e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

CREDIT CARD FRAUD DETECTION USING NEURAL NETWORK

R Akaash[*1], Chandru V[*2], Robert P[*3] , Dr. M Anand[*4]

[*1,2,3]B. Tech Students ,Electronics and Communication Engineering ,
Dr. MGR Educational and Research Institute , Tamil Nadu , India.

[*4]Professor, ECE , Dr. MGR Educational and Research Institute , Tamil Nadu , India.

ABSTRACT

The credit card business has increased speedily over the last two decades. Corporations and establishments are moving towards various online services, which aims to permit their customers with high potency and accessibility. The evolution is a huge step towards potency, accessibility, and profitableness of view. Nevertheless, it additionally has some downsides. These smart services are recently prone to significant security related vulnerabilities. Developing business through card depends on the fact that neither the card nor the user needs to be present at the point of transaction. Thus, it is impossible for merchandiser to check whether the cardholder is real or not. Companies loss in recent times are majorly due to the credit card fraud and the fraudsters who ceaselessly obtain new ways to commit the unlawful activities. As we know that Artificial Neural Network (ANN) has the ability to work as a human brain when trained properly. So, we will be implementing a neural network along with Self Organizing Map (SOM) and discuss about its performance and accuracy. Credit Card extortion are defined as the frauds which take place using the Credit Cards or Debit Cards particularly in the online transaction. Fraud detection methods are designed with an objective to prevent the online frauds in the system. By analysing existing data and detecting fraud is the foremost among the best techniques to reduce the successful frauds. Any variation in “usual spending” will also help to determine frauds. Some ways in which the fraudster can commit frauds are Merchant Related Fraud, Site Cloning, False Merchant Site, Credit Card Generators etc.

Keywords: Artificial Neural Network (ANN), Machine Learning, Self-Organising Maps (SOM).

I. INTRODUCTION

In many places credit card frauds and banking frauds have increased significantly causing a lot of problems for the users and also banks to keep their money safe and also detecting these frauds have been very difficult as the pattern of frauds keep on changing hence, we have thought of developing an application that can detect frauds automatically irrespective of the trends followed. The aim of the project is to create a simple web application tool for credit card fraud detection that will help users to keep their credit card safe and also for banks to maintain a secure application and keep their money safe from frauds. Fraud detection methods are designed with an objective to prevent the online frauds in the system. By analysing existing data and detecting fraud is the foremost among the best techniques to reduce the successful frauds. Any variation in “usual spending” will also help to determine frauds. Since human tend to follow specific behaviouristic profile such as the category of shopping. In our project report we will be taking a survey on how this application helps in and the feasibility of this application. Then we will be explaining the core architecture and design of our project and give a detail idea on the requirement analysis and the time taken to complete this project. Then we will be explaining the design of our project and will also give a detail diagrammatic explanation on how our project functions for general users. Then we will perform the testing for our project and also, we will also be quoting about of future works based on this project with the reference section on how we got an idea to do this project.

II. LITERATURE SURVEY

‘Fraud’ in Mastercard transactions is unauthorized and unwanted usage of an account by somebody aside from the owner of that account. Necessary hindrance measures are often taken to prevent this abuse and also the behaviour of such dishonourable practices are often studied to reduce it and shield against similar occurrences within the future. In different words, Mastercard Fraud are often outlined as a case wherever someone uses somebody else’s Mastercard for private reasons whereas the owner and also the card issuance authority’s area unit unaware of the actual fact that the cardboard is being employed. They obtained the dataset from Kaggle, an information analysis web site that provides datasets. within this dataset, there are thirty-one columns out of

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

that twenty-eight are named as v1-v28 to shield sensitive knowledge. The approach that this paper proposes, uses the newest machine learning algorithms to find abnormal activities, known as native outlier issue and also the model is isolation forest algorithmic program. It is Associate in Nursing unsupervised Outlier Detection algorithmic program. 'Local Outlier Factor' refers to the anomaly score of every sample. It measures the native deviation of the sample knowledge with reference to its neighbours. The Isolation Forest 'isolates' observations by indiscriminately choosing a feature and so haphazardly choosing a split price between the most and minimum values of the selected feature. While the algorithmic program will reach over 99.6% accuracy, its exactness remains solely at twenty eighth once a tenth of the info set is taken into thought. However, once the whole dataset is fed into the algorithmic program, the exactness rises to thirty third. This high proportion of accuracy is to be expected thanks to the massive imbalance between variety| the amount |the quantity} of valid and number of real transactions.

