IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

CREDIT SYSTEM USING FACIAL RECOGNITION

G. Srujana[1], G.Balachennaiah[2], D. Pavan Kumar[3], A.Venkatesh Babu[4], C.Anish[5]

[1]Assistant Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

[2]B.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

[3]B.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

[4]B.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

[5]B.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

Abstract: The goal of data analytics is to delineate hidden patterns and use them to support informed decisions in a variety of situations. Credit fraud is escalating significantly with the advancement of modernized technology and became an easy target for frauds. Credit fraud has highly imbalanced publicly available datasets. In this paper, we apply supervised machine learning algorithms to detect credit card fraudulent transactions using a real-world dataset. Furthermore, we employ these algorithms to implement a super classifier using ensemble learning methods. The software identifies faces which are already recognized and automatically adds the credit points to the customer's account. If the customer is not found, then the system requests the customer picture and contact details for customer to be added to the database. The points can be redeemed as the company pleases. Additionally, we compare and discuss the performance of various supervised machine learning algorithms that exist in literature against the super classifier that we implemented in this paper. Finally, we design and assess a prototype of a fraud detection system able to meet real-world working conditions that is able to integrate investigators feedback to generate accurate alerts.

Keywords: Credit Card, Fraud detection, supervised machine learning, face recognisation Classification, Imbalanced dataset, Sampling.

I.INTRODUCTION

Today, all around the world data is available very easily; from small to big organizations are storing information that has high volume, variety, speed and worth. This information comes from tons of sources like social media followers, likes and comments, user's purchase behaviors .All this information used for analysis and visualization of the hidden data Pattern. Early analysis of big data was centered primarily on data volume, for example, general public database, biometrics, financial analysis. To commit credit, fraud sterstry to steal sensitive information such as credit card number, bank account and social security number. Fraudsters try to make every fraudulent transaction legitimate which makes fraud detection a challenging problem. Increased credit card transactions show that approximately 70% of the people in the US can fall into the trap of these fraudsters. Credit card dataset is highly imbalanced dataset because it carries more legitimate transactions as compared to the fraudulent one. That means prediction will get very high accuracy score without detecting a fraud transaction. To handle this kind of problem one better way is to class distribution, i.e., sampling minority classes. In sampling minority, class training example can be increased in proportion to the majority class to raise the chance of correct prediction by the algorithm .In this paper, we use machine learning models and compare their Accuracy, TPR, FPR, Cohhen Kappa, Recall, Precision, Specificity and F1-Score.All machines learning algorithm is evaluated using a real world credit card transaction to identity fraud or non fraud transaction. The main motive of this paper to apply supervised learning method on the real-world dataset.

II.RELATED WORK

[1] The paper proposes a version for credit score card authentication the use of face reputation and face detection. In this model, Local Binary Pattern (LBP) algorithm has been used with Open CV framework for accurately recognizing the consumer's face. In conventional technique, user faces numerous vulnerabilities related to safety just like the credit score card consumer gave the details to surprising individual or the cardboard is misplaced. . This model based totally on way authentication affords high safety. In the first step, OTP is proven followed by using Face recognition. If each the conditions are glad, then the transaction will be allowed else transaction will be terminated. Local server is used for storing the pictures.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

[2] Nowadays, on line bills are concerned about safety. This is especially because of hacking of OTPs or PIN codes by way of the hackers. This paper proposes a technique for credit score card gadget utilized in transaction machine which will combine with the face detection. The hassle faced by credit score card users is lot of private ness troubles. This may additionally typically arise while customers give their credit card numbers to surprising people or while playing cards are misplaced.

[3] Credit playing cards are broadly getting used all around the world. There is an assumption, that if one has a credit card and passes verification, the access is granted. Such an approach entails few threats: the usage of credit card being in possession of unauthorized people (stolen or simply borrowed), threat of cloning card. One of the answers is verification of the biometric linkage among the signed facial photo of the credit card holder embedded in credit card and the consumer's facial photo captured by using a webcam throughout utilization of the cardboard.

