ISSN No:-2456-2165

Machine Learning based 5 Factor Authentication

Aditya Patel
Student, Department of Computer Science & Engineering
Institute of Technology & Management Universe
Vadodara, Gujarat India

Mihir Parikh
Student, Department of Computer Science & Engineering
Institute of Technology & Management Universe
Vadodara, Gujarat India

Archana Magare
Assistant Professor, Department of Computer Science & Engineering
Institute of Technology & Management Universe
Vadodara, Gujarat India

Abstract:- India is growing through a digitalization era where nowadays most of the financial transactions are done by Internet Banking & Mobile Banking, so in this paper the proposed system has redesigned ease of doing transaction. the conventional way of doing any transaction is to open a Merchant order page, select appropriate item you want to buy & enter an OTP at Bank gateway page, so in this paper the proposed system has redesigned a concept to overcome the problem of an OTP is compromised by the user, so the proposed system has redesigned that functionalities. In this proposed system implementation of five factors are used. In this proposed system different factors such as face recognition, location history, card details, Transaction history, OTP are used. So by implementing this five factors the proposed system is making the transaction more secure.

Keywords:- *5 Factor Authentication, Card Details, Database, Face recognition, Location history, Machine Learning, OTP, Regression Algorithm, Servlet, Transaction history.*

I. INTRODUCTION

Overview

What is a fraud elimination system? A fraud elimination system is a system in which unauthorized transaction would not happen, it is been planned in this project to redesign the concept of transaction verification system. In this system not only 1 or 2 factors, are used but instead of that total five factors are used to prevent the frauds which are happening in current system. In this system facial recognition is used, OTP[1] based transaction and also Location & previous transaction based ML model. By using this it is been proposed to eliminate the fraud which are happening in the system due to loop holes. Our system is a fraud-proof system. The possibility of happening fraud is less than 1% in our system. Due to digitalization this concept is really in need for implementation. In this system ML[9] techniques have been used to eliminate frauds, first of all user will purchase all the goods which they needed to buy then after the next step would be the payment gateway system, our system will automatically recognize its previous transaction history, if the current transaction amount value will not fit in the previous transaction history curve then our system will jump to facial recognition model, after recognizing the face the system will redirect to OTP gateway page. This many types of factors and techniques have been implemented in our system. If any of the factor verification is failed then the entire transaction will be cancelled.

Advantages of Multifactor Authentication

E-Commerce websites and applications are the most vulnerable for online transaction fraud. To commit an online transaction no physical card is required, all it requires is just the credentials.

[a] One of the advantage of five factor authentication system will be the reduction in fraud which are happening in the conventional system. Our system will eliminate major types of fraud which are happening because of the loop hole present in the system. [b] Another advantage is ML model, ML model will generate prediction based on the user past transaction history. There is no manual work in our system. & our system is fully automated. [c] Due to advanced facial recognition system, our system will identify the user face and then it will apply the algorithm which have been designed in our system.

II. RELATED WORK

Homayoon beigi[1], In this system author are using controlling multifactor authentication with multimodal biometrics. In this a users can use different types of devices like PDA, cellular mobile or handheld communications. This is only an example. The process of the system can verify any type of transaction which requires any financial transaction, access control and any physical access scenario such as doubling for a passport or an access key to a restricted area (office, vault, etc.). It is also used for remote transactions such as those conducted on internet. Here various Biometric Systems are also used.

Barnan Das et al[2] have used various technologies to verify the user credentials. Here various environmental factors and various multi factor authentication techniques are used. Here by verifying the environmental sensor data system can allow the verified users. To verify computing device may detect accuracy scores based on the environment during authentication for each biometric authentication factor used to authenticate the user. And also, the computing device may determine a login pattern based on collected sensor data during historical authentication attempts by the user over a period of time.

Tamer E. Abuelsaad et al[3], here the system can verify the user credentials through context and pre-registration of objects. Here system uses context of registered device information to verify the users login credentials. Here system will verify the details like phone model number, various hardware specification of user’s device to identify the user. Here the system is designed to run methods which detect and make use of a user's context that includes: a current environment or context, and uses this capability to enable variable strength authentication when attempting to log in or enter another application or resource.

Richard John Hughes et al[4] have used a QC trusted authority to implement Multifactor authorization. Here user device will send the data to trusted authority and trusted authority will verify the data on certain parameters. Then it will pass the info back to the device. Quantum computing plays an important role in this type of authorization. The user device and trusted authority use the device factor information and user factor information (more specifically, information such as a user password that is the basis of the user factor information) in multi-factor authentication that uses QC.