III. METHODOLOGY

The proposed solution is a web application. The reason being the banks is filled with transactions of a wide range of fraud groups. The best and most effective way of detecting and preventing fraud is a good neural network model and a GUI for people to check the security of their card. In small-scale textile companies, a credit card is mostly predicted through manual methods. It is also wasted potential data for business intelligence. Most existing companies have one or more computers, so with a web application, there will not be a need to detect frauds manually an automated system will give an alert if any unusual transactions occur.

ARCHITECTURE DIAGRAM

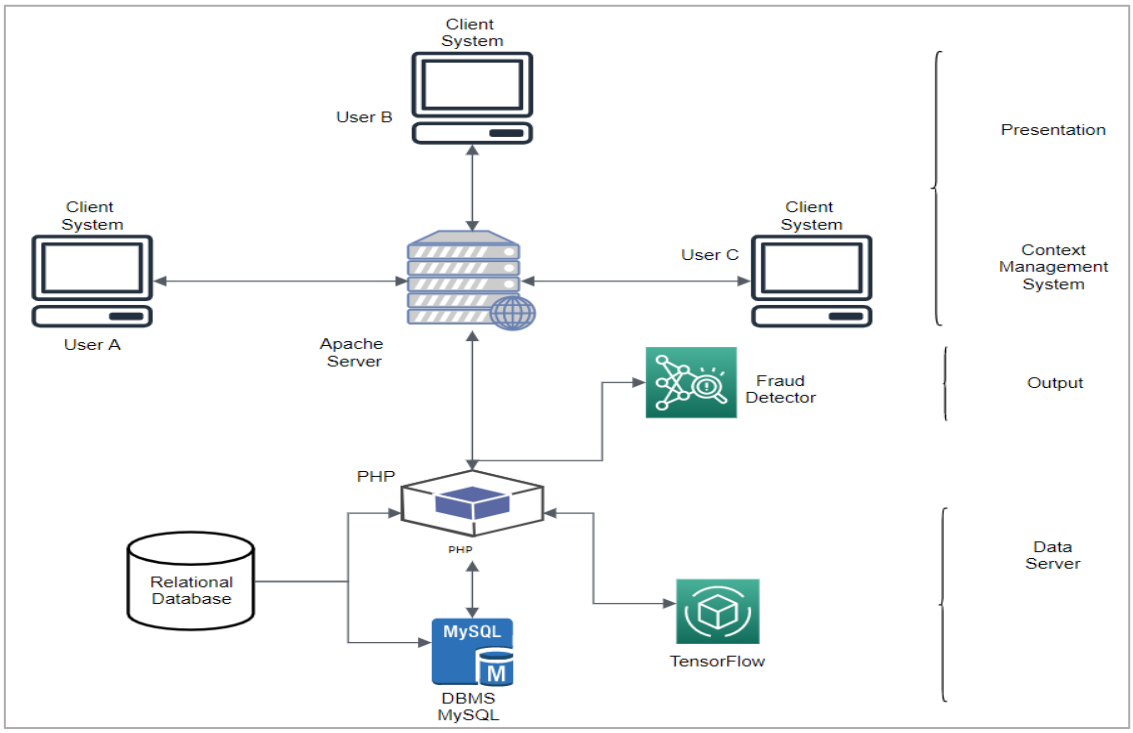

Figure 1: Architecture Diagram

The web architecture is designed in such a way that we can use it as credit card fraud detection. The web app was developed using PHP, python as server-side scripting and also the website will help the user to input the file with his details that will be read by the server and based on the details it will determine whether the transactions will have probability of fraud that has occurred. We will also be using the TensorFlow module to perform the prediction and detecting the credit card frauds.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