[4] The paper proposes a version for credit card authentication the use of face recognition and face detection. In this version, Local Binary Pattern (LBP) algorithm has been used with Open CV framework for correctly recognizing the user's face. In traditional approach, person faces a lot of vulnerabilities associated with security just like the credit card person gave the information to unusual character or the cardboard is misplaced.

III. PROBLEM DEFINITION

Credit stands as major problem for word wide financial institutions. Annual lost due to it scales to billions of dollars. We can observe this from many financial reports. Such as (Bhattacharyya et al., 2011) 10th annual online fraud report by Cyber Source shows that estimated loss due to online fraud is $4 billion for 2008 which is 11%increase than $3.6 billion loss in 2007and in 2006, fraud in United Kingdom alone was estimated to be £535 million in 2007 and now costing around 13.9 billion a year (Mahdi etal., 2010). From 2006 to 2008, UK alone has lost £427.0 million to £609.90 million due to credit and debit card fraud (Woolsey &Schulz, 2011).

Although, there is some decrease in such losses after implementation of detection and prevention systems by government and bank, card-not-present fraud losses are increasing at higher rate due to online transactions. Worst thing is it is still increasing un-protective and un-detective way. Over the year, government and banks have implemented some steps to subdue these frauds but along with the evolution of fraud detection and control methods, perpetrators are also evolving their methods and practices to avoid detection. Thus an effective and innovative methods need to be develop which will evolve accordingly to the need. In this proposed project we designed a protocol or a model to detect the fraud activity in credit card transactions. This system is capable of providing most of the essential features required to detect fraudulent and legitimate.

In the Existing system, Logistic Regression is a supervised classification method that returns the probability of binary dependent variable that is predicted from the independent variable of dataset that is logistic regression predict the probability of an outcome which has two values either zero or one, yes or no and false or true. Logistic regression has similarities to linear regression but as in linear regression a straight line is obtained, logistic regression shows a curve. The use of one or several predictors or independent variable is on what prediction is based; logistic regression produces logistic curves which plots the values between zero and one. Regression is a regression model where the dependent variable is categorical and analyzes the relationship between multiple independent variables. There are many types of logistic regression model such as binary logistic model, multiple logistic model, and binomial logistic models. Binary Logistic Regression model is used to estimate the probability of a binary response based on one or more predictors. And the problems in Existing System

- It requires more preprocessing because it does not works on missing values.
- It produces less accuracy than random forest.
- Logistic Regression will perform with a large number of training data, but speed during testing and application will suffer.

IV. PROPOSEDSYSTEM

In proposed system, we are applying Randon Forest Algorithm for classification of the credit card dataset. Random Forest is an algorithm for classification and regression. Summarily, it is a collection of decision tree classifiers. Random Forest has advantage over decision tree as it corrects the habit of over fitting to their training set. A subset of the training set is sampled randomly so that to train each individual tree and then a decision tree is built; each node then splits on a feature selected from a random subset of the full feature set. Even for large data sets with many features and data instances training is extremely fast in random forest and because acute is trained independently of the others. The Random Forest algorithm has been found to provide a good estimate of the generalization error and to be resistant to over fitting.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

Advantages of Proposed System

(i) The results obtained by the Random Forest Algorithm are best compared to any other Algorithms.
(ii) The Random Forest algorithm also works well when data has missing values.
(iii) The Accuracy obtained was almost equal to cent percent which proves using of Random Forest algorithm gives best results.
(iv) The detection of the fraud use of the card is found much faster that the existing system.

V. SYSTEM ARCHITECTURE

The current application is being developed by taking the 3-tier architecture as a prototype. The 3-tier architecture is the most common approach used for web applications today. In the typical example of this model, the web browser acts as the client, IIS handles the business logic, and a separate tier MS-SQL Server handles database functions.
Although the 3-tier approach increases scalability and introduces a separation of business logic from the display and database layers, it does not truly separate the application into specialized, functional layers. For prototype or simple web applications, the 3-tier architecture may be sufficient. However, with complex demands placed on web applications, a 3-tiered approach falls short in several key areas, including flexibility and scalability. These shortcomings occur mainly because the business logic tier is still too broad- it has too many functions grouped into one tier that could be separated out into a finer grained model.

