Abstract—In today’s world of e-commerce, credit card payment is the most popular and most important mean of payment due to fast technology. As the usage of credit card has increased the number of fraud transaction is also increasing. Credit card fraud is very serious and growing problem throughout the world. This paper represents the survey of various fraud detection techniques through which fraud can be detected. Although there are serious fraud detection technology exits based on data mining, knowledge discovery but they are not capable to detect the fraud at a time when fraudulent transaction are in progress so two techniques Neural Network and Hidden Markov Model(HMM) are capable to detect the fraudulent transaction is in progress. HMM categorizes card holder profile as low, medium, and high spending on their spending behavior. A set of probability is assigned to each cardholder for amount of transaction. The amount of incoming transaction is matched with cardholder previous transaction, if it is justified a predefined threshold value then a transaction is considered as a legitimate else it is considered as a fraud.

Keywords: credit card, fraud detection, Hidden Markov model.

I. INTRODUCTION
Credit card fraud detection is a fraud committed by using another individual card for their personal reasons without the owner of the card being aware of the fact that card is being used by another individual.

In today’s day to day life of e-commerce has become popular for purchase of goods and services. Due to rapid advancement in the e-commerce credit cards become the most important mean of payment Due to the requirement for greater flexibility and convince technology has given rise to credit card payments. But unfortunately as the usage of credit card is increased rate of fraudulent use of credit card has also increased. Credit card fraud has become serious problem throughout the world. Due to credit card fraud companies and institutes looses a huge amount of money annually.

II. FRAUD TECHNIQUE
There are many ways in which fraudsters commits a credit card fraud either physically or virtually. There are various types of methods as described below.

A. Card Related Fraud
There is various card related fraud as described below

1) Application Fraud
Application fraud occurs in two ways:

a) Assumed Identity
Here the individually illegally obtains another’s individual personal information to open account by his or her name and commit a fraud.

b) Financial Fraud
Here an individual provide false information about his or her financial status to gain more credit than he or she is permitted to.

2) Lost/Stolen Cards
Here an individual loses his card or is stolen by someone else for criminal purpose here the fraudsters get the information of card holder without any help of modern technology. It is the hardest form of credit card fraud to tackle.

3) Account Takeover
The criminal illegally gathers personal information about the valid customers. The criminal or fraudster takeover a legitimate account by providing customer account number and then contacts the card issuer as the genuine card holder and ask card issuer to redirect the mail to a new address.

4) Fake and Counterfeit Cards
Fraudsters are finding more and more innovative ideas to create counterfeit card. Some of the techniques for creating fake and counterfeit cards are mention below:

a) Erasing the magnetic strip
A fraudster will erase the magnetic stripe by using powerful electromagnet and then tampers with the details of the credit card which will match with the valid credit card details which they have acquired illegally.

b) Creating a fake card
Here a fraudster uses a sophisticated machine to create a fake card from the starch. This is one of the common type of fraud done by the fraudster even though it difficult and requires a lot of skills and effort to do.

c) Skimming
It is a process where actually information held either on the magnetic strip or the data stored on the smart chip is electronically copied from one card to another. Skimming is difficult for a cardholder to trace.

d) Altering card details

Survey on Credit Card Fraud Detection Using Different Data Mining Techniques
Twinkle Patel1 Ms. Ompriya Kale2
1M.E. 2Assistant Professor 1,2computer Engineering Department
1,2L J Institute of Engineering and Technology Ahmedabad, Gujarat, India
Here the fraudster alters the cards by using re-embossing or re-encoding them.

B. Merchant Related Fraud

Merchant related frauds are either committed by either merchant or their employees. These types of fraud are described below.

1) Merchant Collision

The merchant’s owner or employee steals the personal information of the cardholder and pass the information to the fraudster. Here the merchant’s owner or employee commits fraud by using customer’s account or personal information.