USE CASE DIAGRAM

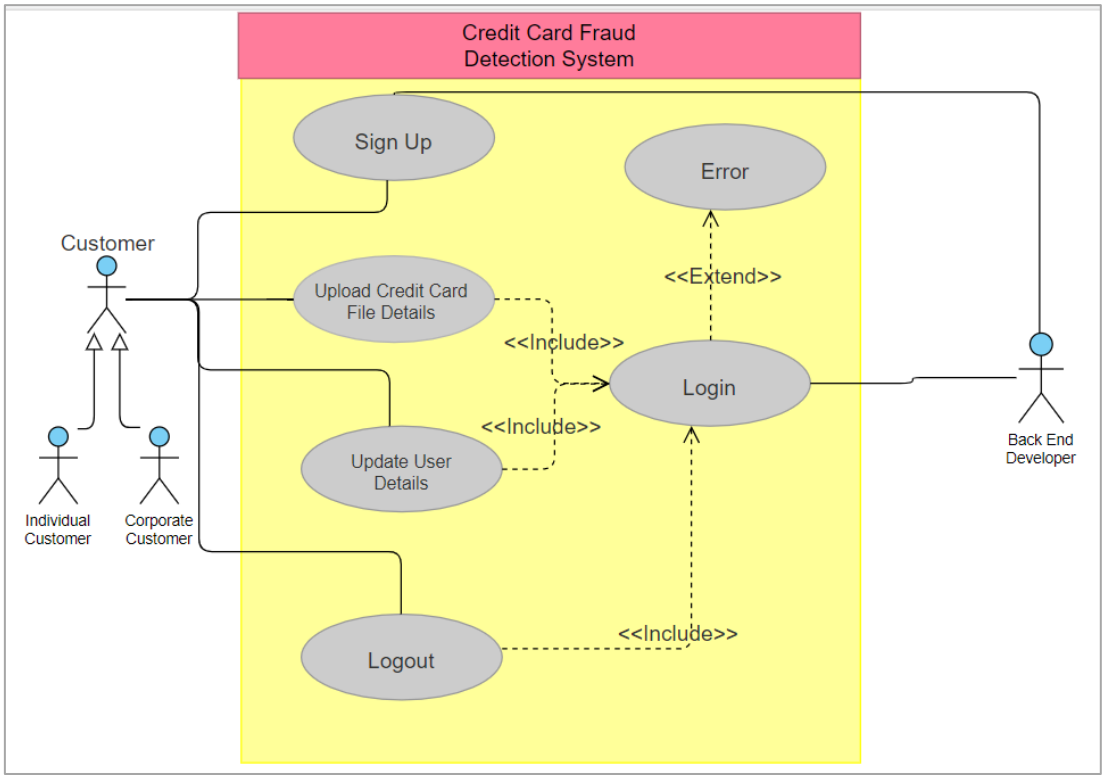

Figure 2: Use Case Diagram

Use case in description format

Use Case Title	**Transfer Data**
Description	A user who wants to find out whether his credit card is fraud or not, can enter his details to signup and login in which he can modify his account details or upload the details of his card in the form of file, which will inform the user whether his card is fraud or not.
Actor (s)	User, Back-end developer / Admin
Preconditions	The file must contain the details of card which is issued by the bank on request. The user must have an account in the website.
Postconditions	The user gets his result (credit card is fake or not) or his personal details that he has modified is updated.
Main success scenario	User enters his details and selects the “signup” button. The user’s information’s are accepted and grants the user to login to the main page. User selects the “upload file” option and uploads his file containing the card details. The user gets his desired results. Or the user selects “account setting” option and modifies his personal information. His account details have been updated.
Extensions	The user does give proper personal information. The user’s account is not created. User backs out of the use case

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

	The user does not upload file with proper card details User's file is not getting accepted User doesn't get his desired results.

