WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Machine Learning Based Secure Digital Transactions

S. Parthasarathy[1], Dr. C. Kumuthini [2]

[1]Student, Department of Computer Applications, Dr. N.G.P. Arts and science college, Coimbatore.
[2]Professor, Dr. N.G.P. Arts and science college, Coimbatore. kumuthini@drngpasc.ac.in

A B S T R A C T

The credit card fraud detection is used to detect the credit card was on the mode like the detection occurs only after the complaint of the card holder about fraud done. It is not a convenient way to avoid the loss happens to the card holder. After getting the complaint they detected the fraud on the basis of the IP address. For this they need the help of the Cyber crime to detect the fraud and make action on it. The proposed method aims to prevent credit card fraud during online purchases by implementing multi-level authentication. Users register and log in to the system to make purchases and payments via credit cards. The application allows users to set a purchase threshold, and if a transaction exceeds this limit, it triggers a multi-level verification process. This includes answering a security question followed by OTP verification via email. If the user fails these checks, the card is automatically blocked, ensuring secure. The another verification process is done by using the method as pattern matching. The pattern matching is one of the familiar method in machine learning algorithm is used to verify the security question ask in the childhood name as match in the stored data. If its match, the user proceeds purchase process completion with the help of their Customized Threshold Limit Estimation.

Keywords: Fraud Detection, Cyber Crime, OTP, Machine Learning, Pattern Matching

1. Introduction

Online payments using credit cards are common in today's digital world, but they also increase the risk of credit card fraud. The "Secure Digital Transactions" (fraud detection system) proposed work aims to protect users from such fraud by providing a secure payment system. This web-based application is developed using Python and MySQL. Users can register, log in, view their purchase history, and make payments securely [1].

To ensure safety, the system includes a multi-level authentication process. If a transaction exceeds a user's set purchase limit, the system asks a security question. After that, an OTP is sent to the user's email for verification. If the user fails these checks, the system blocks the credit card to prevent misuse. The work also has a fraud detection system that monitors transactions and sends alert emails if suspicious activity is found. This system provides a safe and reliable platform for online payments and protects users from unauthorized transactions [2].

2. Literature Review

1. Using ResNet-50 for Fraud Detection (Mahesh Valentina G, 2024)

Mahesh Valentina G. (2024) explores using ResNet-50, a deep learning model, to detect fraudulent online transactions. The model's deep layers can improve fraud detection accuracy by combining it with decision trees to reduce errors and improve precision.

2. Machine Learning for Online Payment Fraud (Almazroi & Ayub, 2023)

Almazroi and Ayub (2023) examine various ML techniques like Random Forest and Neural Networks for detecting fraud. They suggest that these methods can learn from transaction data and improve over time, offering better fraud detection than traditional systems.

3. Cost-Sensitive Decision Trees for Fraud (Sahin, Balkan, & Duman, 2013)

Sahin et al. (2013) propose using cost-sensitive decision trees, which put more weight on detecting fraud (often rare in datasets). This approach improves accuracy by reducing false negatives, meaning fewer fraudulent transactions are missed.

4. Comparing Machine Learning Techniques (Awoyemi, Adewunmi, & Oluwadare, 2017)

Awoyemi et al. (2017) compare several ML methods, including Decision Trees and Neural Networks, for credit card fraud detection. They find that ensemble methods like Random Forest perform better than single models, especially when using multiple transaction features.

5. Isolation Forest for Anomaly Detection (Liu, Ting, & Zhou, 2008)

Liu et al. (2008) introduce the Isolation Forest method, which detects fraud by identifying unusual transactions. It is effective for large datasets and imbalanced data, making it useful for fraud detection.

6. Fraud Detection with ML (Patil & Kulkarni, 2020)

Patil and Kulkarni (2020) highlight various ML techniques like SVM and Decision Trees for real-time fraud detection. They recommend using a hybrid approach that combines multiple methods for better performance.

7. Survey on Credit Card Fraud Detection (Kaur & Singh, 2017)

Kaur and Singh (2017) provide an overview of fraud detection techniques, from rule-based methods to modern ML approaches. They note the growing trend of using hybrid models that combine multiple techniques to improve detection accuracy.

