 ISSN: 2454-4248
75 – 77

Fraud Detection using Machine Learning in the Mobile Payment Service

[1]Mr.Riju Bhattacharya,[2]Arshiya Fatima,[3]Priyanka Kale
[1]Asst. Prof (CSE), SSIPMT Raipur,[2]B.E. (CSE), SSIPMT Raipur,[3]B.E. (CSE), SSIPMT Raipur
[1]riju@ssipmt.com, [2]arshiya.fatima@ssipmt.com, [3]priyanka.kale@ssipmt.com

***Abstract*:-**The transformation of payment mechanism from face-to-face transactions to non-face-to-face transactions has led to increased popularity of Internet Banking, credit card, online billing in the mobile phone itself and, hence, it is directly proportional to the advancement of smartphones in particular. However, the probability of any kind of anomalous payments increases and due to that the requirement of fraud detection arises. This paper provides the idea of the trend followed in the detection of fraud in online payment through mobile phone with the help of machine learning [1].

Keyword*:-Fraudulent, Transactions, Training, Testing, accuracy, cross-validation, Artificial Intelligence.*

*****

I. Introduction

The requirement of FDS (Fraud Detection System) is increasing day by day due to various criminal issues. The system exhaustively evaluates the terminal data which is used in the transaction. FDS stabilize various techniques which are based on the past fraud analysis. But the dependencies on past cases are not sufficient to deal with attackers as various new approaches can also be generated by them to fetch the data used in processing. So to avoid those kinds of situations, various strategies need to be followed [5].

Machine Learning Technology

Machine learning technology has a resemblance to Artificial Intelligence. In actuality, machine learning is a subpart of Artificial Intelligence which somehow let the machine to think its own and take crucial and critical decisions whenever requires. Instead of providing command explicitly it allows the system to positively learn and enhance the result from experience. The whole process initiates from examining the data and to look up all the aspects related to that data followed by various instructions. The primary purpose is to let the system free without any interaction of human [7].

The machine learning comprises categorization and assembling of data. It is of various types.

Supervised learning – This learning method is trained with some labeled examples. The input with its desired output is known before initiating so that classification can be done accurately with the help of training data (fraud or non-fraud). The algorithm needs to learn the relationship between input and output and it is expected that for the upcoming data, the same theory can be applied and then resolved. Hence, it is applied in those conditions where the events of past depict the upcoming events. Basically, these method is used for the classification of data and it comprises - random forest [3], Support vector machine (SVM), Neural network [2], etc.

Example –This type of learning can judge the instance where the credit card is likely to be fraudulent.

Unsupervised learning– This learning method does not predict any pattern but analyzes the data thoroughly. The output is unknown here. It does not have any previous label. The main intention is clustering. Popular techniques are K-means clustering [3], self-organizing map [1], etc.

Example - This type of learning can be used to segment text, and to endorse things.

Reinforcement learning – This learning method depends on the hit and trial mechanism. It has three basic elements: the agent (the one who takes the decision), the environment (for the communication of agent) and actions (what agent need to perform). The agent selects certain actions that will maximize the expected output as per the provided time. The agent can achieve the desired target by following a good strategy. So, the purpose of this type of learning is to learn the policy [6].

Example – This type of learning is used in the field of robotics, gaming, and technology.

II. . Fraud Detection System

The Fraud detection system is that kind of system which comprehensively examines all the transactions details along with the terminal data and IP address used in the electronic transaction so that all the fraudulent acts can be exposed.
It basically works as per four different functions [3].

Data gathering – This type of function gather the environment data and accident-type data for the accurate investigation of the whole process.

Analysis and detection – This type of function analyze the data and also keep an eye on the uncommon transaction by using rule inspection mechanism. That type of transaction can be detected by using misuse detection model and abnormality detection model.

Response – This function reacts vigorously if the abnormality is found on it.

 ISSN: 2454-4248
75 – 77

Monitoring and Audit – This function manages all the process and audit [2]function addresses the risk of fraud.

Detection using Machine Learning

With the help of FDS functions,the very first task is data gathering and also segmenting it. After this task machine learning model is included with some training sets so as to find the probability of fault [7].

Extraction of data – The date is simply fragmented into three segments: training, testing, cross-validation. The algorithm will be trained on a selective set and parameters entitled to the testing set. The measurement of behavior of the data is done with the help of cross-validation set. The performing model is then examined for different splits [4] [5].