IV. MODELING AND ANALYSIS

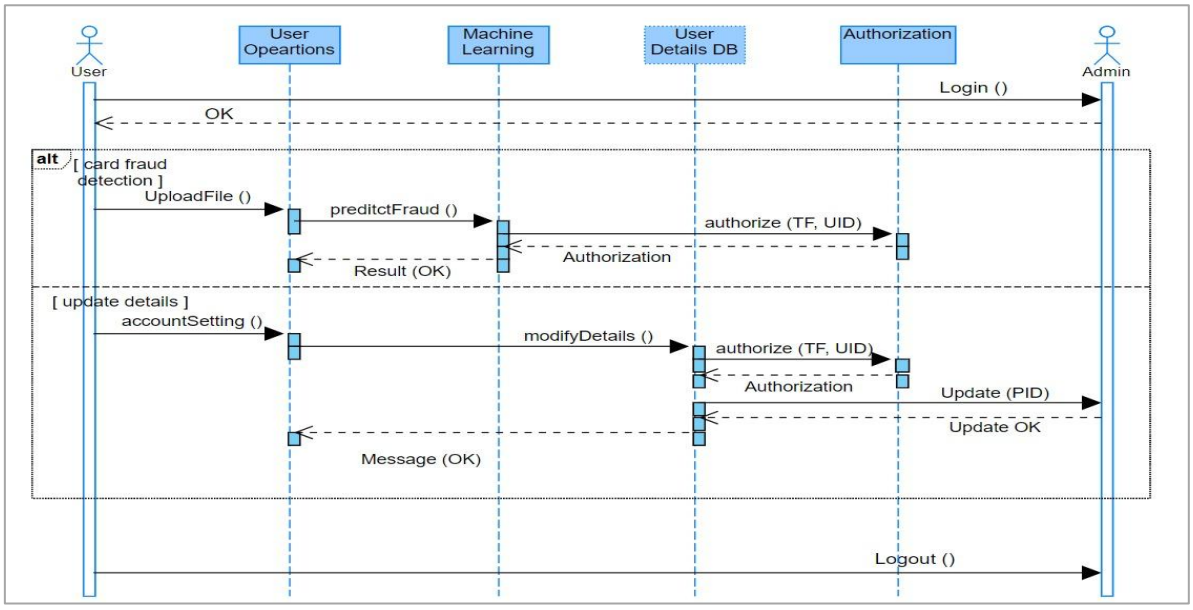

Figure 3: Interaction Diagram

UI DESIGN

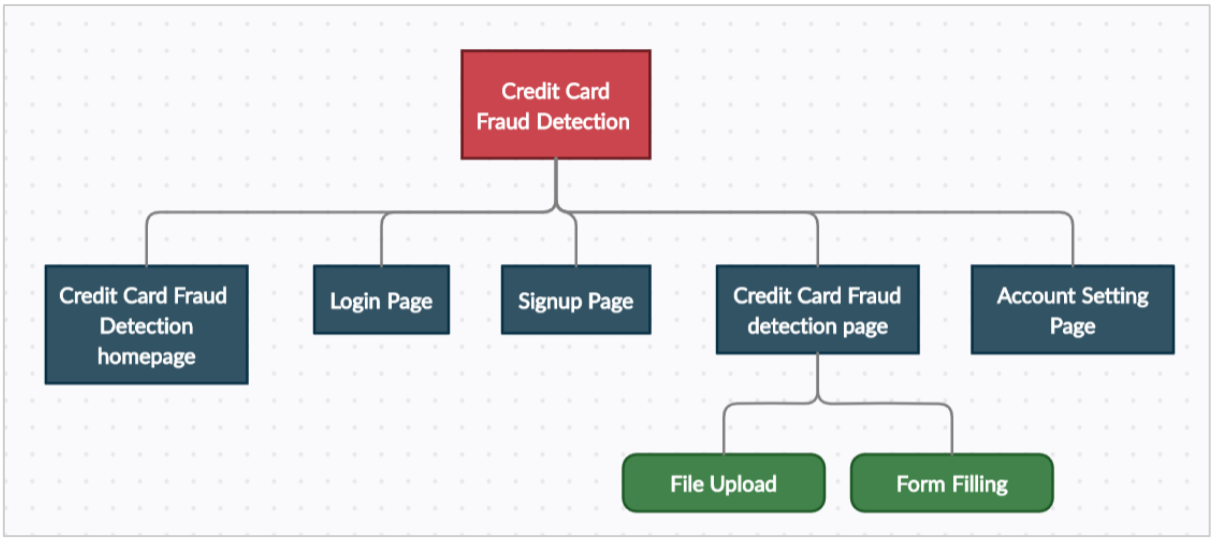

Figure 4: UI Design

1. The system will formulize the user's dynamic spending pattern based on first N purchases, comparing each purchase with the pattern and update the pattern gradually.
2. Many factors are considered in building the pattern including user's approximate annual income; gender; address; when and where most of the transaction had taken place; the average amount per transaction; the frequency of using ATM; user's tipping habits; categories of items that had been bought and so on.
3. In terms of comparing the most recent purchase P1 with the pattern P, the system will analyse a set of figures G, which includes the distance between P1 and P, the amount of transaction between P1 and P, the time of P1 and P and many other factors, used to come up with a numeric value Gs.
4. Based on the value of Gs, the system will determine the suspicious level S of P1 and notify the users whether the credit card is fraud or not.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