Byoung-Wook Kwon et al[5], Many security systems simply rely on solutions based on Artificial Intelligence, which are weak in nature. These security solutions can be easily manipulated by malicious users who can gain unlawful access. Here Authentication is verify based on CCTV footage. CCTV video are stored on DVR. DVR will check the user credentials based on the received footage. Here CCTV plays an important role in authentication system.

Sabout Nagaraju et al[6] have used multi factors like User ID and password, ID and password shows what user knows, fingerprint and biometric represents who the user is, and random strings are used to verify the identity to servers. Server verifies user identity and user verifies server’s identity. They have proposed multi stage protection using random strings.

Song et al[7] have submitted the idea of OTP based authentication method and system, here transceiver is there to receive the request from the client side & then a decoder is there to decode the information. A server side OTP is there to generate server OTP & client side OTP is there to validate the client side. so that`s how the whole system works.

Chen et al[8], Here Java XMPP (Extensible Messaging and Presence Protocol) servlet container is used instead of Java Servlet model, here container is provided to server so that the communication application can be programmed with objects defined by an XMPP[15] servlet API. Java XMPP servlet container includes a point for managing network connections. XAMPP sessions are also used in this proposed system.

Balogh et al[9], Here computer system and methods are provided for using a ML system to analyze authentication system, first authentication includes the first image that corresponds to the first ID received and First validation information that corresponds to a first validation fault is received from a validation system. Storage system of ML stores the first information which are validated, second authentication information corresponds to second image that corresponds to second image received, ML determines first validation values related to second image with first validation fault, in accordance with fault review criteria, second image is transmitted.

Stapleton et al[10], Here various techniques are described to limit the openness of ML models for example various techniques are defined to detect the attack or exploitation. Additionally, various embodiments described herein promote the protection of sensitive and/or valuable data, moreover techniques are various techniques re there for version tracking, usage tracking and for other ML models.

Baghdasaryan et al[11], In this system authentication is performed using data analytics and machine learning. Here system will analyze set of parameters based on user`s activity. After receiving request to authenticate user. System will measure the risk between current transactions & previous transactions. Here one or more authentication techniques are required to validate the user. Here parameters are updated after each of the transactions.

III. SYSTEM ANALYSIS

A. *Problem Definition*

In the rise of frauds in the transaction, a concept of five factor authorization have been introduced. Here total five different factors have been implemented to verify the user identity. Here Our ML based system will detect any suspicious transaction & will take appropriate steps to avoid it. The steps are five factors verification. Location, OTP[7], Debit card/Credit Card, Face recognition & time based authentication. The combination of five factors will introduce fraud-free method in our system. Our system can have an accuracy up to 99%.Major types of frauds can be prevented by implementing this type of system. In the earlier system the problem was various loopholes which hackers were exploiting to gain the access in the system. By implementing our system major types of frauds can be avoid.

B. *Proposed System Feature*

There are total five factors which have been implemented in our system. 1. Location Based Verification .2 Time Based Authentication 3. Face Recognition .4. OTP[7] Based Verification five. Card Details based verification. Our database will store user information like past transaction time, past transaction location history, past transaction amount value. Our system will predict the next transaction range in which the user would buy by that amount. If the system will detect the current transaction value within the range of system predicted ML based transaction value then it will jump to OTP based authentication. If the system will detect any suspicious activity like the amount is not in the proposed range then it will jump to facial recognition then after it will jump to OTP based authentication. After the completion of all the system proposed steps, user can finish the transaction.

IV. SYSTEM DESIGN AND IMPLEMENTATION

A. Proposed of five Factor Authentication System

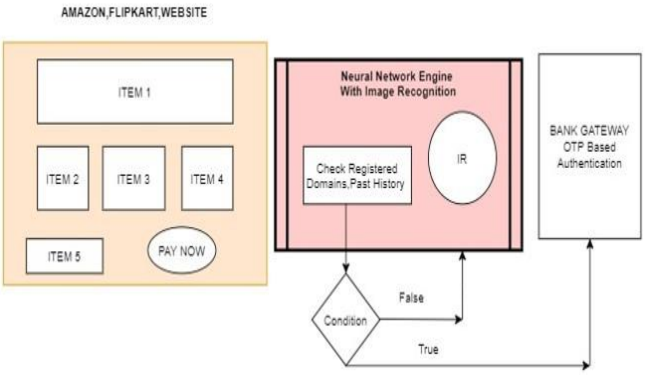

AMAZON,FLIPKART,WEBSITE
ITEM 1
ITEM 2
ITEM 3
ITEM 4
ITEM 5
PAY NOW
Neural Network Engine With Image Recognition
Check Registered Domains,Past History
IR
BANK GATEWAY OTP Based Authentication
Condition
False
True

