e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 2, February 2024 |

| DOI:10.15680/IJMRSET.2024.0702011 |

Money Transaction in E-Commerce Applications Using Biometric Methods

P.Sathiyapriya, K.Boopathi, K.Kumana vallal, S.Akash

Assistant Professor, Department of Cyber Security,Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security,Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security,Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security,Muthayammal Engineering College, Rasipuram, India

ABSTRACT: In response to the escalating threat of online transaction fraud in the financial industry, a robust system has been developed to safeguard transactions, particularly those surpassing the customer's established transaction limit.[1] This innovative framework relies on a Fraud Detection System (FDS) that meticulously assesses each transaction, promptly declining any flagged as potential fraud. To fortify transaction security, the system scrutinizes user spending patterns and geographical location, utilizing this information to verify the user's identity.[2] Any deviation from established patterns triggers a re-verification process, ensuring that potentially fraudulent activities are subjected to additional scrutiny.

Drawing insights from the user's historical transaction data, the system adeptly identifies irregularities in the payment procedure, adding an extra layer of defense against unauthorized transactions. To deter malicious actors, the system implements a stringent policy: after three unsuccessful attempts, the user is automatically blocked from further transactions.[3] This proactive measure serves as a deterrent against brute force attacks and unauthorized access. In the event of suspicious activities indicating a potential security breach, the system promptly alerts the user, providing real-time notifications to keep them informed. This dynamic approach not only prevents fraudulent transactions but also empowers users with timely information, fostering a secure and vigilant online financial environment.[4]

I. INTRODUCTION

The surge in online transactions has undeniably brought convenience to consumers, but it has also ushered in a concerning rise in online transaction fraud, significantly impacting the financial industry. As technology evolves, so do the tactics employed by fraudsters, necessitating advanced systems to counteract these threats. In response to these challenges, a sophisticated system has been developed to specifically address transactions exceeding a customer's current limit, bolstering security measures to safeguard against fraudulent activities. At the core of this innovative framework is a Fraud Detection System (FDS) that rigorously evaluates each transaction. If the FDS identifies a transaction as potentially fraudulent, the system prompts the bank to decline the transaction, thereby preventing unauthorized access to financial resources. To enhance identity verification, the system leverages user spending patterns and geographical location, adding an extra layer of protection by ensuring that transactions align with established user behavior.

Recognizing the dynamic nature of fraud, the system employs continuous monitoring. If any unusual patterns emerge during a transaction, the system initiates a re-verification process, further scrutinizing the legitimacy of the transaction. Drawing insights from the user's historical data, the system adeptly identifies irregularities in the payment procedure, contributing to a proactive defense against potential threats. In response to multiple failed attempts at verification, the system takes a decisive step by blocking the user after three invalid efforts. This stringent measure acts as a deterrent against brute force attacks and unauthorized access, fortifying the security of the online transaction environment. Furthermore, in the unfortunate event of malicious activity, the system promptly notifies the user, keeping them informed in real-time. Contrasting this advanced system with the manual processes of the existing system reveals significant shortcomings. The current approach relies on a formatted online shop system for sales, entailing extensive paperwork.

The Grassmann manifold, a mathematical space representing all possible subspaces of a fixed dimension in a high-dimensional space, becomes instrumental in comparing the subspaces that represent facial features. Each face is then represented as a subspace in the feature space, with the Grassmann algorithm projecting these subspaces onto the

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 2, February 2024 |

| DOI:10.15680/IJMRSET.2024.0702011 |

Grassmann manifold. This process creates a set of points that can be effectively compared, forming the basis for subsequent distance computation. Distance computation, utilizing a distance metric such as the Grassmann distance, takes into account the geometry of the Grassmann manifold. This computation provides a measure of how similar or dissimilar the subspaces are, offering valuable insights into the distinctiveness of facial features. The final step involves classification, where computed distances are utilized to classify faces into known or unknown individuals. This critical step incorporates setting a threshold value for the distance metric, above which a face is considered unknown. This classification process ensures the accurate identification of individuals, adding an extra layer of security to the system. In conclusion, this comprehensive system not only addresses the escalating challenges of online transaction fraud but also introduces a transformative approach to online shopping. The integration of face detection and the Grassmann algorithm brings forth a secure, efficient, and user-friendly solution, promising enhanced protection for credit card transactions in the dynamic landscape of online commerce.

II. SYSTEM ANALYSIS

The existing system is handled manually. The system has a formatted online shop system for Sales in paper work. The indent is prepared when items are to be purchased and bill is generated for sale of items. The system follows large number of paper work for maintaining product details and user can be difficult to search the product in database. In some places the Barcodes are often intended for consumer use where using a barcode device, a consumer can take an image of a barcode on a product.

Limitations:
Customers have to wait for painfully long durations during the checkout process. The billing process at a shop is the most tedious part of shopping. If a bar code is damaged or dirty, they are not capable of reading any data. In terms of data storage, bar codes can hold less data, mostly numeric, and take up greater space as they are one dimensional.