V. RESULTS AND DISCUSSION

IMPLEMENTATION DETAILS

For implementing the credit card fraud detection using neural network, we took the dataset from UCI repository

DATASET: http://archive.ics.uci.edu/ml/datasets/statlog+(Australian+Credit+Approval)

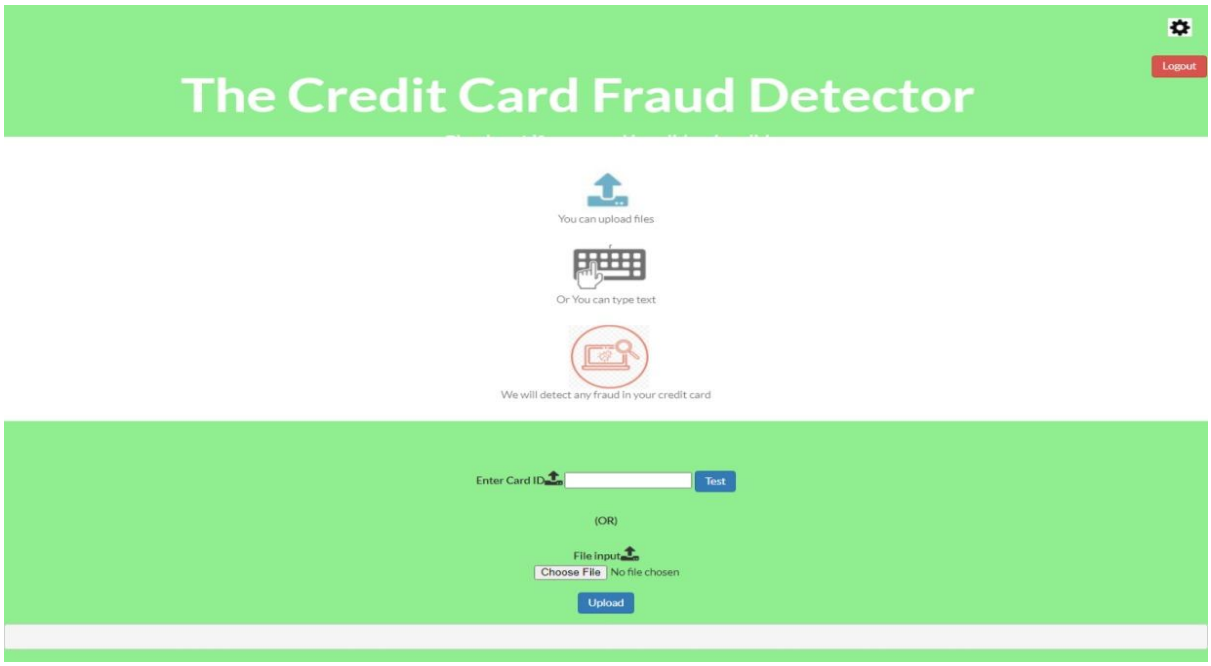

Figure 5: Credit Card Fraud Detection Page

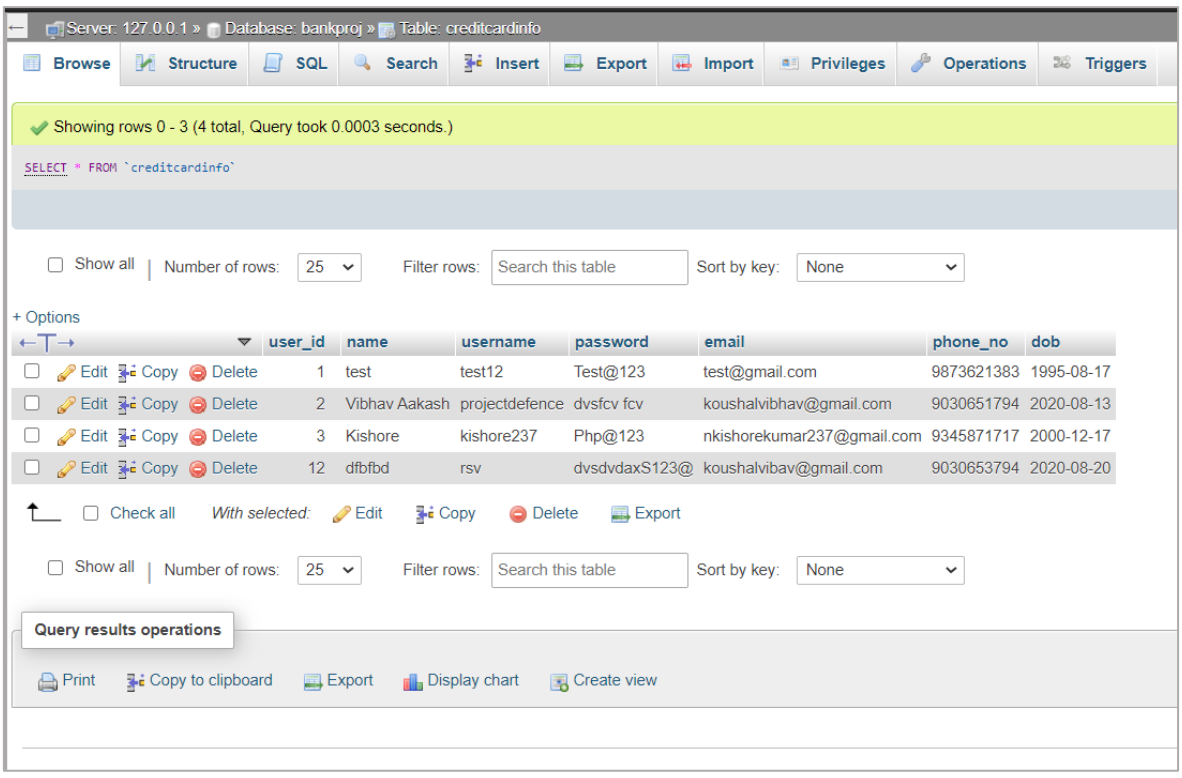

Figure 6: Database(phpMyAdmin)