3. Proposed Methodology

The various steps involved in the proposed work online secure digital transactions are listed below,

1. User Registration and authentication

This module is mainly based on user. Using this module user can register in the registration form he has to fill with personal details such as name, address, mobile number mail-id and username, password etc. This will maintain in a separate table. Using this password user and admin can log on this web application. After the successful login they can use app feature effective manner.

2.Upload Card Information

This module is fully based on Admin control. In this application admin has to upload card holder information Such as, Card Holder name, Card Number, Limit, Valid from and Valid to etc., This information will be maintained in a separate table.

3. Customized Threshold Limit Setting

This module is fully based on user control. The user can view card information and set threshold limit to their card for security reason. This information will be maintained in separate table.

4.Product Buying Process

This module based on user side. After successful of user login, they can purchase the product in this website. Purchase details include user name and purchase type, purchase id, date of purchase, product name, total quantity, amount etc., In this all information to be stored into purchase table. In this purchase table order id set as primary key to avoid duplicate entry.

5.pattern Matching

Pattern matching is a machine learning Searching Algorithms and is considered as a part of the String algorithms. These algorithms are useful in the case of searching a string within another string. Once user purchase process completion this pattern matching algorithm verify with user Customized Threshold Limit Estimation.

6.Multi level verification

If user billing amount exceed with purchase thresholds level this application asks Multi level verification system. initially this application asks security question once user successfully submit the correct answer this application ask OTP security code this will receive user via mail. Once multi-level authentication failed application automatically block the card. This wills high level of security. Hacker cannot able to misuse credit card.

4. Proposed Fraud detection system

Methods on objects are functions attached to the object's class; the syntax instance. Method(argument) is, for normal methods and functions, syntactic sugar for Class. Method (instance, argument). Python methods have an explicit self-parameter to access instance data, in contrast to the implicit self (or this) in some other object-oriented programming languages.

1. User Registration and Login

Users register by providing their details, which are securely stored in a MySQL database. Only registered users can log in and access the system, ensuring secure and authorized transactions.

2. Transaction Handling

When a user makes a purchase, the system stores the transaction details. Users can view their purchase history. The system also checks if the transaction exceeds a set purchase limit for added security.

3. Multi-Level Security Check

If a transaction exceeds the user's limit, the system asks a security question. If answered correctly, an OTP is sent to the user's email. Users must enter the OTP to complete the payment. If they fail, the system blocks the card.

4. Fraud Detection and Alerts

The system monitors all transactions. If it detects suspicious activity, it sends an alert via email. If multi-level verification fails, the card is automatically blocked to prevent fraud.

