##### A Project report on

**CASHLESS SOCIETY MANAGING PRIVACY AND SECURITY IN TECHNOLOGICAL AGE**

###### A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree.

###### **Bachelor of Technology**

**in**

**Computer Science and Engineering**

Submitted by

1. Madhuri

(19H51A0525)

1. Sree

(19H51A0556)

S. Abhinav

(19H51A0557)

Under the esteemed guidance of

Mr. A. Vivekanand

(Associate Professor)



**Department of Computer Science and Engineering**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

(An Autonomous Institution under UGC & JNTUH, Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA.)

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD - 501401.

#### 2019- 2023

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



#### CERTIFICATE

This is to certify that the Major Project Phase-1 report entitled **"cashless society managing privacy and security in technological age"** being submitted by S.Madhuri (19H51A0525), S.Sree (19H51A0556), S.Abhinav (19H51A0557) in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out his/her under my guidance and supervision.

###### The results embodies in this project report have not been submitted to any other University or Institute for the award of any Degree.

**Mr.A.Vivekanand Dr. Siva Skandha Sanagala**

**Associate Professor Associate Professor and HOD**

**Dept. of CSE Dept. of CSE**

#### ACKNOWLEDGEMENT

With great pleasure we want to take this opportunity to express my heartfelt gratitude to all the people who helped in making this project work a grand success.

We are grateful to **Mr.A.Vivekanand, Associate Professor,** Department of Computer Science and Engineering for his valuable technical suggestions and guidance during the execution of this project work.

We would like to thank **Dr. Siva Skandha Sanagala,** Head of the Department of Computer Science and Engineering, CMR College of Engineering and Technology, who is the major driving forces to complete my project work successfully.

We are very grateful to **Dr. Vijaya Kumar Koppula**, Dean-Academic, CMR College of Engineering and Technology, for his constant support and motivation in carrying out the project work successfully.

We are highly indebted to **Dr. V A Narayana,** Principal, CMR College of Engineering and Technology, for giving permission to carry out this project in a successful and fruitful way.

We would like to thank the Teaching & Non- teaching staff of Department of Computer Science and Engineering for their co-operation

We express our sincere thanks to **Mr. Ch. Gopal Reddy**, Secretary, CMR Group of Institutions, for his continuous care.

Finally, We extend thanks to our parents who stood behind us at different stages of this Project. We sincerely acknowledge and thank all those who gave support directly and indirectly in completion of this project work.