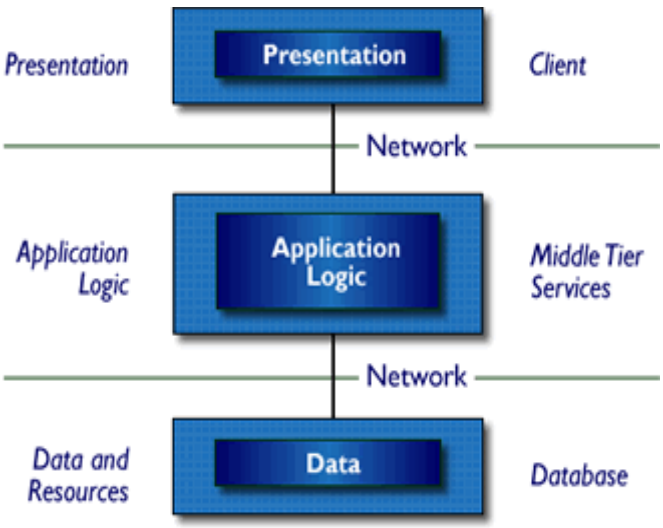

Fig: Proposed System Architecture

IMPLEMENTATION

Implementation is the process of converting a new or revised system design in to operation alone. There are three types of Implementation:
(a) Implementation of a computer system or place a manual system. The problems encounter dearer converting files, training users, and verifying print outs for integrity.
(b) Implementation of a new computer system to replace an existing one. This is usually a difficult conversion. If not properly planned there can be many problems.
(c)Implementation of a modified application to replace an existing one using the same computer. This type of conversion is relatively easy to handle, provided there are no major changes in the files.
(d) Implementation in Generic tool project is done in all modules. In the first module User level identification is done. In this module every user is identified whether they are genuine one or not to access the database and also generates the session for the user. Illegal use of any form is strictly avoided.
In the Table creation module, the tables are created with user specified fields and user can create many tables at a time. They may specify conditions, constraints and calculations in creation of tables. The Generic code maintains the user requirements throughout the project. In Updating module user can update or delete or Insert the new record into the database. This is very important module in Generic code project. User has to specify the filed value in the form then the Generic tool automatically gives whole filed values for that particular record. In Reporting module user can get the reports from the database in 2Dimentional or3Dimensional view. User has to select the table and specify the condition

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

then the report will be generated for the user.

Sample code:

```
# import the necessary packages
from tensorflow.keras.applications.mobilenet_v2 import preprocess_input
from tensorflow.keras.preprocessing.image import img_to_array
from tensorflow.keras.models import load_model
from imutils.video import VideoStream
import numpy as np
import imutils
import time
import cv2
import os

def spammer_detect(frame, faceNet, creditNet):
	# grab the dimensions of the frame and then construct a blob
	# from it
	(h, w) = frame.shape[:2]
	blob = cv2.dnn.blobFromImage(frame, 1.0, (224, 224),
		(104.0, 177.0, 123.0))

	# pass the blob through the network and obtain the face detections
	faceNet.setInput(blob)
	detections = faceNet.forward()
	print(detections.shape)

	# initialize our list of faces, their corresponding locations,
	# and the list of predictions from our face credit network
	faces = []
	locs = []
	preds = []

	# loop over the detections
	for i in range(0, detections.shape[2]):
		# extract the confidence (i.e., probability) associated with
		# the detection
		confidence = detections[0, 0, i, 2]

		# filter out weak detections by ensuring the confidence is
		# greater than the minimum confidence
		if confidence > 0.5:
			# compute the (x, y)-coordinates of the bounding box for
			# the object
			box = detections[0, 0, i, 3:7] * np.array([w, h, w, h])
			(startX, startY, endX, endY) = box.astype("int")

			# ensure the bounding boxes fall within the dimensions of
			# the frame
			(startX, startY) = (max(0, startX), max(0, startY))
			(endX, endY) = (min(w - 1, endX), min(h - 1, endY))

			# extract the face ROI, convert it from BGR to RGB channel
			# ordering, resize it to 224x224, and preprocess it
			face = frame[startY:endY, startX:endX]
			face = cv2.cvtColor(face, cv2.COLOR_BGR2RGB)
			face = cv2.resize(face, (224, 224))
			face = img_to_array(face)
			face = preprocess_input(face)
```