Flow Diagram of secure digital transformation

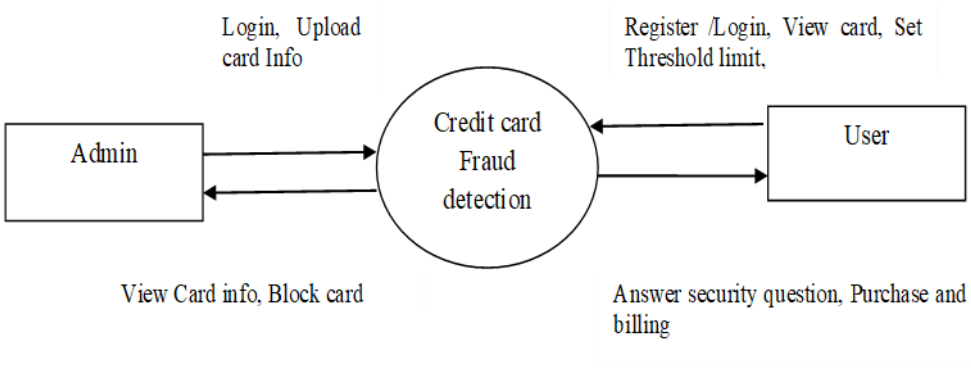


Figure 1: Overall flow diagram of fraud detection system

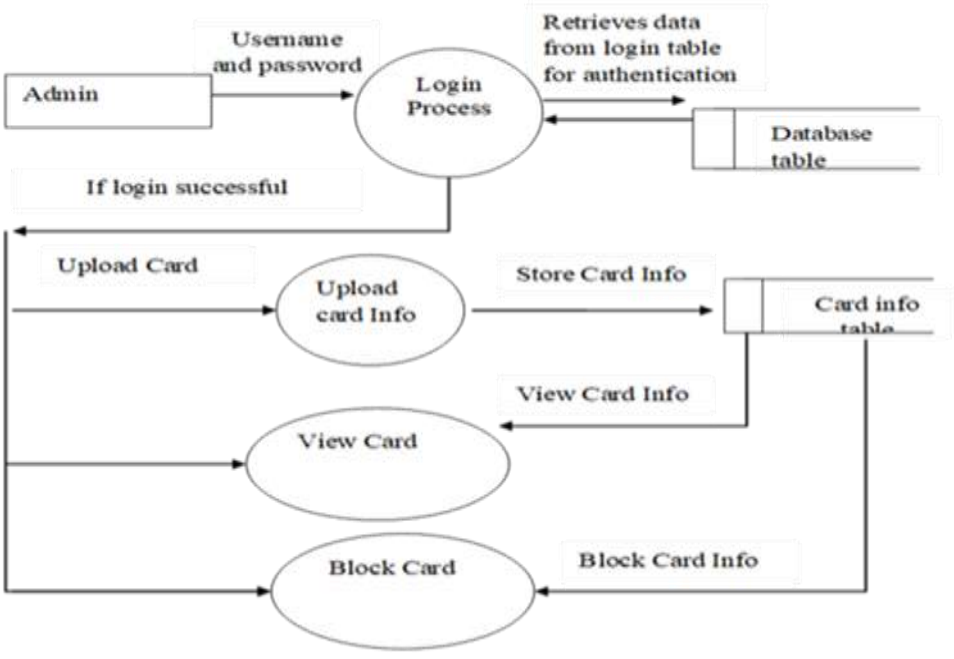


Figure 2: Data movement between the admin, processes, and databases within the Credit Card Fraud Detection System