S.Madhuri 19H51A0525

S.Sree 19H51A0555

S.Abhinav 19H51A0557

**TABLE OF CONTENTS**

**CHAPTER**

**NO. TITLE PAGE NO.**

LIST OF FIGURES ii

LIST OF TABLES iii

ABSTRACT iv

**1** **INTRODUCTION** 1

1.1 Problem Statement 2

1.2 Research Objective 2

1.3 Project Scope and Limitations 3

**2** **BACKGROUND WORK** 4

2.1. Detection of Credit card fraud using K-NN Algorithm 4

2.1.1. Introduction 4

2.1.2. Merits, Demerits, and Challenges 6

2.1.3. Implementation of Detection of Credit card fraud

using K-NN Algorithm 9

2.2. Detection of Credit card fraud using Naive Bayes 12

2.2.1. Introduction 12

2.2.2. Merits, Demerits, and Challenges 14

2.2.3. Implementation of Detection of Credit card fraud

using Naive Bayes 16

2.3. Detection of Credit card fraud using Logistic Regression 19

2.3.1. Introduction 19

2.3.2. Merits, Demerits, and Challenges 22

2.3.3. Implementation of Detection of Credit card fraud

using Logistic Regression 24

**3 RESULTS AND DISCUSSION** 28 3.1. Comparison of Existing Solutions 28

3.2. Data Collection and Performance metrics 31

**4** **CONCLUSION** 32

6.1 Conclusion 32

**5** **REFERENCES** 33

**List of Figures**

**FIGURE**

**NO. TITLE PAGE NO.**

1.2 <Figure Name> 21

2.2 <Figure Name> 28

3.1 <Figure Name> 32

**List of Tables**

**FIGURE**

**NO. TITLE PAGE NO.**

3.1 <Figure Name> . 21

3.3 <Figure Name> 28

3.4.2 <Figure Name> 32

# **ABSTRACT**

A cashless society is an economic state which handles financial transactions not in the form of traditional mediums of currency, such as cash or coins, but by transferring digital data (usually by electronic means, such as credit cards and mobile data) between participating parties. Participants of a cashless society must figure out a way to protect their transaction data, acknowledging the risks of organizations collecting mass amounts of said data, which result in a reduction of personal privacy. Balancing individual privacy with data security is vital in the information age, especially considering the increased risk of data breaches and exploitation. In order to increase privacy in a cashless society, a few courses of action can be combined to produce a lasting and desirable result for users: A new kind of banking service that assigns randomized numbers to credit cards and a campaign to educate and inform key stakeholders about security and privacy risks to provide the necessary tools and background knowledge to safeguard their own information before interaction with a foreign entity or other third parties Card number randomization is susceptible to zero-day errors, bugs, and varying levels of social acceptance. This preliminary research draws on a systems analysis of cashless systems to identify and analyze a set of social and technical solutions to support a robust cashless system that protects users’ privacy and maintains the security of the system. The information found and analyzed will be beneficial by exposing weak points in current methods of data integrity and security. Learning about current and future methods of managing privacy and data security in the technological age would be helpful in creating preventative countermeasures. This study provides critical steps to prevent the loss of personal privacy in a cashless system.

**CHAPTER 1**

**INTRODUCTION**

**INTRODUCTION**

As the economic system has been growing enormously the tasks related to the economy have also been expanding and up surging. Due to the increase in these tasks, it has become more hectic to maintain the data and provide service efficiently. In traditional money transaction methods, there is an increase in crime rates with tangible money to steal, money laundering, and difficulty in storing and depositing paper money. A cashless society has been developed to overcome the limitations of the traditional system. In the traditional medium, financial transactions are made using currency, cash, or coins. But cashless society uses digital or virtual platforms to make transactions. Participants of a cashless society must figure out a way to protect their transaction data, acknowledging the risks of organizations collecting mass amounts of said data, which result in a reduction of personal privacy. Balancing individual privacy with data security is vital in the information age, especially considering the increased risk of data breaches and exploitation.

Financial fraud is an activity where someone willfully impersonates a legal customer of a bank and uses his/her credit card, debit card, or credit account to make a big purchase or payment. Financial fraud can happen in several ways like stealing of financial ***card***, stealing sensitive data for instance personal identification number (PIN), credit number (card#), card verification value (CVV) number, etc. And then use stolen information to make a big purchase or payment before the cardholder ascertains. As per the annual report published by the MEIT, Govt. of India, the digital transitions in India have registered a growth of 51% in the 2018–19 financial year.

In spite of the 51% growth in digital transactions in India, their safety remains a concern as fraudulent activities have increased severalfold, with around 52,304 cases of credit/debit card fraud reported in FY’19 alone. Due to this sharp increase in banking fraud, it is highly imperative to detect these fraudulent transactions in order to help consumers as well as banks, who are losing several hundred crores of rupees due to fraudulent transactions. As per the report given by the Federal Trade Commission, Consumer Information (FTC), USA, it is next to impossible to completely avoid fraud. Fraudulent transactions occur very rarely (almost one in ten thousand) is, therefore, very cumbersome to identify fraudulent transactions from several millions of legitimate transactions.

**1.1. Problem Statement**

Digital transactions are where money lending, borrowing, depositing, and withdrawing can be done on the internet. In the information age, due to the increased risk of data breaches and exploitation, it is vital to balance individual privacy with data security. The data stored to perform digital transactions are being disclosed to third parties or hackers. To overcome these issues in our project we have introduced a security mechanism that is using a randomized credit card system that will help prevent unwanted parties from collecting sensitive and personal information about people.

**1.2. Research Objective**

The main objective of this project is to create a cashless society where there is an increase in the ease of conducting online transactions, eliminate several business risks (robbery of cash), reduce the risk of handling cash, reduce the cost of production of paper currency, and coins, and increase transparency among transactions among people by balancing both individual privacy with data security. Our research objective is to find the idea about the emerging cashless society, the background of cashless transactions, and the privacy and security concerns of the cashless society. Through our research, we are able to figure out that the cashless society poses risks for its member’s data as all of their transactions will be tracked online.

**1.3.** **Project Scope And Limitation**

* The Cashless Society will increase employment, and reduce risks related to cash like corruption, robbery, and carrying large amounts of cash, helping people to transfer the money with security and safety at high speed.
* If one reduces the use of cash, the compliance level in various things gets better. For example, better recognition of economic activities, more efficient collection of tax, etc. The GDP can get positively impacted by 0.5-0.6% due to digitization.
* Going cashless can also influence people’s propensity to save in fact, studies have shown that plastic money induces people to overspend.
* Transitioning to a cashless economy also has the burden of financial exclusion due to a lack of digital literacy, especially in the case of the poor and elderly.