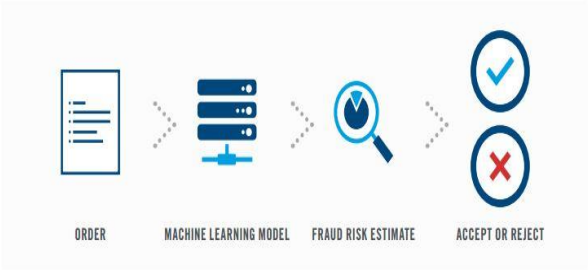

Figure 1. The Process of detection of fraud

Furnish training sets – The main significance of machine learning is the ability of prediction. It needs to predict some output, such as boolean value (true for success and false for failure) for the given input.

The data which is responsible to train the machine learning models comprises records with both the output values forvarious input values. The records are usually obtained from the historical data.

Building models – It is an essential step in predicting the abnormality in various sets of data. One can determine in what sense the prediction should be made with the help of input and output values.Prediction problem splits into two types: Classification and Regression [7].

III. The Approach to Machine Learning

In supervised learning, the support vector machine (SVM) provides high accuracy in terms of classification because of its architectural feature of selecting the appropriate standard to categorize the given data properly.

In unsupervised learning, the accuracy is obtained in K-means. It categorizes the input data as per the K-value setting. To differentiate between normal transactions and fraudulent transactions, for grouping the value of K=2 is taken [2][5].

4. Mobile Payment System

It involves three major identities:

- the user
- mobile telecommunication company
- the payment agencies

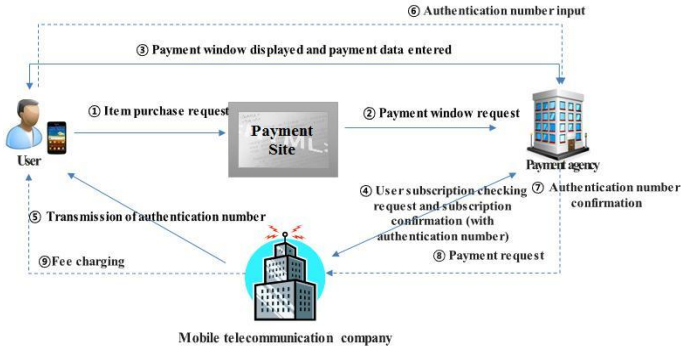

Figure 2. Mobile payment service

The mobile services allow users to pay through a mobile device as it combines with telecommunication company which authenticates the individual user and the payment agencies handle the process.

The fraud detection system is allocated in the payment agency and it checks the user's information with the service provider (base stations) and transmits the authentication number (if the success message is received from the service provider). But if the FDS indicates abnormality then the service is terminated and additional ARS authentication using voice is carried out.

IV. . Analysis of abnormal Transaction

The analysis with the help of prediction needs some scope under which the different probability should be considered.
There are various factors under which analysis or the investigation can get a clue about abnormality. They are Transaction date, Transaction amount, Cancellation date, Cancellation time, Sales type, etc.
The difference between transaction time and authentication time should not exceed 20 sec because usual time is 10-20 sec and if it crosses these, that means the data is taking time to travel and hence the chances of fraud increases.

V. Conclusion

Machine learning is that part of Artificial Intelligence which predicts the upcoming move with the help of historical data. Fraud detection is a must requirement for the payment through the mobile phone. There are various types of models for that. In supervised learning the support vector machine and in unsupervised learning K-value provides accuracy in fraud detection. There are various stages which need to follow in FDS right from data gathering to audit function. The whole scenario of fraud detection is dependent on how accurately the

 ISSN: 2454-4248
75 – 77

algorithm predicts the next pattern. Machine learning provides relief to the financial industry by providing a safe environment to access the mobile device accurately.

VI. . References

[1] Mitali Bansal and Suman, Credit Card Fraud Detection Using Self Organised Map, International Journal of information & Computation Technology, ISSN 0974-2239 Volume 4, Number(2014), pp. 1343-1348, 2014.

[2] Guide to Fraud Detection System Technology, Financial Security Institute, 2014.

[3] C. Whitrow, D.J. Hand, P. Juszczak, D. Weston, N.M. Adams, "Transaction Aggregation as a Strategy for Credit Card Fraud Detection," Data Mining and Knowledge Discovery, Vol. 18, No. 1, pp. 30-55, Feb. 2009.

[4] Abhinav Srivastava, Amlan Kundu, Shamik Sural, "Credit Card Fraud Detection using Hidden Markov Model," Dependable and Secure Computing, Vol. 5, No. 1, pp. 37-48, Jan. 2008.

[5] https://www.sas.com/en_us/insights/articles/risk-fraud/fraud-detection-machine-learning.html#/ [online]

[6] http://www.expertsystem.com/machine-learning-definition/[online]http://www.ulb.ac.be/di/map/adalpozz/pdf/Dalpozzolo2015PhD.pdf."