Proposed System:
In the proposed system, we are using face detection using web application to provide secure transaction authenticity of credit card holder for online shopping. In this project the user can buy a product through this website, after buying the products the user can pay the amount using credit card transaction with face detection. So face detection verifies user face by capturing it using camera, after successful face detection method the user can pay the purchased amount.

Excepted Merits:
Reduction of paper work. Automation of existing manual information systems.
Reduction of manual processing. Keep track of daily information exchange at the server by the administrator. Increase in processing and transfer speeds of information over the network.

ALGORITHM

GRASSMANN ALGORITHM

1. The Grassmann algorithm is a mathematical technique that is often used in face recognition to analyze and compare facial features. Here are the basic steps involved in using the Grassmann algorithm for face recognition.
2. Feature Extraction: The first step is to extract facial features from the images of the faces to be recognized.
3. Face Representation: Next, the extracted facial features are represented as points in a high-dimensional space. This space is often referred to as a feature space or a face space.
4. Grassmann Manifold: The Grassmann manifold is a mathematical space that represents all possible subspaces of a fixed dimension in a high-dimensional space. The Grassmann algorithm uses this manifold to compare the subspaces that represent the facial features of different faces.
5. Subspace Projection: Each face is represented as a subspace in the feature space. The Grassmann algorithm then projects these subspaces onto the Grassmann manifold to create a set of points that can be compared.
6. Distance Computation: Finally, the distance between the subspaces is computed using a distance metric such as the Grassmann distance. The distance metric takes into account the geometry of the Grassmann manifold and provides a measure of how similar or dissimilar the subspaces.
7. Classification: The computed distances are then used to classify the faces into known or unknown individuals. This step typically involves setting a threshold value for the distance metric, above which a face is considered to be unknown.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 2, February 2024 |

| DOI:10.15680/IJMRSET.2024.0702011 |

SOFTWARE DESCRIPTION:

FRAMEWORK CREATION:

Login
In this module, the admin can login in the system using his/her username andpassword.

Add Employee/ Product
In this module, the admin can add the employee information like employee name, id, phone number, mail id, location etc. After the login process the employee can add the product details like product id, name, type, amount, quantity and so on.

View booking Details
In this module, the admin/employee can view the user booking details. The booking details contain booking id, product details, user details etc

View User Details
In this module, the admin can view the user information's like user name, email, gender, mobile number, address, and etc.

User Enrolment And Add Product purchase DetailsRegister
There is registration form available where new user can create their account by providing required information to the system. The registration form details are like username, email, gender, mobile number, address, and etc. These details are stored in the database. And then can getting to the username and password in the system.

Login
In this module, user can login in the system using his/her username and password.

Product Purchase
In this module, the user can view the product details like product name, type, amount, description etc. After viewing all products, the user can buy product using this module. The user buying details are sent to the employee/admin.

Make Payment:

In this module used to make payment. This module contains user's card details like name, card no, amount etc.

Face Recognize :

