Mathematical Statistician and Engineering Applications
ISSN: 2326-9865
https://doi.org/10.17762/msea.v71i1.32

Analysis of Scope of Data Mining in Fraud Detection and Studying Solutions to Prevent Them

Nouby Mahdy Ghazaly
Associate professor mechanical engineering departments
Faculty of engineering
South valley university
Egypt

Article Info
Page Number: 16 – 20
Publication Issue:
Vol 71 No. 1 (2022)

Article History
Article Received: *12 November 2021*
Revised: *20 November 2021*
Accepted: *02 December 2021*
Publication: *01 January 2022*

Abstract

This paper will explain the process of fraud detection suing datamining techniques. Fraud detection is important task and many domains have risk of attack of fraudsters in the data that they have stored. It is very important that each domain like banking etc should have reliable fraud detection scheme so that the personal details of the users of the banks is safe and secure. There are a lot of techniques which can be used to detect fraud attack in the system

Keywords: - Fraud detection, Data mining techniques, Preventive solution

Introduction: - Whenever there is information and data are shared, there is always risk of it getting attacked by a fraud. It is essential that the data and identity of individual is safe and secure so that it does not get affected by the unauthorised attack. The security attack can happen in one of the following ways: -

- In the era of internet, the risk of security threat is very high. The fraud can send spam message on which if the user clicks then all the login details of the user can be passed on to the fraudster.
- In banking domain, if the system is not so secure and does have implemented security checks then there is possibility that the banking id of the user can be leaked and all the money from his account can be stolen.
- In social media apps, some people make fake profiles and pretend to be genuine and this can be a threat to other person's identity.
- There are chances of accounts getting hacked and can be used by the fraud for his own purpose.
- In case of debit and credit card, there are chances that the cards get hacked along with the pin and can be used by the fraud for his own use.

Thus, security attacks, fraud in the area of banking etc, is common and each domain should have proper fraud detection facility and should take preventive measures to not let it happen. The organisations are using latest techniques to detect and prevent the fraud. Following are the ways by which the fraud detection is being done: - [1]

- Fraud detection using fraud detection tools.
- Artificial intelligence using data mining techniques
- Data Analysis to study the fraud and prevent it
- Fraud identification using fraud detecting software.

Basically, there are two approaches to detect fraud: -

1. Statistical Data Analysis to detect Fraud: -

>In this technique, there are several steps which can be done to detect the fraud. First of all, the statistics study of all the calculations involved in the system should be done. The study of all the performance metrics, averages etc should be done and seen for any pattern.

>The relationship between components which are dependant on other components is done and also independent variables are also studied.

>The data which is stored twice means the duplicate data and components are identified and then removed.

2. Artificial Intelligence: - This can be done using one of the following technologies: -

> Data mining techniques: - Since many transactions can be performed at once and at the same time in data mining, it makes it easy to study the patterns in order to find fraud.

>Machine Learning: - This is the technique which is useful to identify the fraud pattern immediately and it is automated.

>Pattern identification technique: Its major role is to study the pattern and trends in any transactions and if identified it is further checked for fraud.

The business or the organisation should always take preventive measures to avoid the security attacks. They should implement such techniques that they could identify the chances of fraud attacks even before it occurs. First the organisation should have proper smart fraud identification and prevention solutions and then they should also have the arrangements to track and monitor any fraud activity that might happen. The advantage of the fraud detection will be that the frauds can be identified and reported and the business can be saved from a big loss due to that security attack. This will also help the business to grow in terms of performance attribute and customer satisfaction. The business should give confidence to the users that their investment is safe and their confidential data is safe with the business.

The organisations can also use following two methods to identify threat: -

a. Manual and automated: - In this method there will be separate dedicated team whose task is to identify all the trends and patterns of the transaction happening in the system. If they find any unauthorised access or user then they should immediately report it and save the further threats. This is manual way of identifying the threats and saving them.

   In automated fraud detection there will be tools which makes the task easy for the identification of the fraud. The tools provide facility to code and automate using algorithms which has the capability to identify the security threats. They even have the facility to report them automatically. So, in this type of technique there is no need for separate monitoring team to detect and prevent the fraud. Only once the coder needs to code the fraud detecting algorithms and rest will be taken care of. The code should make sure that the algorithms are coded in such a way that it cannot be hacked by the unauthorised user. The disadvantage of manual fraud detection is that a separate team will be needed to continuously monitor the transactions happening in the system in order to detect fraud which in turn put unnecessary pressure on the team and their efficiency to perform other tasks also decreases. So, this manual method is rarely used these days.

Fraud Detection Process: - [2]

There is proper process to perform the task of identification of the security attacks which should be performed to enhance the whole process: -

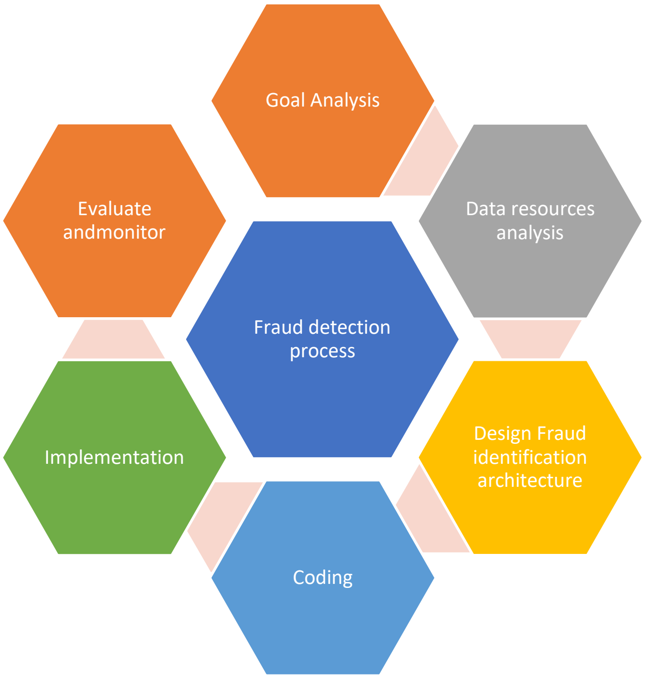

Figure 1 Fraud Detection Process.

