International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | June 2022 www.irjet.net p-ISSN: 2395-0072

OCR DETECTION AND BIOMETRIC AUTHENTICATED CREDIT CARD PAYMENT SYSTEM.

Adesh Shinde, Suraj Pilaware, Ashutosh Garud, Murtza Merchant.

Dept of Information Technology, JSCOE, Savitribai Phule Pune University, Pune, Maharashtra, India.

Abstract: The number of personnel using online transaction methods has made tremendous growth over the last few years so we need a safe place to complete the same. To authenticate and confirm online transactions, we recommend employing biometric authentication. As a result, consumers save time by reducing a multi-step method to a single step. To enable devices to detect visual signals using a webcam, simplify the operation of manually entering the details of the card intended for OCR. Device users are ordinary people who are frustrated by the extra time spent on the internet. The present authorization system uses an OTP that is difficult to recover. We have developed a Python backbone that would simulate the system billing process and the OTP system billing procedure. We utilised it to see if users enjoyed the new method of payment verification and to seek feedback on how to enhance the product. We describe a project that could make internet payments possible without any additional hurdles.

Credit card companies have no security features other than OTP (one-time password) and CVV. If this program does its job without any problem, credit card and debit card companies can use this program to reduce the fraud of online transaction.

Keywords: *Dataset, CNN(Convolutional Neural Network),Django ,Fido Authenticator, OCR Architecture.*

1. INTRODUCTION

When utilising e-commerce sites, we all face issues with OTP (One-time Password) generation, the most common of which are obsolete OTP, prior OTP generation, OTP theft, and more. A big number of customers prefer online transactions due to the growing number of credit card/debit card holders and the convenience of online transactions. Banks also play a vital role in ensuring that transactions are completed and that consumers can withdraw funds as needed. This also contributes to the term "Digital India."

Despite the fact that credit/debit card firms provide CVV security and banks provide OTP protection, there is still a high risk of fraud at high pricing. This could lead to a sense of unease when conducting online transactions.

As a result, we created a system to try to resolve the situation. Using a fingerprint authentication approach and OCR for credit/debit card text identification. Millions of people's lives are directly or indirectly impacted by the digital store industry in the E-commerce sector. With the current architecture, this particular area can be easily exploited. This has the potential to transform the lives of everyone linked to the network. E-commerce has exploded in popularity over the previous decade. As a result, it is critical to construct digital storefronts for businesses with additional protection so that they can earn safely in this online market, as traditional e-commerce is not as secure or as simple for small business owners to establish their online presence. To improve the overall efficiency of the E-commerce sector, features such as traceability, detectability, tracking, verification, and accountability should be included.

REQUIREMENT SPECIFICATION AND ANALYSIS -

To enhance the approach of the traditional payment system using Fingerprint Authentication and Credit/Debit Card OCR detection and cutting a multi-step process into a one-step process, therefore, saves consumer time. To enable devices to detect visual signals using a webcam, simplify the operation of manually entering the details of the card intended for OCR.