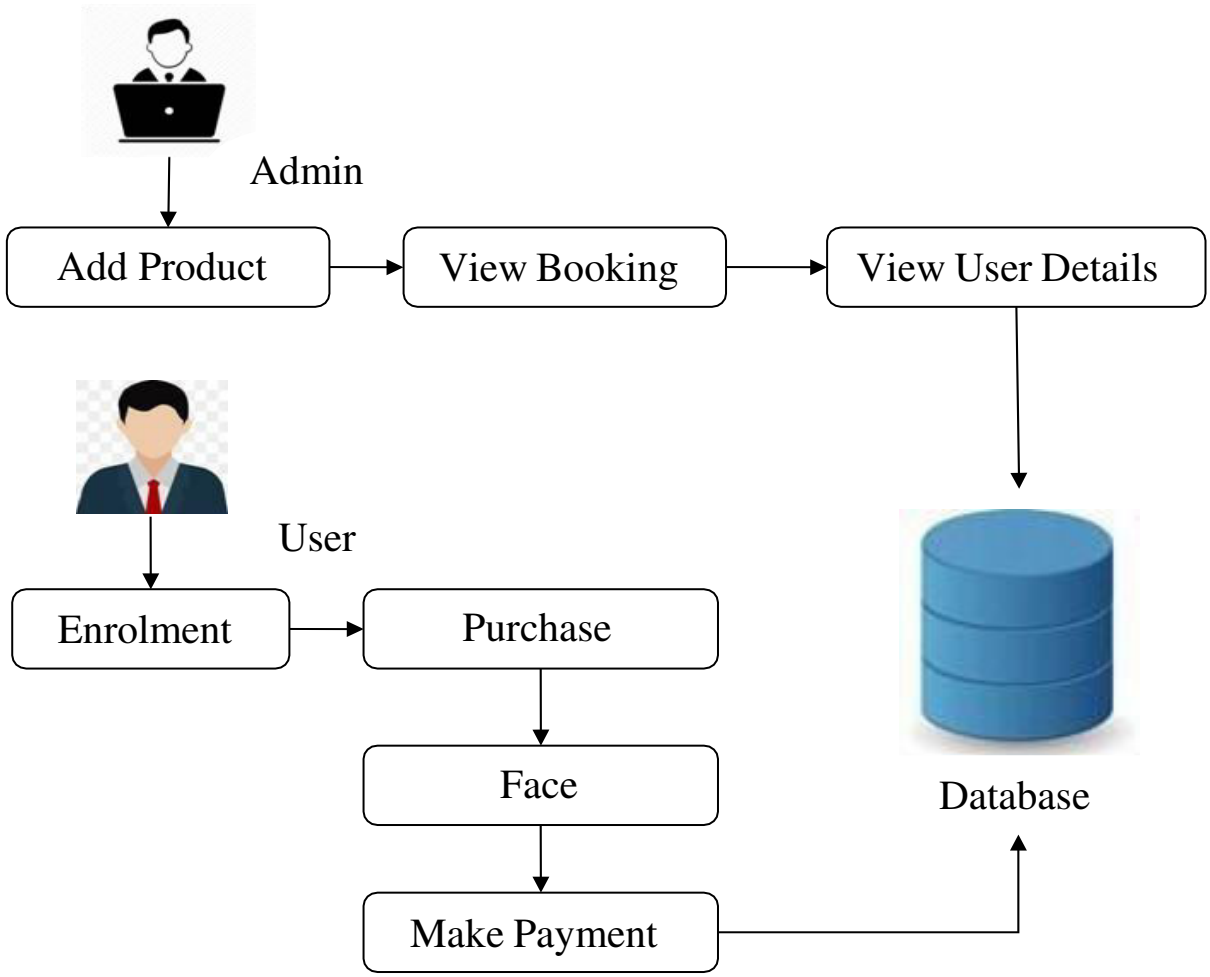
After successfully entered the card details the system camera can capture the user face image to match the particular card holder account database. If the user face image is matched with database, the user payment is transferred. Otherwise the user payment is not transferred.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 2, February 2024 |

| DOI:10.15680/IJMRSET.2024.0702011 |

System Architecture:



III. CONCLUSION

The implementation of the proposed system, integrating advanced fraud detection measures, streamlined online shopping processes, and innovative face detection technology, is anticipated to yield a multifaceted set of outcomes. Foremost, the system is expected to significantly mitigate the risks associated with online transaction fraud, providing a robust defense against unauthorized access and fraudulent activities. By leveraging user spending patterns, geographical location verification, and continuous monitoring for unusual patterns, the system aims to create a secure transaction environment, instilling confidence in both financial institutions and users. The introduction of face detection in credit card transactions is poised to revolutionize the online shopping experience. Users will benefit from a seamless and efficient payment process, reducing checkout durations and eliminating the challenges associated with traditional methods. The biometric authentication provided by face detection adds an additional layer of security, ensuring that only authorized credit card holders can complete transactions. Moreover, the integration of the Grassmann algorithm into face recognition enhances the accuracy and reliability of identity verification. The algorithm's ability to analyze and compare facial features contributes to precise classification, minimizing the likelihood of false positives or negatives. Overall, the expected outcome is a technologically advanced and user-centric system that not only safeguards financial transactions but also enhances the overall efficiency and security of online shopping, fostering a trusted and seamless digital commerce landscape.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 2, February 2024 |

| DOI:10.15680/IJMRSET.2024.0702011 |

REFERENCES

[1] Sahu, Aanchal, G. M. Harshvardhan, and Mahendra Kumar Gourisaria. "A dual approach for credit card fraud detection using neural network and data mining techniques." In 2020 IEEE 17th India council international conference (INDICON), pp. 1-7. IEEE, 2020.
[2] Panda, Agyan, Bharath Yadlapalli, and Zhi Zhou. "Credit card fraud detection through machine learning algorithm." Big Data and Computing Visions 1, no. 3 (2021): 140-145.
[3] Aziz, Amir, and Hamid Ghous. "Fraudulent Transactions Detection in Credit Card by using Data Mining Methods: A Review." INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) 79, no. 179 (2021).
[4] Shah, Ankit, and Akash Mehta. "Comparative Study of Machine Learning Based Classification Techniques for Credit Card Fraud Detection." In 2021 International Conference on Data Analytics for Business and Industry (ICDABI), pp. 53-59. IEEE, 2021.
[5] Muttipati, Appala Srinuvasu, Sangeeta Viswanadham, Radhika Senapathi, and KN Brahmaji Rao. "Recognizing credit card fraud using machine learning methods." Turkish Journal of Computer and Mathematics Education 12, no. 12 (2021): 3271-3278.

Impact Factor
7.521

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com