**CHAPTER 2**

**BACKGROUND WORK**

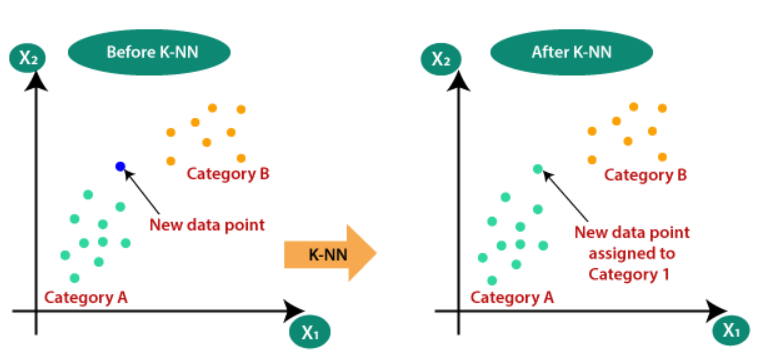
**BACKGROUND WORK**

**2.1. Credit card fraud detection using K-NN Algorithm**

**2.1.1. Introduction: -**

K-Nearest Neighbor is one of the simplest Machine Learning algorithms based on the Supervised Learning technique. K-NN algorithm assumes the similarity between the new case/data and available cases and put the new case into the category that is most similar to the available categories. K-NN algorithm stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a good suite category by using K- NN algorithm. K-NN algorithm can be used for Regression as well as for Classification but mostly it is used for Classification problems.

K-NN is a **non-parametric algorithm**, which means it does not make any assumption on underlying data. It is also called a **lazy learner algorithm** because it does not learn from the training set immediately instead it stores the data set and at the time of classification, it performs an action on the data set. KNN algorithm at the training phase just stores the dataset and when it gets new data, then it classifies that data into a category that is much similar to the new data.



*Fig 1: KNN Classification*

The KNN algorithm can compete with the most accurate models because it makes highly accurate predictions. Therefore, you can use the KNN algorithm for applications that require high accuracy but that do not require a human-readable model. The quality of the predictions depends on the distance measure. Therefore, the KNN algorithm is suitable for applications for which sufficient domain knowledge is available. This knowledge supports the selection of an appropriate measure.

**2.1.2. Merits, Demerits, and Challenges: -**

* It is simple to implement.
* It is robust to the noisy training data
* It can be more effective if the training data is large.
* Always needs to determine the value of K which may be complex sometimes.
* The computation cost is high because of calculating the distance between the data points for all the training samples.
* This model doesn’t provide solutions for preventing fraud.

**2.1.3. Implementation: -**

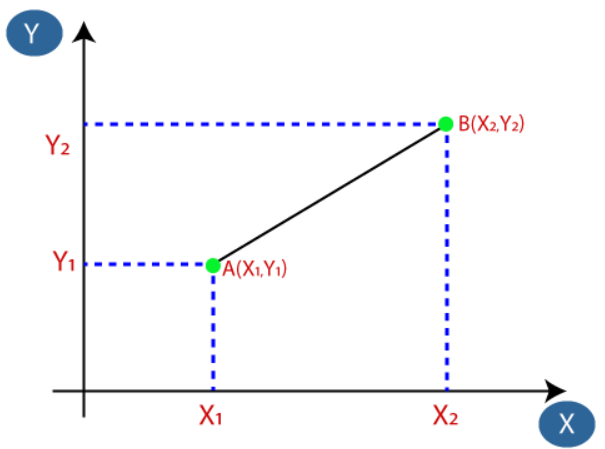
The K-NN working can be explained on the basis of the below algorithm:

* **Step 1:** Select the number K of the neighbors
* **Step 2:** Calculate the Euclidean distance of **K number of neighbors**
* **Step 3:** Take the K nearest neighbors as per the calculated Euclidean distance.
* **Step 4:** Among these k neighbors, count the number of the data points in each category.
* **Step 5:** Assign the new data points to that category for which the number of neighbors is maximum.
* **Step 6:** Our model is ready.