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

```
                # add the face and bounding boxes to their respective
                        # lists
                        faces.append(face)
                        locs.append((startX, startY, endX, endY))
        # only make a predictions if at least one face was detected
        iflen(faces) > 0:
                # for faster inference we'll make batch predictions on all
                # faces at the same time rather than one-by-one predictions
                # in the above `for` loop
                faces = np.array(faces, dtype="float32")
                preds = creditNet.predict(faces, batch_size=32)

        # return a 2-tuple of the face locations and their corresponding
        # locations
        return (locs, preds)

# load our serialized face detector model from disk
prototxtPath = r"spam_detector\deploy.prototxt"
weightsPath = r"spam_detector\res10_300x300_ssd_iter_140000.caffemodel"
faceNet = cv2.dnn.readNet(prototxtPath, weightsPath)

# load the face credit detector model from disk
creditNet = load_model("spam_detector.model")

# initialize the video stream
print("[INFO] starting video stream...")
vs = VideoStream(src=0).start()

# loop over the frames from the video stream
while True:
        # grab the frame from the threaded video stream and resize it
        # to have a maximum width of 400 pixels
        frame = vs.read()
        frame = imutils.resize(frame, width=400)

        # detect faces in the frame and determine if they are wearing a
        # face credit or not
        (locs, preds) = spammer_detect(frame, faceNet, creditNet)

        # loop over the detected face locations and their corresponding
        # locations
        for (box, pred) in zip(locs, preds):
                # unpack the bounding box and predictions
                (startX, startY, endX, endY) = box
                (spam, withoutspam) = pred

                # determine the class label and color we'll use to draw
                # the bounding box and text
                label = "spam" if spam >withoutspam else "No spam"
                color = (0, 255, 0) if label == "spam" else (0, 0, 255)

                # include the probability in the label
                label = "{}: {:.2f}%".format(label, max(spam, withoutspam) * 100)

                # display the label and bounding box rectangle on the output
                # frame
```

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115103

V. CONCLUSION

Considering impatience and restlessness of people nowadays the requirement of having faster and seamless transactions is more and is demanding this application which is developed aims to make the processing and checking in of customers easier and more accessible. In comparison to existing modules, this proposed module is applicable for the larger dataset and provides more accurate results. The Random forest algorithm wills provide better performance with many training data. In this paper, Machine learning technique like Logistic regression and Random forest were used to detect the fraud in credit card system. Sensitivity, F1Score, accuracy and error rate are used to evaluate the performance for the proposed system. By comparing all the three method, found that random forest classifier is better than the logistic regression.

VI. FUTURESCOPE

We currently aren't using any database storage for faster retrieval and storage so we would like to improve the project to use a global database which can be distributed across the servers. The processing requires faster CPU as the performance was CPU bound and we plan to include more algorithms for faster processing and enable more efficient recognition.

VII.REFERENCES

[1] Shaikh, Asma & Mhadgut, Aditi & Prasad, Apurva & Shinde, Bhagyashree & Pandita, Rohan. (2019). Two-way Credit Card Authentication With Face Recognition Using Webcam. International Journal of Engineering Trends and Technology. 67. 160-162. 10.14445/22315381/IJETT-V67I5P227. .

[2] Miss. Mayuri Chavan, Miss. Diksha Sawant, "CREDIT CARD AUTHENTICATION USING FACIAL RECOGNITION" International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04 | Apr 2019.

[3] Tison Varghese, Vidya Nambiar, Pushkar Dandekar, "Authentication of Credit Card Using Facial Recognition" International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS) Volume VII, Issue IV, April 2018.

[4] Asma Shaikh, Aditi Mhadgut, "Two-way Credit Card Authentication With Face Recognition Using Webcam" International Journal of Engineering Trends and Technology (IJETT) – Volume 67 Issue 5- May 2019.