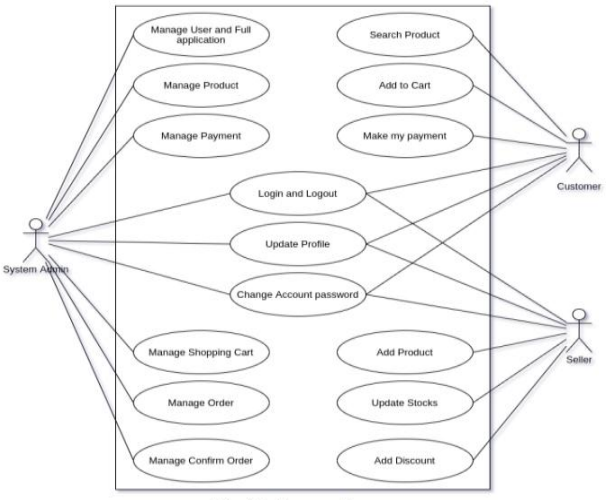


Fig. 4.1 : Use-case diagram

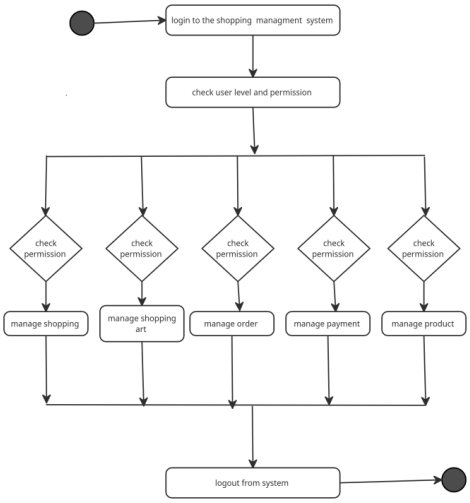


Fig. 4.2 : Activity diagram

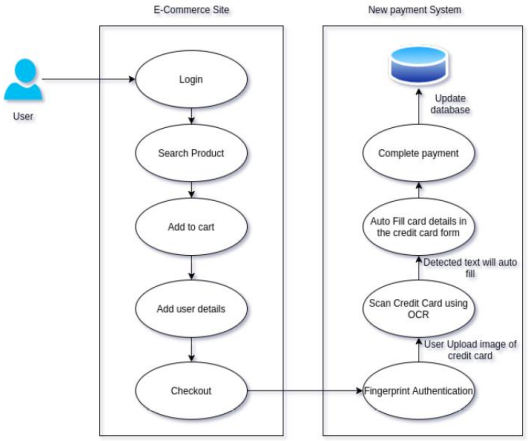


Fig. 5.1.1 : System Flowchart

The core objectives of this project are :

1. Create a Payment system where we authenticate users using fingerprint Scanner.

2. Simplify the function of manually entering the details of the card intended for OCR to enable devices to detect visual signals using a webcam.

3. Protect the data authenticity.

4. Speed up the transaction.

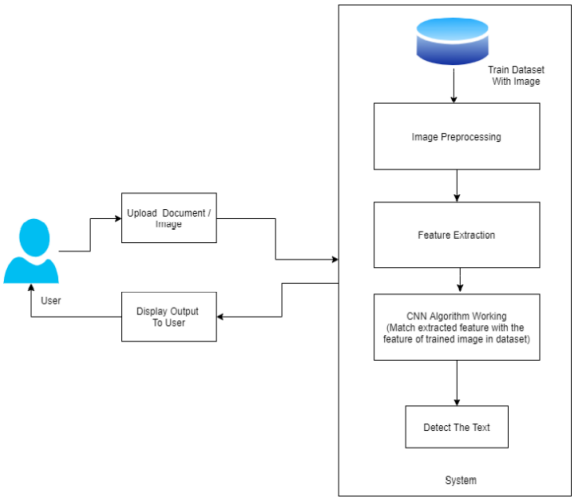
5. Design of payment system to avoid single point of failure.

6. Increasing Security for credit/debit card companies as they just have OTP and CVV as their security system.

PROPOSED METHODOLOGY -

Credit and debit cards are widely utilised in modern society. These days people also choose to use a credit/debit card to do a large number of online transactions. However, one of the most prevalent frauds is some terrible things. According to a recent poll, India is the most targeted country in the world, ranking third. In India, over 2lakh+ online fraud scams have been reported in the last two years. Traditional credit/debit card security is CVV and OTP (One Time Password) authentication However, this security is based on fingerprint .authentication. When a credit/debit card is placed in front of the camera, the appropriate information is immediately input in the form. In card verification, we use the google cloud vision API, then fingerprint authentication we have used navigator. credentials.

OCR ARCHITECTURE-



Pre-processing is the first thing an OCR model does with an image. Depending on the model, this can mean a variety of things, but the image is essentially changed to make it as easy to read as feasible. Rotating the text, straightening it, eliminating any background graphics, making the background as white as possible, and darkening the text if it isn't already dark are all examples of pre-processing.

After then, the OCR begins the process of recognising each character, which can be done in a variety of ways.

One approach is pattern recognition. This is accomplished by first detecting lines of black pixels separated by rows of white pixels.

Individual characters are then examined in the same way, with the black pixels in between columns of white pixels.

Each character is represented as a binary matrix, with white pixels representing 0s and black pixels representing ones. The distance between the matrix's centre and the farthest pixel is calculated using the distance formula. This is used as a radius to make a circle, and it divides the circle into subsections, each of which is compared to a database of characters to find the best match.