Figure 1: Flow diagram of five Factor Authentication

A system have been proposed which includes the combination of five factors. Our system will work the same as it has been designed it. First of all customer have to login through their credentials on our portal. After successful verification of credentials like Email ID & Password, logging through our portal user will be able to browse items, buy items and update items. User can also view its transaction history from our portal. After Selecting or purchasing the items from our portal which user needs to buy, the system will direct it to the next step which is payment gateway page. Our System will perform algorithms to predict the transaction value range based on Users previous transaction history value, our system will also perform some steps to verify the city from which user is purchasing items. If the system detects any changes or it encounters any suspicious activity in the transaction then it will redirect User to facial recognition mode. After successful recognition of facial verification of user will be redirected to payment gateway page. Here Bank will send an OTP to its registered number. After completion of OTP gateway page the transaction finishes. If the system will not detect any suspicious activity like user`s transaction value is in the proposed range detected by ML[17] model then our system will directly ask user to enter the OTP which will be provided by the Bank. It will not jump to facial recognition mode unless and until there arises a need. so that`s how our proposed system works.

B. Proposed of five factor Authenticaton Functions

Five factor authentication function includes verification factors which our system will ask user in order to verify user identity. Five factor includes time, Facial recognition, Card details, Password & Location. Time factors measures the time of proposed transaction and its previous transaction time history. Our system will measure the time activity at which the most transactions occur and our system will generate one ML[17] Model based on the time parameter. Facial recognition includes the Facial verification. Card details includes the users Debit or credit card information like Card number, Expiry date, CVV, etc. Password factor includes the password which user needs to enter at login page. Location factor includes the list of locations at which user has performed the transactions. Our system will update each of the factor information after completion of each transaction.

Figure 2: Functions of 5 Factor Authentication [12]

If System is failed to recognize or verify the user identity at any one of the step then the transaction ends. & user is not able to continue buying the products. So that`s how each factor works and that`s how verification of each factor is done.

C. System Design

First of all Our website`s Home page is Login page. There are two console windows, one is for clients or for users and another one is for Producers. On homepage user needs to enter information like email id & password. After entering the credentials the system will display the list of products which are available for buying. User can select any product, or any quantity which he needs to buy. After selection of products system will display the overall cart items which user has selected. After reviewing the products system will ask for billing information. After successful completion of billing details it is redirected to payment gateway OTP information. Then after the completion of OTP verification user can finally purchase the product. So that's how our overall system design will look like.

D. Implementation Setup

Various technologies have been used in order to publish our idea. We have used HTML[14], CSS, JavaScript, Java EE, Servlets, DBMS technologies[13].For the registration purpose a database have been maintained in which the information of User email ID & password stored by database.

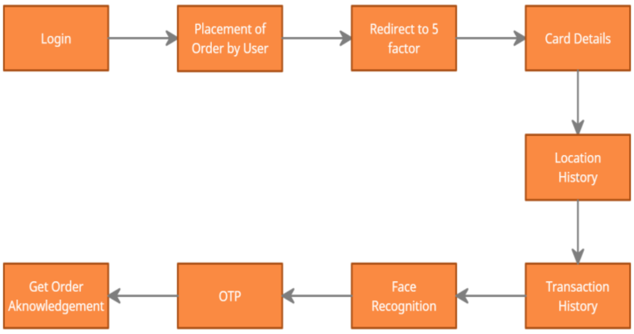
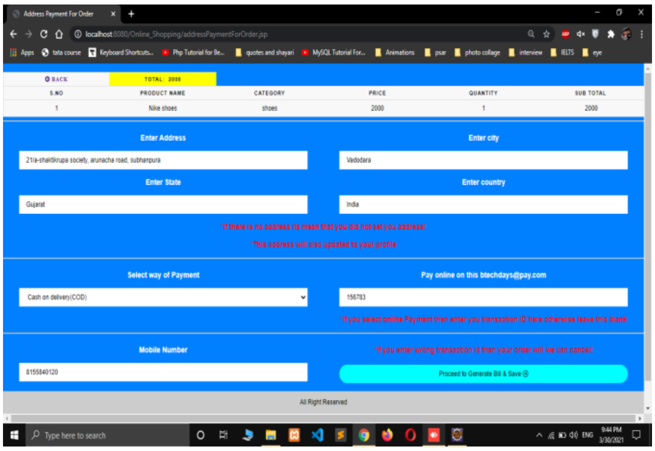


Figure 3: Flow Diagram of the System

A database have maintained for displaying of the list of products. Here all the items are stored in a database Cookie & session have used throughout the login process so that user cannot log out from the website unexpectedly. User can stay on website as long as the process continues. Tomcat[16] as a server have been used us. For ML model a database have been designed for storing information like location & past transaction history. For Bank OTP feature Bank gateway page have been linked. And we have connected all the webpages using session concept of technology. So that's how implementation is done for our project.