2) Triangulation

The merchant offers a product in high discounted rates. When a customer likes to buy a product merchant ask the customer to pay after the item is delivered through emails. The merchant use a stolen card number to make the purchase and send the product to customer who sends his valid credit card details through email. The merchant receives these details he goes to purchase other goods using the credit card number of the customer.

C. Internet Related Fraud

Internet has become easy and simple way for fraudsters to commit a fraud. Due to the rapid increase of e-commerce internet related fraud has also increased. There are various techniques of credit card fraud as mention below.

1) Site Cloning

Here the fraudster clones entire site or just a page from where customer place order. Customer feels that they are viewing the real site. The customer handover a credit card detail to the fraudster and then fraudster sends the customer a transaction receipt via email as real site. Thus fraudsters have all detail of customer credit card so they can commit fraud without customer’s awareness.

2) False Merchant Sites

False merchant sites offer a service /goods to the customer in very low rate. The sites request customer to fill the personal information. Most of the sites claims itself to be free but requires credit card number for verification. So they get the credit card detail in this way so that they can raise revenue by creating fraud or sell the details to the fraudster. The site does not charge by themselves for the goods but the larger criminal network use the site to commit a fraud.

a) Credit Card Generator

These are the computer emulation software that creates a valid credit card number and expiry dates. This generator creates a valid credit card highly reliable that it looks as the valid credit card number only and are also available for free download off the internet.

b) Phishing

Here the fraudulent sends email to the customers that appears to be from the websites or company that customer trust ex. Customer bank directs the customer to the fake website. These website looks exactly like the real one i.e. like customer bank’s website and tells customer to provide the bank with personal details like account details or payment card details.

III. LITERATURE REVIEW

I-Cheng Yeh and Che-hui lien et al describes the “The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients” [4]. In this paper they have examines and compares the performance six major classification techniques. They have shown the results of the classification and predictive accuracy of six data mining techniques. The result shows that there are little difference of error rates and big difference of area ratio among six different techniques. ANN performs better and more accurate among five methods.

Siva Parvatni Nelluri, Shaik Nagul, Dr. M.Kishore Kumar et el describes “Credit card fraud detection using Hidden Markov Model (HMM)” [5]. In this paper they have used the transaction amount as the observation symbols and suggested a method for finding the spending profile of card holder with help of which HMM can detect the incoming transaction is fraudulent or not. Results have shown that it has reduced false positive transaction prediction as fraud.

Sam Maes, Karl Tuyls and Bram Vanschoenwinkel et al describe “Credit card fraud detection using Bayesian and neural network” [7]. In this paper they have shown the two fraud detection techniques – Artificial Neural Network and Bayesian Belief Network. They compared two methods and shown that ANN fraud detection process is faster but BBN yields better results of fraud detection and training is shorter. They have given the future work of ANN and BBN that can improve performance.

Anshul Singh and Devesh Narayan et al describes “Survey on hidden markov model for credit card fraud detection” [3]. In this paper they study how the HMM works on human behaviour while doing online behavior they will detect the future transaction is fraud or not. They have brief discussion of HMM in which they have some advantage and simplicity of a HMM.

Raghavendra Patidar and Lokesh Sharma et al describes “Credit card fraud detection using Neural Network” [2]. In this paper they have shown different kind of credit card frauds techniques and they have used neural network for fraud detection but due to some limitation like topology has large impact on their performance of the network as the neurons in hidden layer changes topology changes and there is no optimal topology given so far so they combines the neural network with genetic algorithm (GANN) to detect credit card fraud successfully.

IV. FRAUD DETECTION TECHNIQUES

Data Mining is a process of discovering patterns from large quantities of data so it is one of the powerful tools for decision support system and plays a key role in fraud detection. Various data mining techniques for fraud detection are mentioned below.

A. Logistic Regression

Logistic regression is a special case of linear regression
Logistic Regression is used for predicting the outcome of a dependent variable based on one or more predictor variables. Here predictor variable can be either categorical or numerical.

1) **Advantage**
   It produces a simple probability formula for classification. It works well with linear data for credit card fraud detection.