Firstly, we will choose the number of neighbors, so we will choose the k=5. Next, we will calculate the **Euclidean distance** between the data points. The Euclidean distance is the distance between two points, which we have already studied in geometry. It can be calculated as:

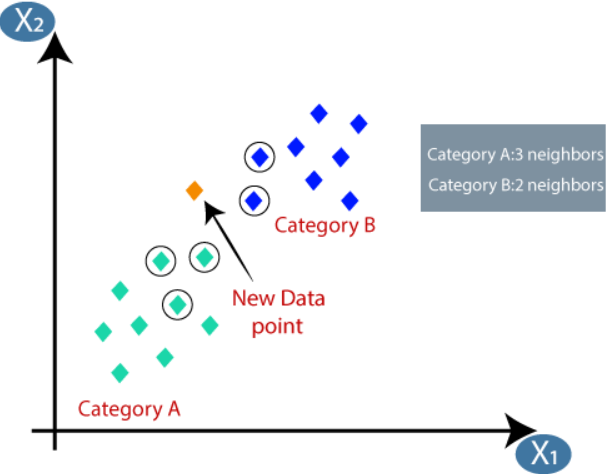


Suppose we have a new data point and we need to put it in the required category. Consider the Fig 2:



*Fig 2: Calculating K-Nearest Neighbors using Euclidean Distance*

By calculating the Euclidean distance, we got the nearest neighbors, as three nearest neighbors in category A and two nearest neighbors in category B. Consider Fig 3:



*Fig 3: Categorising New Data Point*

PCA (Principal Component Analysis) is mainly used to reduce the feature space size while retaining as much information as possible. Here, all the features are transformed into 2 features using PCA.

K-Nearest Neighbors Scores Average Accuracy --> 0.964467005076142

**Performance Metrics: -**

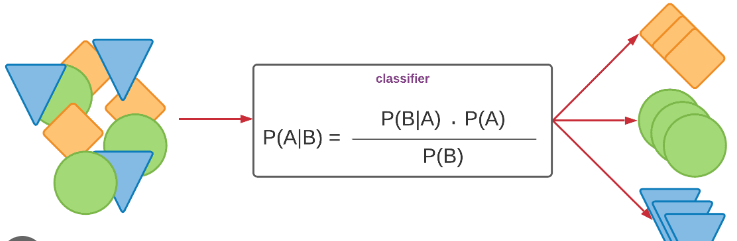
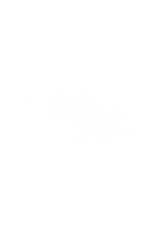
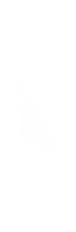
**2.2. Detection of Credit card fraud using Naive Bayes:**

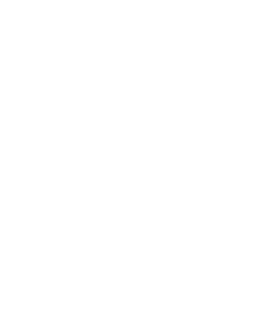
**2.2.1. Introduction: -**

The Naïve Bayes algorithm is a supervised learning algorithm, which is based on **Bayes theorem** and used for solving classification problems. It is mainly used in text classification that includes a high-dimensional training dataset. Naïve Bayes Classifier is one of the simple and most effective Classification algorithms which helps in building the fast machine learning models that can make quick predictions. **It is a probabilistic classifier, which means it predicts on the basis of the probability of an object**. Some popular examples of Naïve Bayes Algorithm are **Spam filtration, Sentimental analysis, and classifying articles**. The Naïve Bayes algorithm is comprised of two words Naïve and Bayes, which can be described as: -

* **Naïve**: It is called Naïve because it assumes that the occurrence of a certain feature is independent of the occurrence of other features. Such as if the fruit is identified on the bases of color, shape, and taste, then red, spherical, and sweet fruit is recognized as an apple. Hence each feature individually contributes to identify that it is an apple without depending on each other.
* **Bayes**: It is called Bayes because it depends on the principle of [Bayes' Theorem](https://www.javatpoint.com/bayes-theorem-in-artifical-intelligence).Bayes' theorem is also known as **Bayes' Rule** or **Bayes' law**, which is used to determine the probability of a hypothesis with prior knowledge. It depends on the conditional probability.

There are three types of Naïve Bayes Model, which are given below:

1. **Gaussian**: The Gaussian model assumes that features follow a normal distribution.
2. **Multinomial**: The Multinomial Naïve Bayes classifier is used when the data is multinomial distributed.
3. **Bernoulli**: The Bernoulli classifier works similar to the Multinomial classifier, but the predictor variables are the independent Booleans variables. Such as if a particular word is present or not in a document. This model is also famous for document classification tasks.