V. RESULT


Address Payment For Order
localhost:8080/Online_Shopping/addressPaymentForOrder.jsp
BACK

TOTAL: 2000

S.NO	PRODUCT NAME	CATEGORY	PRICE	QUANTITY	SUB TOTAL
1	Nike shoes	shoes	2000	1	2000

Enter Address: 21/a-shaktikrupa society, arunacha road, subhanpura

Enter city: Vadodara

Enter State: Gujarat

Enter country: India

*If there is no address its mean that you did not set you address!

*This address will also updated to your profile

Select way of Payment: Cash on delivery(COD)

Pay online on this btechdays@pay.com: 156783

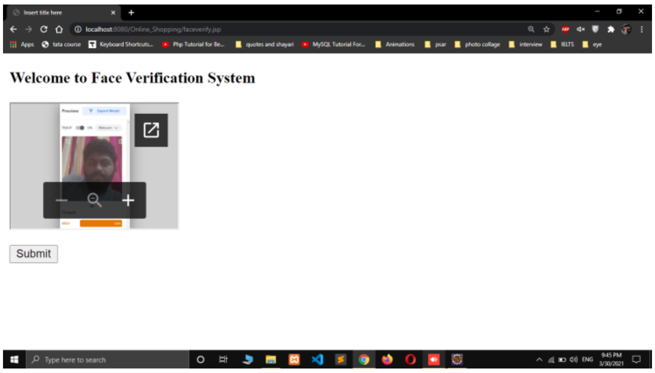
*If you select online Payment then enter you transaction ID here otherwise leave this blank

Mobile Number: 8155840120

*If you enter wrong transaction id then your order will we can cancel!

Figure 4: Bill generation page

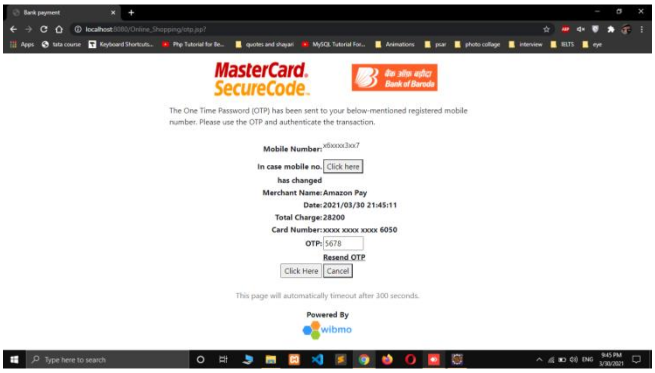
So the system have been proposed where one can buy products, verify its identity and prevent some frauds, so ultimately a system have been developed where there is a very less chance of frauds happening.



Welcome to Face Verification System

Figure 5: Face recognition

The final product is where producer can list items, consumer can purchase the items from separate UI, here consumer can buy items and it can avail the quantity which they want, make payments with our ML Based System which can work efficiently when having enough consumer data, system can make predictions using previous history, with providing enough security to user's financial purchases.



The One Time Password (OTP) has been sent to your below-mentioned registered mobile number. Please use the OTP and authenticate the transaction.

Mobile Number: x6xxxx3xx7

In case mobile no. has changed: Click here

Merchant Name: Amazon Pay

Date: 2021/03/30 21:45:11

Total Charge: 28200

Card Number: xxxx xxxx xxxx 6050

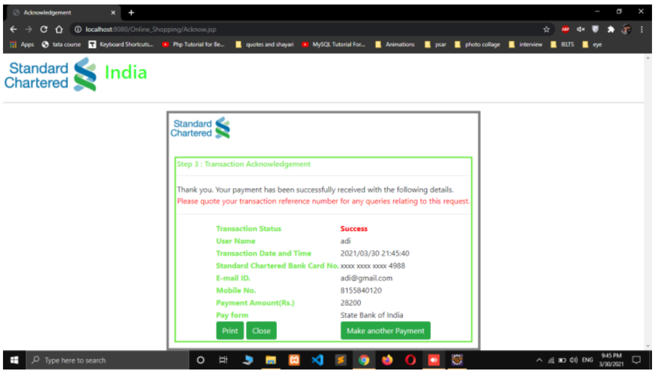
OTP: 5678

This page will automatically timeout after 300 seconds.