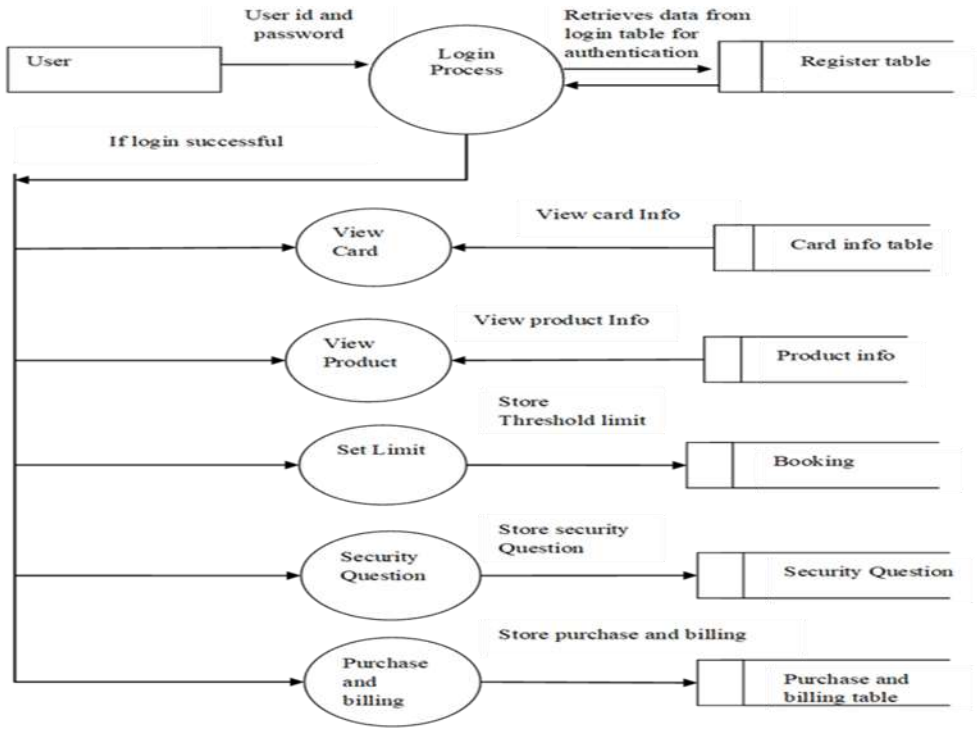
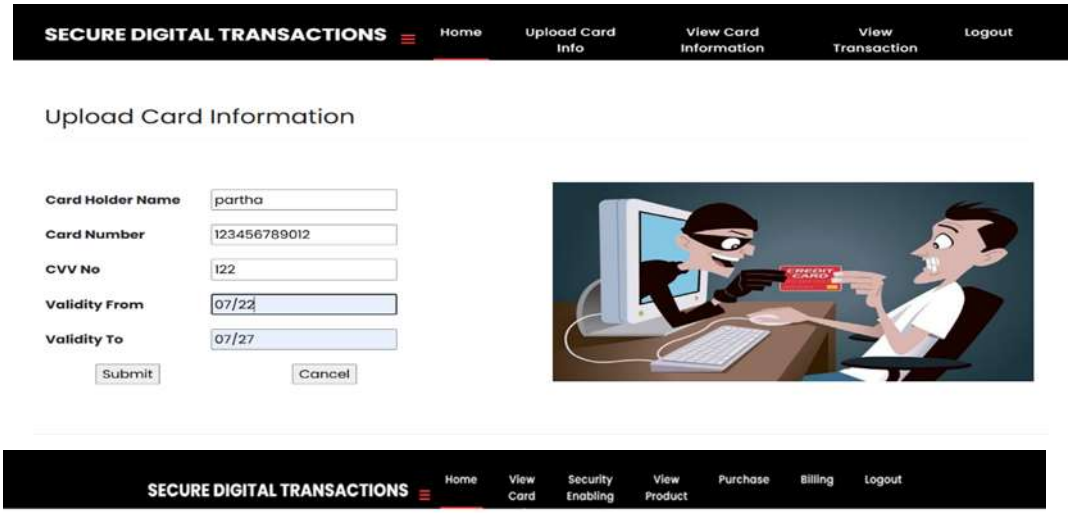
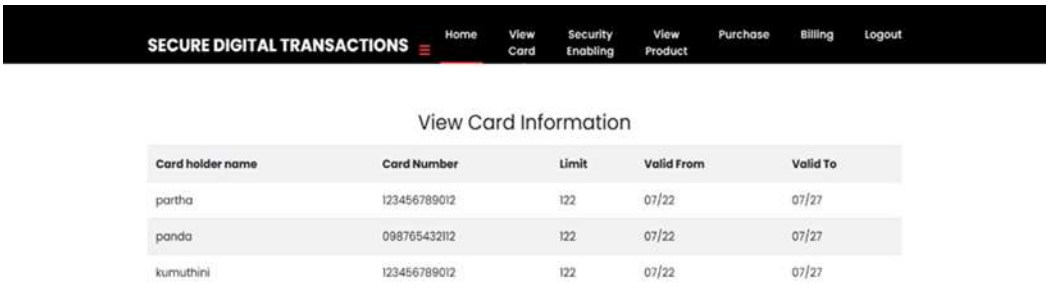