*Fig 4: Naïve Bayes Classifier*

**2.2.2. Merits, Demerits, and Challenges: -**

* Naïve Bayes is one of the fast and easy ML algorithms to predict a class of datasets.
* It can be used for Binary as well as Multi-class Classifications.
* It performs well in multi-class predictions as compared to the other Algorithms.
* It is the most popular choice for **text classification problems**.
* Naïve Bayes assumes that all features are independent or unrelated, so it cannot learn the relationship between features sometimes credit card details can be related to each other.
* This model doesn’t provide solutions for preventing fraud.

**2.2.3. Implementation: -**

Bayes' theorem is also known as **Bayes' Rule** or **Bayes' law**, which is used to determine the probability of a hypothesis with prior knowledge. It depends on the conditional probability. The formula for Bayes' theorem is given as:

IMG_256

**Where,**

**P(A|B) is Posterior probability**: Probability of hypothesis A on the observed event B.

**P(B|A) is Likelihood probability**: Probability of the evidence given that the

probability of a hypothesis is true.

**P(A) is Prior Probability:** Probability of hypothesis before observing the evidence.

**P(B) is Marginal Probability:** Probability of Evidence.

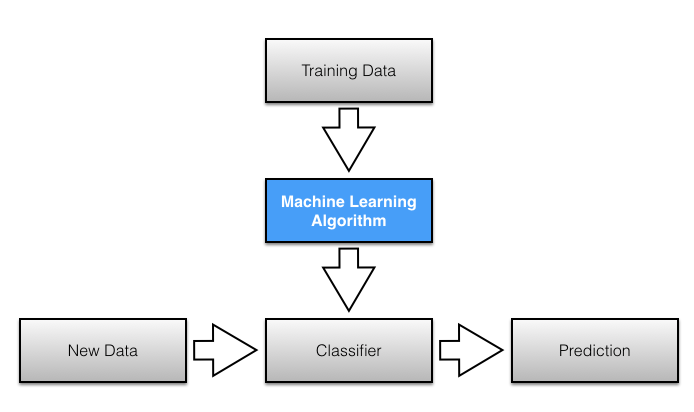
The Naïve Bayes working can be explained on the basis of the below algorithm:

**STEP 1:** Convert the given dataset into frequency tables.

**STEP 2:** Generate a Likelihood table by finding the probabilities of given features.

**STEP 3:** Now, use the Bayes theorem to calculate the posterior probability.

Gaussian Naive Bayes:

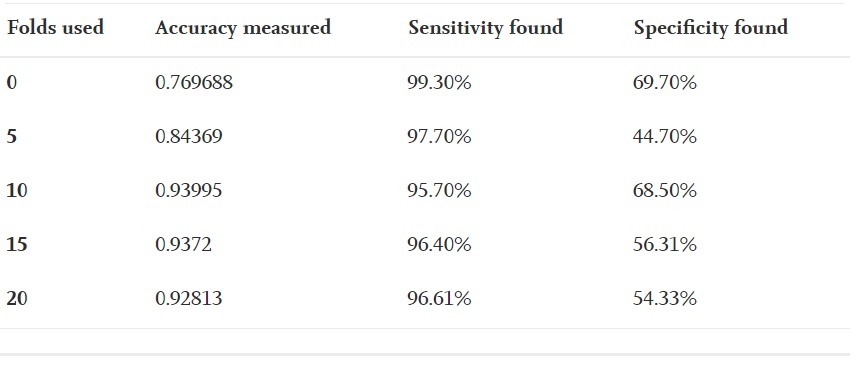
Real-valued attributes are estimated by assuming a Gaussian distribution. Easiest to work with, only need mean and std from training data and calculate mean and std of input values(X) for each class to summarize the distr.

*Fig 5:*

In credit card transactions interesting to note "all transaction amounts > 10K in Genuine Class only". Also, this amount feature is not on the same scale as the principle components. So, we'll standardize the values of the 'Amount' feature using StandardScalar and save them in the data frame for later use.

