https://doi.org/10.46335/IJIES.2022.7.9.10 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 48-51

International Journal of Innovations in Engineering and Science, www.ijies.net

ATM Fraud Detection System using HMM & SVM Algorithm

Gurjeet Ujjainwar[1], Ashish Gacche[2], Aniket Bawankule[3], Aditya Sahare[4], Kajal Labhane[5], Priyanka Gonnade[6]

[12345]G H Raisoni Academy of Engineering & Technology (GHRAET), Nagpur, Maharashtra, India – 440028
[6]Assistant Professor,G H Raisoni Academy of Engineering & Technology (GHRAET), Nagpur, Maharashtra, India

gurjeet.ujjainwar.cs@ghraet.raisoni.net

***Received on**: 11 June ,2022* ***Revised on**: 06 August ,2022,* ***Published on**: 09 August,2022*

***Abstract –** The banking sector has long been a critical institution that contributes significantly to a country's economic sustainability and maintenance. When bank transactions are tampered with by intruders or fraudsters, the results can be disastrous. This article aims to examine the current system of Electronic Fund Transfer (EFT) ATM activities in terms of cash withdrawal, fund transfer, password hacking, pin misplacing, and biotechnology. The article will look at many types of frauds and try to come up with a solution for solving and detecting frauds on ATMs, as well as a more advanced machine that can accept security technology. Fraudsters have untiring times making illegal moneys while the proposed algorithm in this work will combat most efforts of illegalities regarding funds by electronic data processing (EDP) in the Banking sector; this will be achieved by data mining the bio data though biometric combinational operations at the initial opening of the accounts and as such will conform with the algorithm proposed; the paper worked carefully using the existing literatures and systems to combine the approaches of biometric to the already existing ones and making a complete proposal for a design of ATM engine that will be having on it an incorporated thumbprint capture area and the possibility of the eye scanners and also make sure it doesn't slow down the process to unacceptable speed.*

Keywords- ***ATM, Fraud Detection, Machine Learning, Fraud Detection Systems, Security, Electronic fund transfer (EFT), Electronic data processing.***

I- INTRODUCTION

People with data mining-based ATM card fraud detection models have been the most prominent data mining worry in recent years. When it came to detecting ATM card fraud in online transactions, data mining was crucial. Traditional data mining strategies are inapplicable since our challenge is handled as a classification problem. As a consequence, an alternate method using general-purpose meta heuristic procedures like machine learning techniques is developed.

The purpose of this research is to develop a genetic algorithm-based system for detecting ATM card fraud. Machine learning algorithms are iterative algorithms that seek to improve solutions over time. It uses machine learning approaches to optimize a set of interval-valued parameters in order to eliminate false alarms. Using a genetic algorithm, create an ATM card fraud detection system. The fraud is recognized during an ATM card transaction, and a genetic algorithm is used to limit the amount of false warnings.

We constructed an objective function with variable misclassification costs instead of maximizing the amount of transactions that have been accurately categorized, so that correctly categorizing certain transactions is more important than correctly categorizing others. This data is relevant to the analysis of the proposed system. Here are all of the cost and performance considerations that will affect the project's feasibility, as well as the project's purpose.[2][5][11][16]

II-METHODOLOGY

Machine learning algorithms are classified as supervised, unsupervised, or semi-supervised. Algorithms for Supervised Machine Learning: By applying pre-learning to fresh data, you may utilize labeled examples to anticipate future events. The learning algorithm creates a derived function to predict the output value based on the examination of a given training dataset. After adequate training, the system may create a target for each new input. The training method may compare its output to the proper intended output to find and rectify model faults. Unsupervised machine learning approaches are employed when there is no way to categories or tag training data. Unsupervised learning is the study of how computers extract functions from unlabelled input and explain hidden structures. Rather than selecting the best output, the system assesses the input and uses the dataset to infer hidden structures from unlabelled data. Because they train with both labeled and unlabelled data, semi-supervised machine learning algorithms lie between supervised and unsupervised learning, with a small quantity of labeled data and a significant amount of unlabelled data. unlabelled and labeled This method can enhance learning accuracy greatly in systems that use it. When the acquisition of labeled data necessitates the employment of adequate and skilled training/learning resources, semi-supervised learning is frequently utilized. Collecting unlabelled data, on the other hand, seldom necessitates the use of additional resources.[20][12][10][16]

HMM Based Fraud Detection:

HMM (hidden message) A statistical model in which the system under investigation is believed to be a Markov process with an unobserved state is known as a Markov model. It identifies fraud by analyzing user expenditure profiles, which are divided into three categories: Lower profile, moderate profile, and higher profile are the three options .Phases of the procedure include training, detection, and prevention.