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

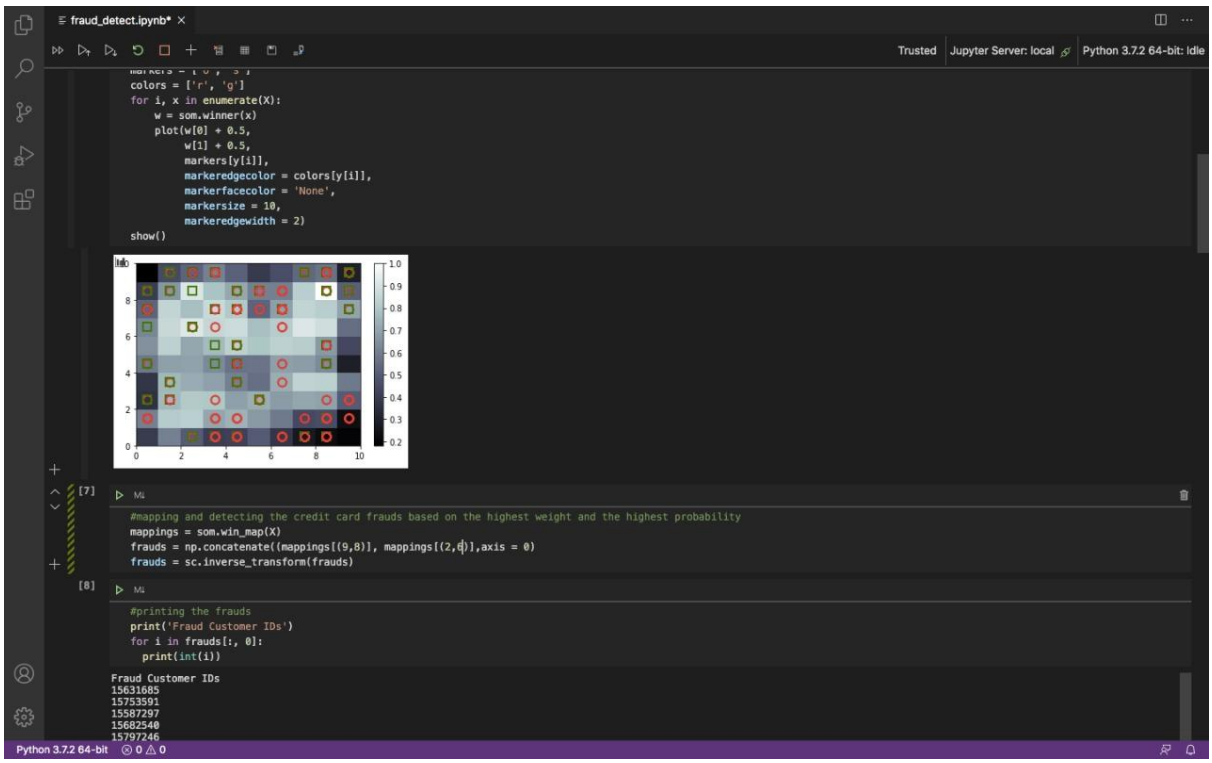

Figure 7: Implementation of Neural Network

VI. CONCLUSION

The described method using Artificial Neural Networks and SOM has better chances of successfully detecting credit card extortion. With every parameter verified and well represented in plot diagram. The singularity of our approach lies in using the clustering mechanism of SOM for the detection of credit card extortion activities. This helps in detecting hidden patterns of the transactions which can't be identified when compared with the other common methods used as of now. With appropriate colour schemes over representation of data sets and with the help of thousands of iterations the system is trained and then it can be used to predict the chances of fraud in the next transaction. Therefore, concept of SOM will be extremely efficient in the detection of the anomalies in credit card fraud cases. Hence, this model may help user or bank to manage frauds and to avoid the occurrence of fraud as early as possible.

VII. REFERENCES

[1] A. Vellidoa, P.J.G. Lisboaa, J. Vaughan "Neural networks in business: a survey of applications". Elsevier, Expert Systems with Applications, (1999). 17; (51–70).

[2] R. T. Trippi, E. Turban (eds), Neural Networks in Finance and Investing, Probus Publishing Company (1993).

[3] Aihua Shen, Rencheng Tong, Yaochen Deng "Application of Classification Models on Credit Card Fraud Detection". (2007).

[4] Anshul Singh, Devesh Narayan "A Survey on Hidden Markov Model for Credit Card Fraud Detection". International Journal of Engineering and Advanced Technology (IJEAT), (2012). Volume-1, Issue-3; (49- 52).