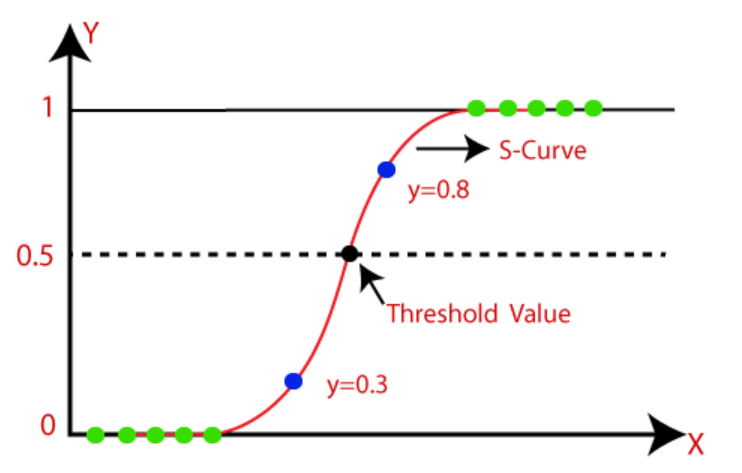
The "Time" feature shows that the rate of transactions is picking up during day time. But the number of transactions has almost similar dependence on the time of the day for both the classes. So, we believe this feature does not yield any predictive power to distinguish between the two classes. But of course, I will later test this assumption. For now, keep this feature in the data frame. We will drop "Time" but keep "Time\_Hr".

**Performance Metrics: -**



**2.3 Detection of Credit card fraud using logistic regression**

**2.3.1.** **Introduction: -**

Logistic regression is one of the most popular Machine Learning algorithms, which comes under the Supervised Learning technique. It is used for predicting the categorical dependent variable using a given set of independent variables. Logistic regression predicts the output of a categorical dependent variable. Therefore, the outcome must be a categorical or discrete value. It can be either Yes or No, 0 or 1, true or False, etc. but instead of giving the exact value as 0 and 1, **it gives the probabilistic values which lie between 0 and 1.**

*Fig 5: Logistic Regression Curve*

In Logistic regression, instead of fitting a regression line, we fit an "S" shaped logistic function, which predicts two maximum values (0 or 1). The curve from the logistic function indicates the likelihood of something such as whether the cells are cancerous or not, whether a mouse is obese or not based on its weight, etc. Logistic Regression is a significant machine learning algorithm because it has the ability to provide probabilities and classify new data using continuous and discrete datasets. On the basis of the categories, Logistic Regression can be classified into three types:

* **Binomial:** In binomial Logistic regression, there can be only two possible types of dependent variables, such as 0 or 1, Pass or Fail, etc.
* **Multinomial:** In multinomial Logistic regression, there can be 3 or more possible unordered types of the dependent variable, such as "cat", "dogs", or "sheep".
* **Ordinal:** In ordinal Logistic regression, there can be 3 or more possible ordered types of dependent variables, such as "low", "Medium", or "High".

**2.3.2. Merits, Demerits, and Challenges: -**

* In a **low-dimensional dataset** having a sufficient number of training examples, logistic regression is **less prone to over-fitting**.
* Logistic Regression **requires a large dataset** and also sufficient training examples for all the categories it needs to identify
* This model doesn’t provide solutions for preventing fraud.
* Accuracy in a highly unbalanced data set does not represent a correct value for the efficiency of a model. Initially, a method should be applied to balance the data before taking into account any performance evaluation metrics.

**2.3.3. Implementation: -**

The Logistic regression equation can be obtained from the Linear Regression equation. The mathematical steps to get Logistic Regression equations are given below:

IMG_256We know the equation of the straight line can be written as:

In Logistic Regression y can be between 0 and 1 only, so for this let's divide the above equation by (1-y):

IMG_257

But we need range between -[infinity] to +[infinity], then take logarithm of the equation it will become:

IMG_258

The above equation is the final equation for Logistic Regression.

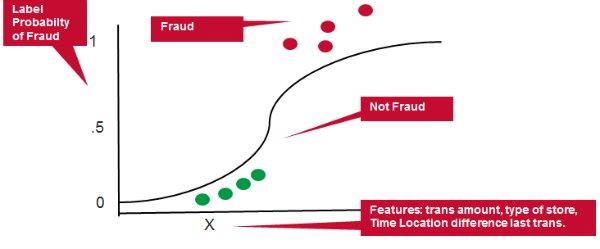
In this model the dataset used, contains transactions carried out by European credit card holders that took place over two days in September 2013, and is available on kaggle at <https://www.kaggle.com/mlg-ulb/creditcardfraud/version/3>.

It is a very unbalanced data set, that is, it has 492 fraud transactions, which represents only 0.172% of the 284,807 transactions.

The input variables are numeric, the result of a PCA transformation. Due to confidentiality issues, the original data and other complementary information were not made available.