FINGERPRINT AUTHENTICATION

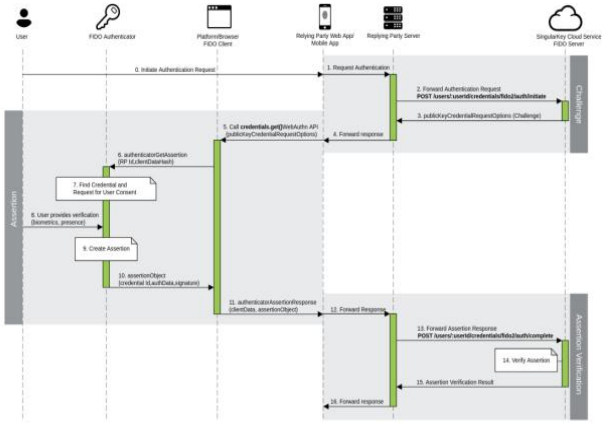
ARCHITECTURE -

While two-factor authentication was formerly the industry standard, the FIDO and World Wide Consortium (W3C) WebAuthN standards are paving the way for modern password-free browsing.

This open standard, developed with the help of IT heavyweights like Google and Microsoft, provides a more convenient and secure authentication experience than traditional 2FA authentication solutions.

Singular Key, as a dependable multi factor authentication service provider, allows you to give your clients the option of using current authenticators such as Windows Hello, Biometrics, or Security Keys for frictionless online connections, engagements, and transactions.

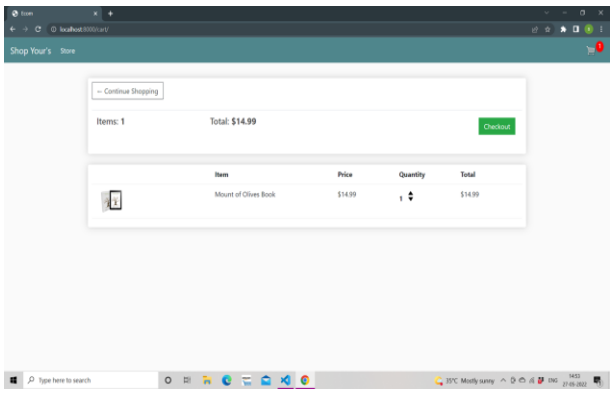
You may add strong authentication to improve security and overall user experience with a few code changes on your application's login page with Singular Key's FIDO certified Authentication Service. The WebAuthn sequence diagrams and steps shown below walk you through an end-to-end flow for registering a FIDO credential and authentication using a FIDO credential.



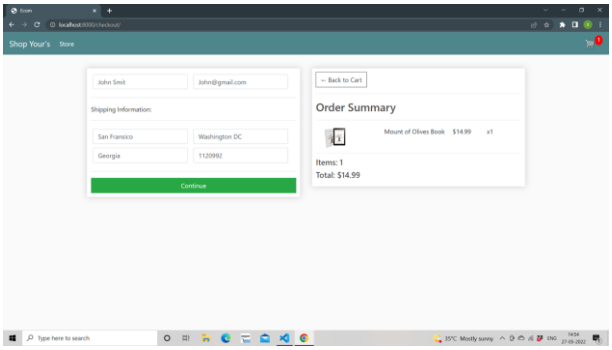
Details step:

1. User initiates Authentication Request
2. RP App forwards Request
3. WebAuthn Authentication Initiate Request
4. WebAuthn Authentication Initiate Response
5. RP Server response to RP App
6. Invoke Web Auth Credentials.Get() API
7. Assertion
8. WebAuthn Credentials.Get() API Response
9. RP App forwards Assertion Response
10. WebAuthn Authentication Complete Request
11. Assertion Verification
12. WebAuthn Authentication Complete Response
13. RP Server creates session and responds back to RP App .