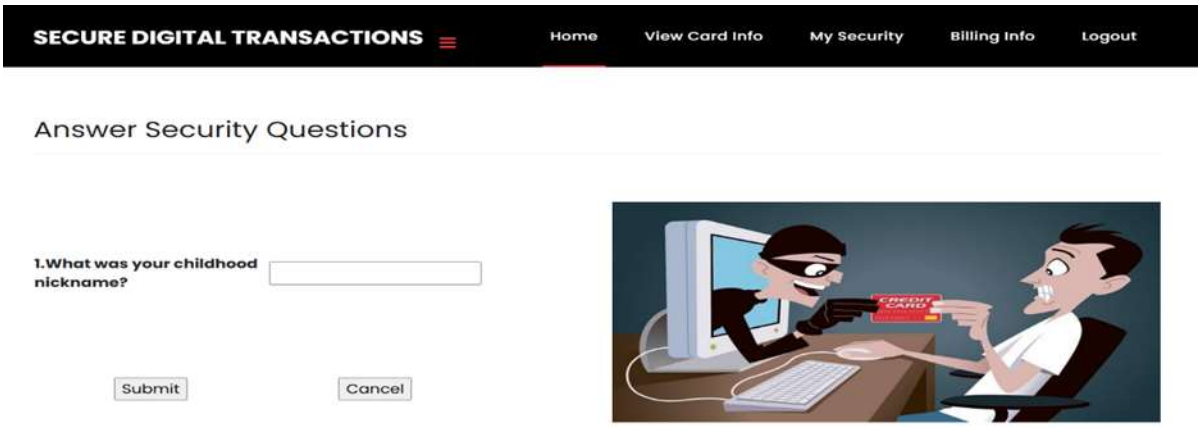
Figure 3 : System's functionality, emphasizing the interaction between the user, various processes, and multiple data storage tables.

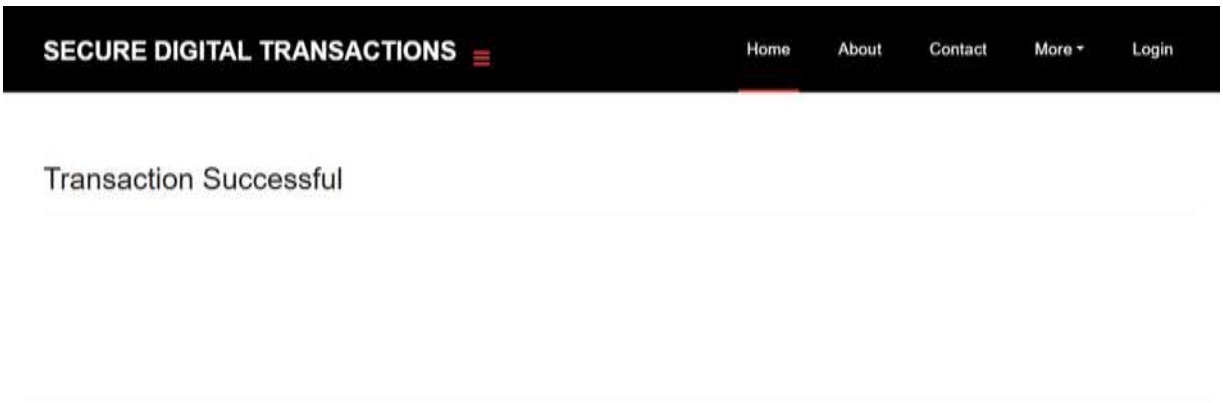
5. Modelling and Analysis





Card holder name	Card Number	Limit	Valid From	Valid To
partha	123456789012	122	07/22	07/27
panda	098765432112	122	07/22	07/27
kumuthini	123456789012	122	07/22	07/27





6. Conclusion

Implementation is the stage of the proposed work when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. This module

enables the user to use a banking application. The main goal of this application is to minimize financial losses for both cardholders and card issuers by quickly identifying and stopping unauthorized or suspicious transactions. The beneficial is employing fraud detection especially those that use machine-learning algorithms and behavioral analysis can flag suspicious transactions before they are processed.

7. REFERENCES

Mahesh Valentina G(2024)Enhancing the fraudulent behavior in online transaction using ResNet-50 in searching the purpose of decision trees to enhance precision5TH INTERNATIONAL CONFERENCE ON MATHEMATICAL SCIENCES (ICMS5)10.1063/5.0228167(020002).

Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. IEEE Access, 11, 137188-137203

Sahin, Y., Balkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications*, 40(15), 5916-5923.

Awoyemi, J. O., Adewunmi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *Journal of Applied Security Research*, 12(1), 1-12.

Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. *Eighth IEEE International Conference on Data Mining*, 413-422.

Patil, V., & Kulkarni, R. (2020). Detection and prevention of online transaction fraud using machine learning. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 9(3), 562-567.

Kaur, H., & Singh, M. (2017). A survey on credit card fraud detection techniques. *International Journal of Computer Applications*, 164(1), 1-5.