send an OTP along with additional security questions as requested by the service provider's server.
- The customer's issuing bank provides a response to the card association, indicating whether the transaction is approved or declined.
- The card association relays this response back to the merchant's payment processor.
- The payment processor communicates this response to the payment gateway.
- The payment gateway informs both the customer and the merchant of the transaction response.

## 4. Results

### 4.1 Registration Phase

#### Home Page

Fig 1: Home Page



The screenshot shows a web browser window displaying the registration page for AES Bank of India. The page title is "Please Register Here". The form includes the following fields: Username (filled with "Nobitha"), Password, Confirm Password, Email Address (filled with "nobitha@gmail.com"), Account Number (filled with "654456489779"), and Phone (filled with "9564974548"). There is a "Check me out" checkbox and a "Sign In" button at the bottom.

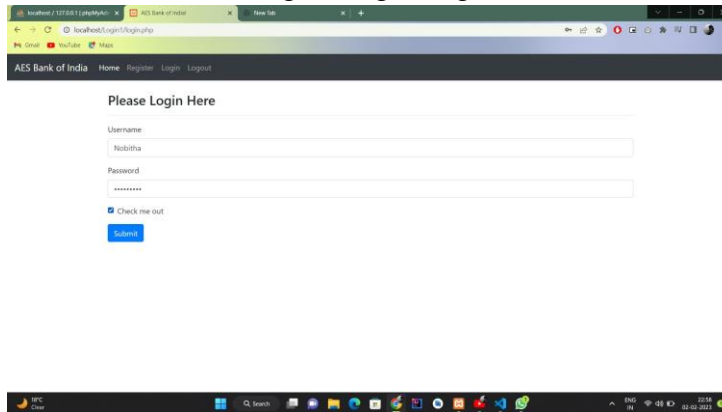
The Home screen of our web application is designed to fill the basic details of the customer that are required to sign in. This page contains the details of the customer such as user name and password. Authors have kept in mind about the customer's technical capabilities and have design the application in such a

way that any person without any proper technical knowledge can use the application and get satisfactory results with respect to their situation.

The information taken in this page are basic details just to register the identity of the user. This page include name, phone number, address and check box to confirm the inputs.

## Login Page

Fig 2: Login Page

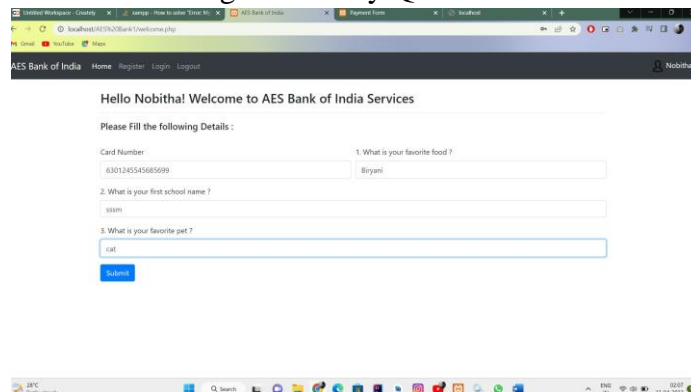


The initial homepage or sign-in page contains essential customer details needed for account registration. To enhance security and ensure successful registration, it is advisable for customers to log in once more to confirm their account setup, assuring their readiness for future logins.

The authors primary objective was to develop the most straightforward and engaging web application to boost the service provider's revenue and enhance customer satisfaction. Given the abundant resources available in the market, it was crucial for the authors to create a product that stands out and is user-friendly. Consequently, the user interface has been designed to be straightforward and easy to navigate, catering to customers with varying levels of familiarity with online card transaction methods, from novices to experts. This page requires customer action, involving the input of various details such as a login ID and password.

## Customization

Fig 3: Security Questions



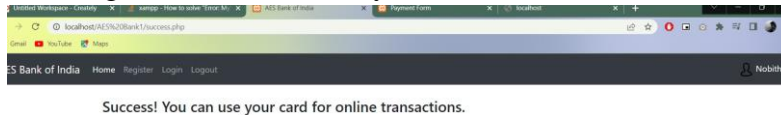
The "Customization" screen of our web application is designed to give customers complete control over their question-and-answer decisions.

This screen includes several key components, such as:

**Credit card number:** This component allows customers to preview their document before printing, ensuring that the final product meets their exact specifications. With its user-friendly interface and robust customization features, the “Customization” screen of our web application helps ensure that customers are able to produce the exact prints they require, every time.