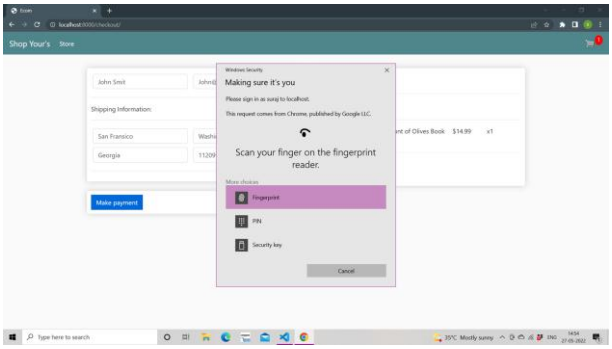
IMPLEMENTATION -



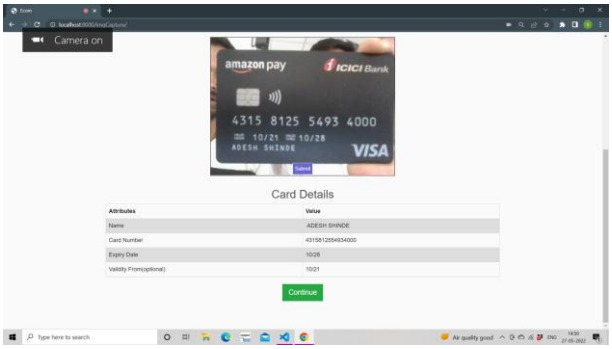
STEP:01



STEP : 02



STEP: 03



STEP:04

CONCLUSION -

We have developed a security model for credit card verification using webcam and fingerprint authentication to provide high security that helps reduce online transaction fraud. The proposed system is integrated with a one-way security module, fingerprint verification, that can only be accessed by an authorized user to protect users from online transactions. This initiative will aid in the promotion of internet transactions. This project can be used in future by Credit/Debit Card companies increasing their security in the system and also we can add more layers of security in the system using Face Recognition or any Biometric Security which in turn make the system more secure. We can also add more powerful models in our system and make our system more robust and fraud proof.

REFERENCES -

1. Amit Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015, 5080-5084 "Multimodal Biometric System in Secure e-Transaction in Smart Phone"

2. Namita Jain, Vikrant Mukkawar, Mahesh Jadhav, Prof. Shruti Sekra. "Survey on Online Transaction using Face Recognition"

3. Asma Shaikh, Aditi Mhadgut, Apurva Prasad, Bhagyashree Shinde, Rohan Pandita. "Two-way Credit Card Authentication with Face recognition using webcam"

4. Shuo Wang and Jing Liu , Department of Biomedical Engineering, School of Medicine, Tsinghua University, P. R.China " Biometrics on Mobile Phone " www.intechopen.com

5. Informatica Economică vol. 13, no. 1/2009 " Biometric Security for Cell Phones "

6. Nimalan Solayappan and Shahram Latifi, Department of Electrical engineering, University of Nevada at Las Vegas, USA, " A Survey of Unimodal Biometric Methods"

7.International Conference on Telecommunication Technology and Applications, Kounoudes et al., 2006, Voice Biometric Authentication for Enhancing Internet Service Security, pp. 1020-1025, with permission from IEEE.

8. G. Williams, "More than a pretty face", Biometrics and martCard Tokens. SANS Institute reading room, 2002, pp. 1-16.

9. A. K. Jain, K. Nandakumar, U. Uludag, and X. Lu, "Multimodal Biometrics", from Augmenting Face With Other Cues, in W.Zhao,and R. Chellappa, (eds) Face Processing: Advanced Modelling and Methods, Elsevier, New York, 2006. pp. 675-705. Recognition", in Proceeding

10. J.P. Campbell, D.A. Reynolds, and R.B. Dunn, "Fusing High And Low Level Features for peaker

11. J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez, "Authentication Gets Personal With Biometrics", in IEEE Signal Processing Magazine, Vol. 21, 2004, pp. 50–62.

12. A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction To Biometric Recognition", in IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, 2004, pp. 4–20

13. Mohamed Abdolahi, majid mohamadi, mehdi jafary 2013. Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic. IJSCE ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

14. Fan Yang and Baofeng Ma. 2007. A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palmprint. In Image and Graphics, 2007. ICIG 2007. Fourth International Conference on, pages 689–693. IEEE

APPENDICES -

Base Papers

T. Chumwatana and W. Rattana-umnuaychai, "Using OCR Framework and Information Extraction for Thai Documents Digitization," 2021 9th International Electrical Engineering Congress.

Amit Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015, 5080-5084 "Multimodal Biometric System in Secure e-Transaction in Smart Phone"

I. Anuradha, C. Liyanage, H. Wijayawardhana and R. Weerasinghe, "Deep Learning Based Sinhala Optical Character Recognition (OCR)," 2020 20th International Conference on Advances in ICT for Emerging Regions (ICTer), 2020

Asma Shaikh, Aditi Mhadgut, Apurva Prasad, Bhagyashree Shinde, Rohan Pandita. "Two-way Credit Card Authentication with Face recognition using webcam"