Start the bank server and the HMM server first in this model. When a transaction is initiated by the client, HMM begins observing and comparing the operation. If fraud is detected, the transaction is halted and blocked. User enters a password on a mobile phone and sends it through Bluetooth to the same bank ATM, or sends it by SMS. When the password is verified for authenticity, the transaction is accepted. After three attempts, the transaction is completely blocked.[3][7][18][17]

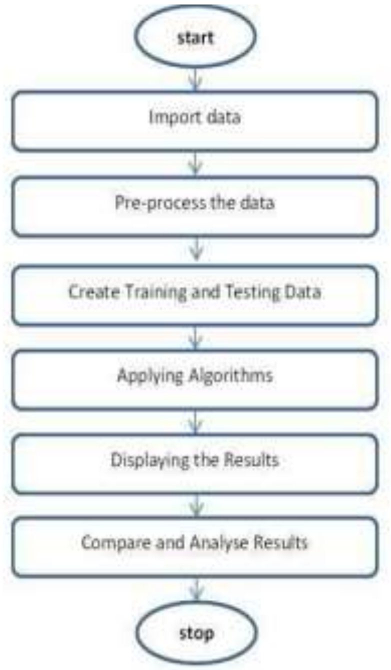

Fig. 1 -describes the flowchart of the algorithm

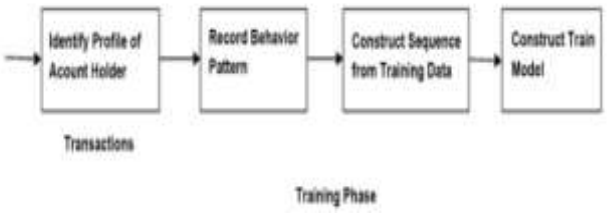
Identify Profile of Acount Holder
Record Behavior Pattern
Construct Sequence from Training Data
Construct Train Model
Transactions
Training Phase

Fig. 2- Training Phase of model

Support Vector Machine (SVM) Based Fraud Detection:

SVMs, or Support Vector Machines, are statistical learning systems that have been employed in a variety of applications. The hyper plane is used as the decision plane in the SVM classification approach, and the distance between the positive and negative modes is maximized. For classification, regression, and other issues, SVM is a common machine learning method. A SVM library is LIBSVM. LIBSVM is usually used in two steps: first, to train a model, and subsequently, to predict data from a test dataset. The key characteristics of SVM are as follows:1) Create the training data for the model first. 2) Then, for the newly produced dataset, set SVM parameters and send it to Training in SVM. 3) SVM Trainer: This software trains every single data point in the enormous dataset. 4) After the dataset has been fully trained, the SVM Predictor predicts the training data.[4][6][13][21]

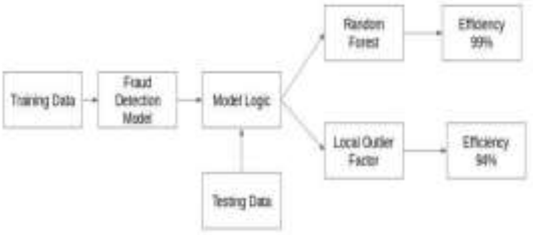

Fig. 3- Flow of Implementation

The fig.3 describes the flow of implementation

Algorithms:

The Decision Tree Algorithm and How to Use It
Step 1: The data must first be imported.

Step 2: Determine the training-to-testing data ratio.

Step 3: Using the most significant attribute as the root, divide the dataset into subgroups.

Step 4: Determine the number of buckets associated with the construction parameters.

Step 5: The Confusion Matrix and the Underlying Data Accuracy

III -RESULT

Dataset Description:

In the dataset, a client of a fictitious bank made ATM card transactions. This dataset contains 492 frauds out of 2,84,807 transactions in the preceding 48 hours. Positive categories (fraud) account for 0.172 percent of all transactions, suggesting a highly skewed data set. Only PCA-converted digital input variables are used. We can't provide the data's original properties or any underlying information for security concerns. "Time" and "Amount" are the two qualities that are unaffected by PCA. The 'Time' method keeps track of how many seconds have passed since the initial transaction in the collection. The "Amount" attribute represents the transaction's total value. Both cost-aware and example-based learning can benefit from this feature. The response variable "Grade" is set to 1 if cheating occurs; otherwise, it is set to 0.[1][9][14][15]

ATM FRAUD SYSTEM

admin

Log In

Form

Select File Choose File No file chosen

Fig.4 -Login Page

The fig.4 describes the login page information

Fig. 5 -Dashboard page

The fig.5 describes the Annual fraud detected in system

Fig. 6 -Bar graph representing the Fraud

The fig.6 describes the detected fraud in bar graph format

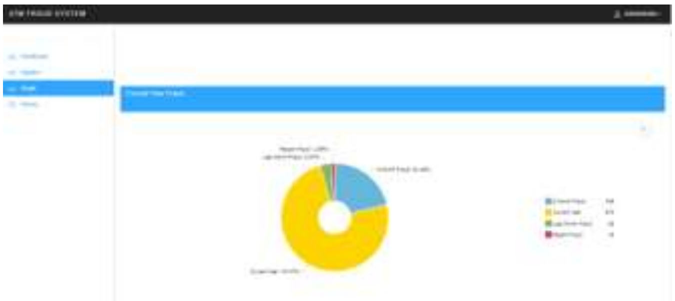

Fig. 7-Pie Chart for Annual detected fraud

The fig.6 describes the detected fraud in bar graph format

The output screens are depicted in the figures above. This screen displays the results of the algorithm applied to the original dataset. The following columns are included in the aggregated list of results:

- Total Fraud Hours
- Fraud transaction
- Graphical representation of Fraud Transactions
- Customer ID

IV- CONCLUSION

This method works well for identifying fraudulent transactions and decreasing false alarms. Machine learning techniques are innovative in this literature in terms of application domain. If this strategy is used in a bank's ATM card fraud detection system, fraudulent transactions may be anticipated shortly after they occur. Anti-fraud tactics can also be used to protect institutions from large losses and minimise risks. The study's aim was approached differently than normal classification tasks since we had a changing misclassification penalty. Because typical data mining approaches did not effectively fit this instance, we chose to use multi population machine learning procedures to generate an ideal parameter.

REFERENCES

[1] *Intelligent Anomaly Detection Model For Atm Booth Surveillance Using Machine Learning Algorithm: Intelligent ATM Surveillance Model:- S. Viji; R. Kannan; N. YogambalJayalashmi IEEE 19 Feb,2021*

[2] *Financial Fraud Detection Using Machine Learning:-C.Maheswara Reddy, Marri Saiteja, B.Shashank, Mrs.Dhikhi ACADEMIA Nov,2020.*

[3] *Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network:-Ermatita, IndrajaniSutedja IOP Publishing 10 Oct,2019*

[4] *Bethapudi, Dr Prakash & Murthy, G. & Ashok, P. & Prithvi, B. & Kira, S.. (2018). ATM*

[5] *Card Fraud Detection System using Machine Learning Techniques. International Journal*

[6] *for Research in Applied Science and Engineering Technology. 5.10.22214/ijraset.2018.4836*

[7] *Abdullahi, Ibrahim & Mishra, Amit & Ahmad, Barroon. (2010). Fraud Detection and Control on ATM Machines, an Algorithm for Combating Cash and Fund Transfer International journal of Physical Science. 5*

[8] *R. Laimek and N. Kaothanthong, "ATM Fraud Detection using Behavior Model," 2018 5th Asian Conference on Defense Technology (ACDT), 2018, pp. 21-25, doi:10.1109/ACDT.2018.8593092.*

[9] *Diebold Inc.(2006,"ATM Fraud and Security", White paper , www.diebold.com, pp.2*

[10] *Case, P. and S. N. Sisat, "Secured Automatic Teller Machine (ATM) and Cash Deposit Machine (CDM)," vol. 7782, pp. 118–121, (2014)*

[11] *Bank Indonesia, "MengenalKartu Debit & ATM," pp. 1–2, (2009).*

[12] *DepartemenKebijakanMakroprudensial, "Kajian StabilitasKeuangan," Igarss 2014, no. 1, pp. 1–5, (2014).*

[13] *Otoritas Jasa Keuangan, "Bijak Ber-eBanking," Bank Indonesia, (2015).*

[14] *Auditor General Western Australian, "Fraud Prevention and Detection in the Public Sector," pp. 1–24, (2013).*

[15] *Jog, Vivek V., and Nilesh R. Pardeshi. "Advanced Security Model for Detecting Frauds in ATM Transaction," International Journal of Computer Applications 95, no. 15, pp. 47-50, (2014). ICONISCSE IOP Conf. Series: Journal of Physics: Conf. Series 1196 (2019) 012076 IOP Publishing doi:10.1088/1742-6596/1196/1/012076 9*

[16] *Anderka, M., T. Klerx, S. Priesterjahn, and H. K. Büning, "Automatic ATM Fraud Detection as a Sequence Based Anomaly Detection Problem," Proc. 3rd Int. Conf. Pattern Recognit. Appl. Methods (ICPRAM 2014), (2014).*

[17] *Lepoivre, M. R., C. O. Avanzini, and G. Bignon, "Credit Card Fraud Detection with Unsupervised Algorithms," vol. 7, no. 1, (2016).*

[18] *Kass, G. V., "An Exploratory Technique for Investigating Large Quantities of Categorical Data," Applied Statistics, Vol. 29, No. 2, pp. 119–127, (1980).*

[19] *Svigals, J.;"The Long Life and Imminent Death of the Mag-Stripe Card"; IEEE Spectrum; (June 2012); 73-76*

[20] *M. Paliwal and U. A. Kumar: Neural networks and statistical techniques : A review of applications. Expert Syst. Appl., vol. 36, no. 1. (2009) 2–17*

[21] *Indrajani, Prabowo, Harjanto, Meyliana, "Learning Fraud Detection from Big Data in Online Banking Transactions: A Systematic Literature Review." Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 8.3 (2016): 127-131.ISSN 2180-1843 eISSN 2289-8131*