The only variables that have not been transformed with the PCA are 'Time' and 'Value'. The variable 'Time' contains the seconds between each transaction and the first transaction in the data set. The 'Amount' variable refers to the amount of the transaction.

The 'Class' variable is the response variable (Target) and has a value "1" in case of fraud and "0" otherwise.



**Performance Metrics:-**

With the Logistic Regression Model, we have:

85290 transactions classified as normal and were actually normal;

18 transactions classified as fraud but that were really normal (type 1 error);

61 transactions classified as normal but which were fraud (type 2 error);

74 transactions classified as fraud and were actually fraud.

Thus, although the accuracy was excellent, the algorithm wrongly classified about 4 out of 10 fraudulent transactions.Accuracy in a highly unbalanced data set does not represent a correct value for the efficiency of a model.



**2.4 Credit card fraud detection using decision tree**

**2.4.1 Introduction:-**

Decision Tree is a **Supervised learning technique**that can be used for both classification and Regression problems, but mostly it is preferred for solving Classification problems**.**In a Decision tree, there are two nodes, which are the **Decision Node** and**Leaf Node.** Decision nodes are used to make any decision and have multiple branches, whereas Leaf nodes are the output of those decisions and do not contain any further branches.The decisions or the test are performed on the basis of features of the given dataset.

It is a graphical representation for getting all the possible solutions to a problem/decision based on given conditions.It is called a decision tree because, similar to a tree, it starts with the root node, which expands on further branches and constructs a tree-like structure.In order to build a tree, we use the **CART algorithm,** which stands for **Classification and Regression Tree algorithm.**A decision tree simply asks a question, and based on the answer (Yes/No), it further split the tree into sub trees.

## Decision Tree Terminologies

**. Root Node:** Root node is from where the decision tree starts. It represents the entire dataset, which further gets divided into two or more homogeneous sets.

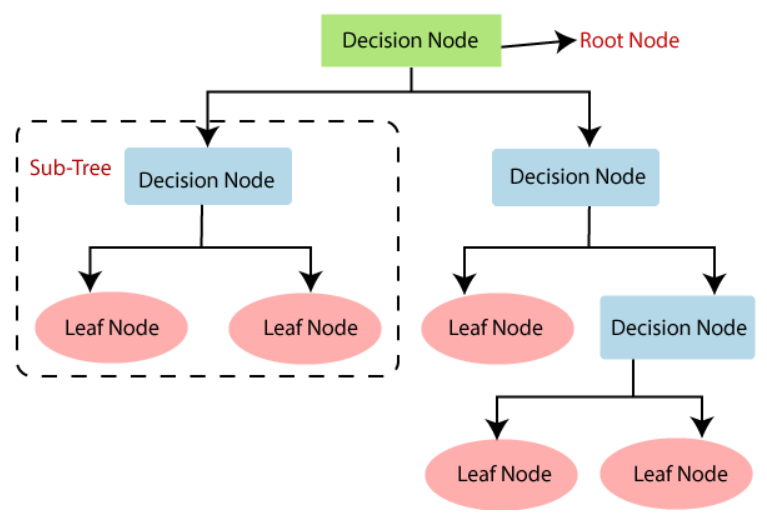
· **Leaf Node:** Leaf nodes are the final output node, and the tree cannot be segregated further after getting a leaf node.

· **Splitting:** Splitting is the process of dividing the decision node/root node into sub-nodes according to the given conditions.

· **Branch/Sub Tree:** A tree formed by splitting the tree.

· **Pruning:** Pruning is the process of removing the unwanted branches from the tree.

· **Parent/Child node:** The root node of the tree is called the parent node, and other nodes are called the child nodes.



**2.4.2. Merits,Demerits and Challenges :-**

* It is simple to understand as it follows the same process which a human follow while making any decision in real-life.
* There is less requirement of data cleaning compared to other algorithms.
* The decision tree contains lots of layers, which makes it complex.
* It may have an overfitting issue, which can be resolved using the **Random Forest algorithm.**
* For more class labels, the computational complexity of the decision tree may increase.
* This model doesn’t provide solutions for preventing fraud.

**2.4.3. Implementation:-**

In a decision tree, for predicting the class of the given dataset, the algorithm starts from the root node of the tree. This algorithm compares the values of root attribute with the record (real dataset) attribute and, based on the comparison, follows the branch and jumps to the next node.