## Success Page

Fig 4: Status of Security Questions Customization

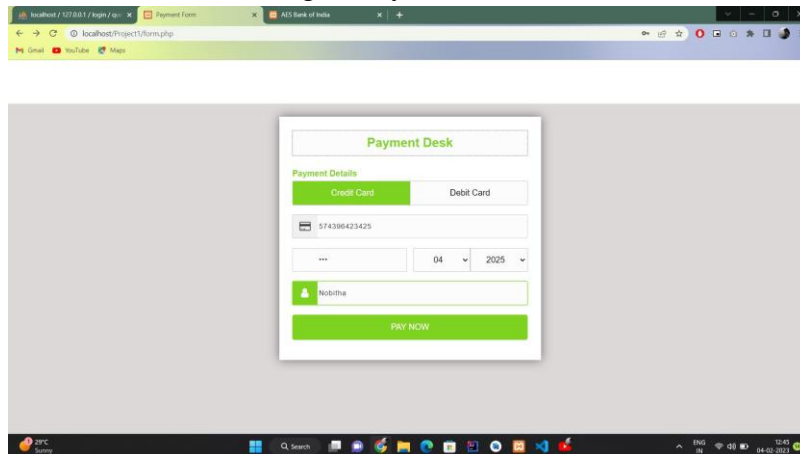


This page indicates the successful registration of the candidate.

## 4.2 Transaction Phase

### Payment Desk

Fig 5: Payment Desk



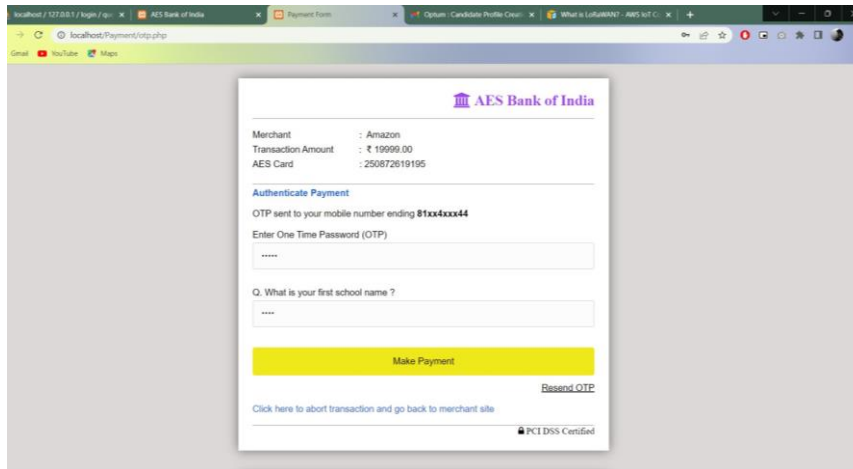
This is the initial page of the transaction phase and this page contains some confidential and sensitive information of the user such as

- Card Holder Name
- Card Number
- CVV
- Expiry Date

Users are required to input the specified information in order to verify their legitimacy. This process aims to enhance user protection against cyber threats and bolster data security.

## Authentication

Fig 6: Security Question & OTP Authentication



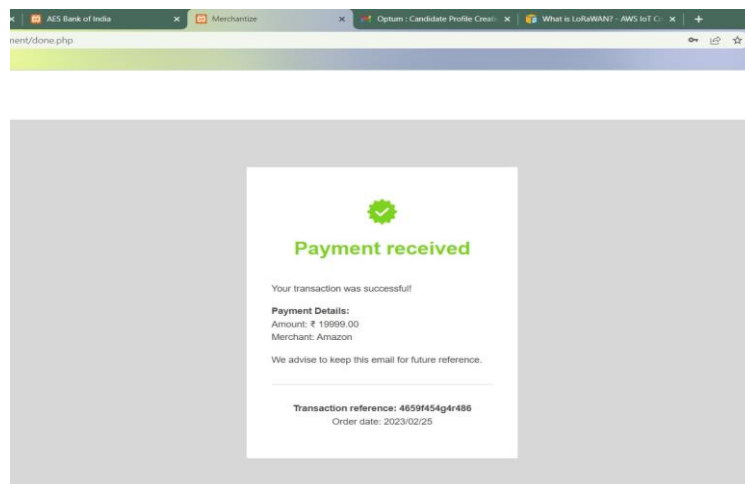
This is one of the most critical steps in the transaction process. Here, users are asked to give certain inputs which are used to authenticate the user's identity and to check whether the transaction is not fraudulent. In this page there are certain dialog boxes which take the inputs such as:

- OTP
- Security question

After this process, the transaction is processed to further stages.