[5] B.Sanjaya Gandhi , R.Lalu Naik, S.Gopi Krishna, K.lakshminadh "Markova Scheme for Credit Card Fraud Detection". International Conference on Advanced Computing, Communication and Networks; (2011). (144- 147).

[6] Bidgoli, B. M., Kashy, D., Kortemeyer, G. & Punch, W. F "Predicting student performance: An Application of data mining methods with the educational web-based system LON-CAPA". In Proceedings of ASEE/IEEE frontiers in education conference. . (2003).

[7] Bolton, R. J., Hand, D. J (2002). "Statistical fraud detection: A review". Statistical Science (1994).28(3);

(235—255).

[8] Clifton Phua, Vincent Lee, Kate Smith, and Ross Gayler "A comprehensive survey of data mining-based fraud detection research". In Artificial Intelligence Review. (2005).

[9] Cortes, C. & Vapnik, V "Support vector networks, Machine Learning". . (1995). Vol. 20; (273–297).

[10] De Castro Silva, L. N., & Zuben, F. J. V "An evolutionary immune network for data clustering". In Proceedings of the IEEE SBRN (Brazilian Symposium on Artificial Neural Networks); . (2000). (84–89).

[11] De Castro, L., & Timmis, J "Artificial immune systems: a new computational approach". London, UK: SpringerVerlag. . (2002).

[12] Jeske, D.R. Lin, P.J. Rendon, C. Rui Xiao Samadi, B., Synthetic Data Generation Capabilties for Testing Data Mining Tools. IEEE : Military Communications Conference, pp.1-6, 2006

[13] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar. "Credit Card Fraud Detection using Hidden Markov Model". IEEE Transactions on dependable and secure computing,Volume 5; (2008) (37- 48).