Powered By wibmo

Figure 6: OTP

Here first of all consumer can select the items which they wants, after selecting the items he have to put various details like Address, Payment Methods, Card details, after checking out the cart items Our system will generate predictions whether the user has to verify the face recognition or not. If not then user will directly jump to the OTP based payment gateway system, from there user can avail the final product after making the payment. So that`s how the whole product works.



Step 3 : Transaction Acknowledgement

Thank you. Your payment has been successfully received with the following details.
Please quote your transaction reference number for any queries relating to this request.

Transaction Status	Success
User Name	adi
Transaction Date and Time	2021/03/30 21:45:40
Standard Chartered Bank Card No.	xxxx xxxx xxxx 4988
E-mail ID.	adi@gmail.com
Mobile No.	8155840120
Payment Amount(Rs.)	28200
Pay form	State Bank of India

Figure 7: Bill gateway

VI. CONCLUSION

So conclusion is that a product have been developed selling website with 5 layers of authorization. Here the chances of hackers using user's credentials is less. Here full layer of security have been provided where happening of several types frauds is very less. Here producer can list items, consumer can directly purchase the items from separate UI. Here proposed system encountered user's previous transactions history, location of last previous transaction history so that system can avoid major types of frauds. Only genuine users can avail our services and here facial recognition have been provided for better security. Here factors cannot be bypassed which are required for completing the transaction. So in conclusion we can say that an efficient ML Based Fraud Elimination System have been developed which will eliminate the frauds which are happening in the current system through loopholes.

REFERENCES

[1]. Homayoon Beigi, “Access control through multifactor authentication with multimodal biometrics” , US 10 , 042 , 993 B2.

[2]. Barnan Das, Abhilasha Bhargav-Spantzel, Narayan Biswal, Micah J. Sheller, Ned M. Smith, Hormuzd M. Khosravi, “Technologies for login pattern based multi-factor authentication” , US 10 , 114 , 935 B2.

[3]. Tamer E. Abuelsaad, Vishal C. Aslot, Adekunle Bello, Gregory J. Boss , “Adjusting multi-factor authentication using context and pre-registration of objects” , US 10 , 057 , 289 B2.

[4]. Richard John Hughes, Charles Glen Peterson, James T. Thrasher, Jane E. Nordholt, Jon T. Yard, Raymond Thorson Newell, Rolando D. Somma , “Multi-factor authentication using quantum communication” , US 9 , 887 , 976 B2.

[5]. Byoung-Wook Kwon, Pradip Kumar Sharma, Jong-Hyuk Park , “CCTV-Based Multi-Factor Authentication System” , ISSN: 2092-805X.

[6]. Sabout Nagaraju, Latha Parthiban , “Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway” , DOI 10.1186/s13677-015-0046-4.

[7]. Song, Seong Dae, Hwang, Han Eung, Kim, Seung Kuk, “OTP-based authentication system and method”, United States Patent 9503453.

[8]. Chen, Wei, Zhu, Xiaopu, Liu, Zhiyu, Zhang, Pubing, “Servlet API and method for XMPP protocol”, United States Patent 9215079.

[9]. Balogh, Attila, Hochrieser, Reinhard, Rogojanu, Radu, “Machine Learning for Document Authentication”, United States Patent Application 20190372968.

[10]. Stapleton, Shawn Arie Peter, Tahmasebi Maraghoosh, Amir Mohammad, “Machine learning model validation and authentication”, United States Patent Application 20200234121.

[11]. Baghdasaryan, Davit, “System and method for performing authentication using data analytics”, United States Patent 9875347.

[12]. Lvy wigmore, “Authentication Factor”, Tech target search security, https://searchsecurity.techtarget.com/definition/authentication-factor

[13]. https://www.eclipse.org/downloads/

[14]. https://www.sublimetext.com/

[15]. https://www.apachefriends.org/index.html

[16]. http://tomcat.apache.org/

[17]. https://sennovate.com/how-artificial-intelligence-and-machine-learning-helps-in-mfa/

[18]. https://en.wikipedia.org/wiki/Multi-factor_authentication

[19]. https://en.wikipedia.org/wiki/Machine_learning

BIOGRAPHIES

ADITYA PATEL
Pursuing B.E. in Computer Science & Engineering at Institute of Technology & Management Universe, Vadodara, Gujarat, India.

MIHIR PARIKH
Pursuing B.E. in Computer Science & Engineering at Institute of Technology & Management Universe, Vadodara, Gujarat, India.

ARCHANA MAGARE
Asst. Professor, Computer Science & Engineering at Institute of Technology & Management Universe, Vadodara, Gujarat, India.