1. Goal Analysis: - In this step the goal to implement fraud detection is done to understand its scope. It to identify the areas of the business where there are chances of fraudster. It is studied that what are the measures taken by the business to prevent the security attacks, whether they are reliable or not. Analysis is done on the efficiency of the already existing techniques used in the business. It they are found to be not reliable then it is further studied as to how enhance the fraud detection features or how to implement the new architecture.
2. Analysis Ing the data resources: -Once the objectives and goals of the security attacks has been done then in this stage the data resources in order to implement the detection system are identified. It can be details of all the accounts of clients in the system, the login details, the billing component, what all services and products are being used by the end user. Detailed study of each of the above mentioned will be done properly.
3. Designing of Fraud Detection Architecture: - In this step, based on the goals analysis and analysis of data resources, the designing of the fraud architecture is done. The work flow of the detection system is designed which will have data flow charts, graphs etc to represent everything. It is also decided how the data is passing through the detection system. In designing of the detection system, it is observed that how frequently the data being exchanged is tested for fraud and how accurately the detection system is working in order to identify all the security attacks. It is also checked whether the fraud detection is also been reported or not.
4. Coding and implementation of algorithms: - Based on the designing of the fraud detection system, in this step the coder will start coding the algorithms which will explain the actual working of the fraud detection system. Once the code is ready, the prototype of the module will be tested to check whether it is meeting all the expectations which means it is tested that if the fraud detection system is able to test and identify and report all the security threats to the data being exchanged. If the system is not able to identify then all the steps are repeated until we get results without any bug.
5. Maintenance: - Once the tester is satisfied that the system is not giving any bugs then it is handed over to the business to implement it in their live environment. If the customer wants to make any modifications, then it can be done in this stage once the fraud detection starts working in their

environment. Once it is implemented in real world then it will be little hard to modify as we need to repeat all the steps again.

6. Evaluate and monitoring: - The fraud detection designing team will provide full support to monitor the system to check whether it is working as per the business needs or not. They will give full support in case of any malfunctioning of the detection system. If they find that the fraudster is still not able to identify the fraud then they will make modifications and find out other best possible solutions to prevent those threat.

Above mentioned steps are for the designing and implementation of the common and basic fraud detection system. It will be different for different domains based upon the specifications of the business who will use it. Therefore, each step should be followed in synchronisation of the business goals and objectives.

Fraud Detection using Data Mining: -

Data mining is one of the procedures of Artificial intelligence which is used for the identification of the fraud detection. It is the process in which the data is collected from various resources and then made available in a large storage system which can be used by the users to perform data analysis and for reporting. Once the data is stored then it can be useful for studying various trends and patterns which can be useful for the fraud detection and can be prevented even before it takes place. Following are the three data mining techniques used to identify fraudsters: -

1. Decision Trees: - This type of technique is used in various domains like banking, insurance companies, hospitals etc. In a basic decision tree algorithm, there are nodes and sub-nodes. The main node will see if the answer to the query is yes then it will be sent to that specific node and if it is no then it will be discarded. Similar technique is used to detect fraud. The algorithm will be coded in such a way that for each type of transaction happening in the system will pass through nodes of the tree. If it is found that the access is authorised then user will be given permission to use it but on the other hand if it is identified that the access is unauthorised then it is discarded and transaction will be declined and immediately it should be reported to avoid further attacks.

2. Artificial Neural Networks: - [3]
   This type of technique has three layers. The input is given through first layer which is then transferred to the invisible layer where it is computed as per the algorithms implemented in this layer and then the result is given through the output layer. This is one of the techniques of data mining which can be used for fraud detection. The invisible layer can be programmed in such a way that it can detect any kind of fraud issues and then it can report it through the output layer. If there is unauthorised access then it can be terminated and can be reported for future purpose.

Tools Used for fraud Detection: - [4]

There are variety of fraud detection tools used these days which are intelligent as compared to old methods in order to identify fraud: -

- NetReveal Payments Fraud: - This tool is used to detect fraudster in online payment methods. It uses the concept of machine learning techniques in order to determine the fraud. It gives access to authorised transaction and terminate the unauthorised transaction.
- Fraud.net: - This tool is used where the complexity of the data and information is more and also security risks linked to such complex data are higher. It will implement the concept of data mining, Visual analysis of data etc together to enhance the frauds detection technique.

- SAS Fraud management tool: - This tool is used to detect and prevent the fraud attack even before it happens. It not only keeps a watch on the ongoing payments but also watch the types of users accessing to identify whether it is authorised or unauthorised.

Conclusion: - Hence it is observed that the fraud detection in all fields of the business and organisation is important as it might affect the performance of the overall growth of the business. There are various strategies in which the threat can be prevented even before it happens. In modern business era, the trend of using traditional fraud detection is vanished and most of the big organisations uses latest techniques using artificial intelligence, machine learning etc.

References: -

1.https://www.omnisci.com/technical-glossary/fraud-detection-and-prevention
2.https://www.indellient.com/blog/how-to-build-a-fraud-detection-system/
3.https://www.sciencedirect.com/science/article/pii/S2666285X21000066
4.https://www.bolt.com/thinkshop/15-best-fraud-management-systems-to-stop-fraudulent-chargebacks/