2) **Disadvantage**
   It does not deal with nonlinear data for credit card fraud detection.

### B. Decision Tree

Decision trees are commonly used in credit card fraud detection. Decision tree is a flow-based structure in which internal nodes represent an outcome of the test on an attribute and branch represents an outcome of the test and leaf node represents classes. Root node is the topmost node of the tree. Decision tree predicts the output of the target variable based on one or more input variables. Decision tree algorithms are ID3, C4.5, CART, MARS.

1) **Advantage**
   It can handle nonlinear and interactive effects of input variables.

2) **Disadvantage**
   It has complex algorithm. Even a small change in observed data might change the structure of a tree. Choosing splitting criteria is also difficult.

### C. K-Nearest Neighbour Algorithm

The concept of k-nearest neighbour can be used in many analogy detection techniques. Credit card fraud can be detected by using k-nearest neighbor algorithm. Here in KNN new transaction is classified based on the closeness i.e. distance. In KNN we classify any new incoming transaction by calculating closeness or distance to other transaction. If they are close then transaction is ok else the transaction is indicated as fraud.

1) **Advantage**
   It does not require establishing any predictive model before classification.

2) **Disadvantage**
   Accuracy is highly dependent on the measure of distance.

### D. Naïve Bayes Algorithm

Naïve Bayes classifier makes a conditional independence assumption that the effect of an attribute value of a given class is independent of other attributes. It is based on Bayes’ theorem.

1) **Advantage**
   It only provides a theoretical justification to the fact but does not use Bayes’ theorem.

2) **Disadvantage**
   In real practice the dependences exists between the variable.

### E. Artificial Neural Network

Although there are several fraud detection techniques based on knowledge detection, expert system, data mining etc. but still they are not capable to detect the fraud at the time when fraudulent transaction is in progress but with the help of techniques like Neural Network, Hidden Markov Model the fraudulent transaction can be detected during the transaction is in progress.

- **Advantage**
  - It detects the fraudulent transaction at the time when transaction is in progress.

- **Disadvantage**
  - Number of parameters to be set before training begins. There are no clear rules to set these parameters.
  - Network differ in the way their neurons are interconnected i.e. topology of a network has a large influence on the performance of network and so far there is no method that determine optimal topology for a given problem.

### F. Hidden Markov Model

Hidden markov model is a statistical model with a finite set of states, each of which is linked with a probability distribution. Transaction among these states is done by a set of probability known as transition probability. In particular state outcome can be generated according to the associated symbol of observation of probability distribution. It is only the outcome. In hidden markov model, the state is not directly visible hence it is name hidden markov model. The main advantage of using HMM based model is reducing in false positive (FP) transaction predict as fraud even though they are genuine customer. HMM consider three main prices values (i) low (l) (ii) medium (m) (iii) high (h). For example let l= (0, $50), m= ($50, $100), h= ($100, credit card limit). If transaction of cardholder is $60, then observation symbol is m.
Implementation technique used in HMM is creating cluster of training sets so it can identify spending profile of cardholder. The item purchase by cardholder as states for model and transition from one state to another is determined by probability distribution. It requires at least 10 previous transaction on basis of which it determine incoming transaction is fraud or genuine. HMM model have two stages in first stage training of system is done and in second stage detection of fraud is done based on expected range of amount of transaction. In case of fraud an alarm is generated and transaction is terminated or it is considered genuine.

V. CONCLUSION

In this survey paper various fraud techniques and various approaches of credit card fraud detection techniques has been overviewed. There is also a brief discussion about artificial neural network and hidden markov model fraud detection techniques. From this survey paper we can conclude that by using hidden markov model there is a reduction in false positive (FP) transaction predict as fraud even though they are genuine. HMM results in better fraud detection techniques among other techniques.

REFERENCES


[7] Sam Maes, Karl Tuyls and Bram Vanschoenwinkel ,“Credit card fraud detection using Bayesian and neural network”