## Transaction Status

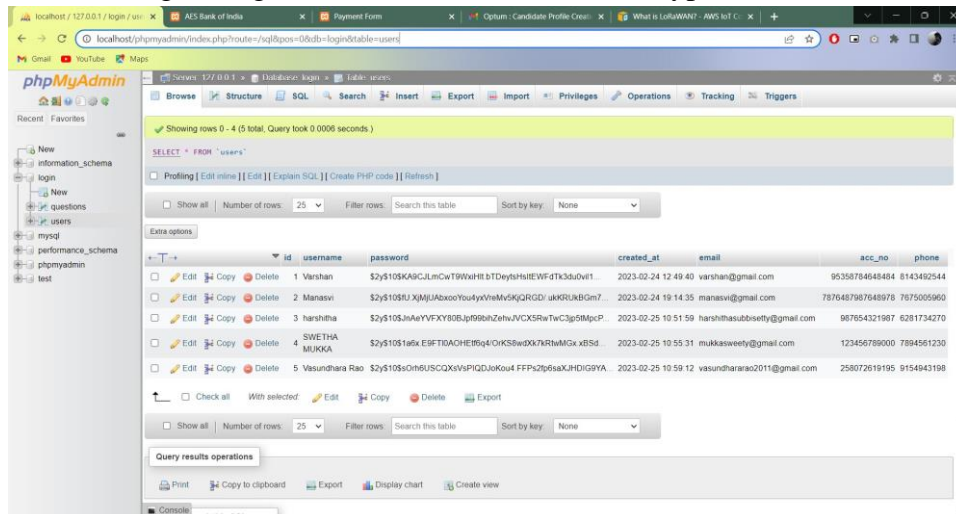
Fig 7: Transaction Status



This is the final page of the web application. In this page, the given output indicates the status of the transaction.

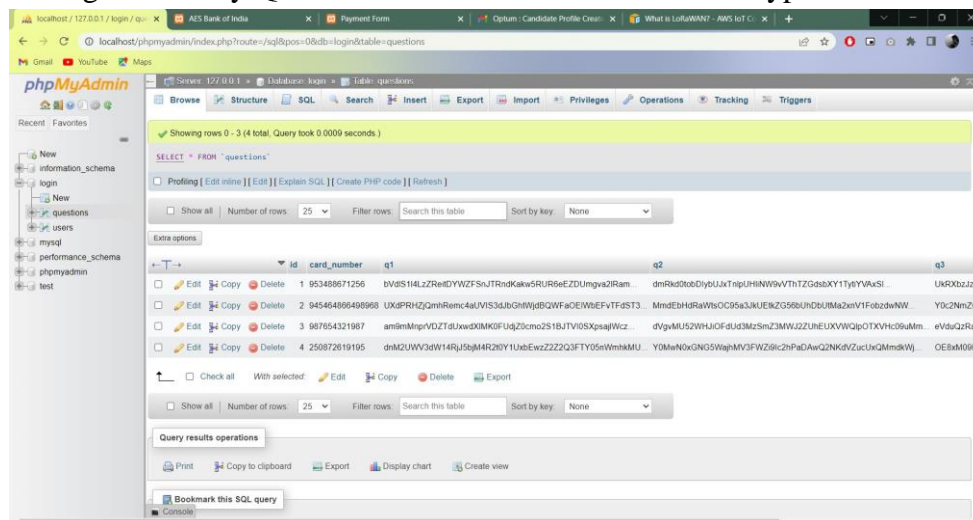
## Database

Fig 8: Login credentials Stored in an Encrypted Format



The user’s information and their given inputs are stored here. Authors of this paper have kept the passwords encrypted to increase customers privacy using one way password hashing.

Fig 9: Security Questions & Answers Stored in an Encrypted Format



## 5. Conclusion

In conclusion, enhancing the existing transaction process with an additional security layer is a crucial and forward-thinking initiative. By implementing this project, we are not only addressing current vulnerabilities but also proactively safeguarding sensitive information and financial transactions. This enhancement ensures trust and confidence among users, instilling a sense of security and reliability in the system. Moreover, it signifies a commitment to staying ahead of potential threats, embracing the ever-evolving landscape of cybersecurity, and ultimately, fostering a safer environment for all stakeholders involved.

As we move forward, continuous monitoring, adaptation, and innovation will be key to maintaining the integrity of this security layer, thereby upholding the standards of confidentiality, integrity, and availability in every transaction conducted.

## 6. References

### Books

1. A.Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar “Securing Online Transactions with Cryptography and Secured Authentication Methods”. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277- 3878 (Online), Volume-8, Issue-1, May 2019.
2. Halunen, Kimmo & Sailio, Mirko. (2014). “Identity-Based Cryptography in Credit Card Payments”. 49-58. 10.1007/978-3-662-44893-9\_5.

### Papers

1. "Secure Credit Card Transactions using AES Encryption" by R. Anitha and V. Kalaivani: This paper proposes a method for encrypting credit card data using AES and discusses the security implications of using this method. It also compares the proposed method to other encryption techniques and analyzes the performance of the system.

### Websites

1. <https://ieeexplore.ieee.org/document/6567226>.
2. <https://www.apachefriends.org/>
3. <https://code.visualstudio.com/>
4. <https://www.creditcards.com/>
5. <https://www.emerchantpay.com/insights/>
6. <https://www.fisglobal.com/en/insights/merchant>



Licensed under [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)