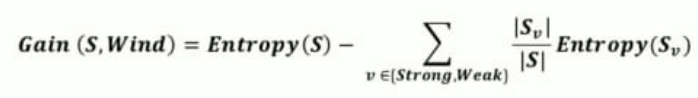
* **Step-1:** Begin the tree with the root node, says S, which contains the complete dataset.
* **Step-2:** Find the best attribute in the dataset using **Attribute Selection Measure (ASM).**
* **Step-3:** Divide the S into subsets that contains possible values for the best attributes.
* **Step-4:** Generate the decision tree node, which contains the best attribute.
* **Step-5:** Recursively make new decision trees using the subsets of the dataset created in Continue this process until a stage is reached where you cannot further classify the nodes and called the final node as a leaf node.

There are two popular techniques for ASM, which are:

* **Information Gain**
* **Gini Index**

Information gain is the measurement of changes in entropy after the segmentation of a dataset based on an attribute.

* It calculates how much information a feature provides us about a class.
* According to the value of information gain, we split the node and build the decision tree.
* A decision tree algorithm always tries to maximize the value of information gain, and a node/attribute having the highest information gain is split first. It can be calculated using the below formula:

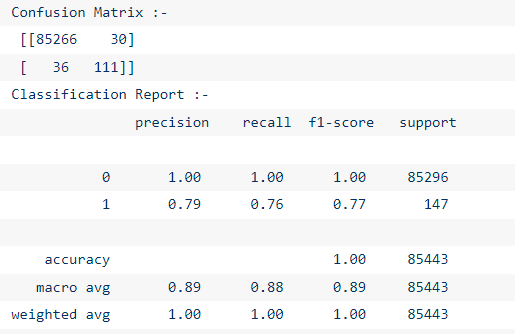


**Entropy(S) -** Entropy can be defined as **a measure of the purity of the sub split**. Entropy always lies between 0 to 1. The entropy of any split can be calculated by this formula

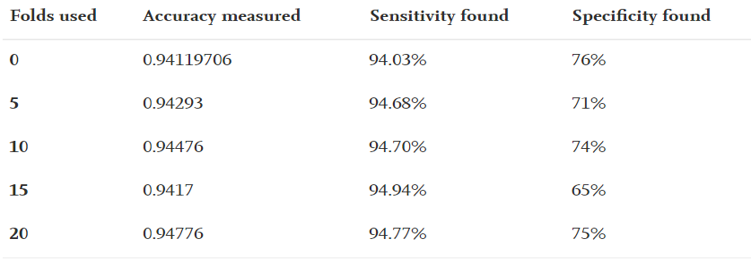
**ΔS = -(m/n)\*log(m/n)**

Information gain is always inversely proportional to entropy, more the entropy less the information gain and vice versa. The Algorithm works effectively if the value of entropy is less and information gain in high.

**Performance Metrics:-**



Sensitivity is a measure of how well a machine learning model can detect positive instances. It is also known as the true positive rate (TPR) .Specificcity is a measure of how well a machine learning model can detect negative instances. It is also known as the true positive rate (TNR) .**The sum of sensitivity (true positive rate) and false negative rate would be 1.**



**CHAPTER 3**

**RESULTS AND DISCUSSION**

**RESULTS AND DISCUSSION**

|  |  |
| --- | --- |
| **METHOD** | **ACCURACY** |
| Logistic Regression | 78.83 |
| Decision Tree | 72.66 |
| K-NN | 72.5 |
| Naïve Bayes | 75.83 |
| Random Forest | 80.61 |

CHAPTER 4

**CONCLUSION**

**CHAPTER 4**

**CONCLUSION**

**CHAPTER 5**

**REFERENCES**

**CHAPTER 5**

## REFERENCES

1. T.Baranidharan,S.Karthik,T.Sumathi, “ Modelling of F3I based feature selection approach for PCOS classification and prediction”, Journal of Ambient Intelligence and Humanized Computing, ISSN 1868-5137, J Ambient Intell Human Comput(Springer) ,DOI 10.1007/s12652-020-02199-1,January 2020.
2. Xiaowei Tang, Fang li,V. Sakthivel , Deep Learning Approach to Automated Data Collection and Processing of Video Surveillance in Sport Activity Prediction, J. of Mult.-Valued Logic & Soft Computing, Vol. 36, pp. 61–82, 2021.

SAMPLE REFERENCES

1. Dr.Vikas Jain, Dr.G. Nalinipriya, Binny. S, Dr.M.Maragatharajan, ‘Brain Computer Interface System using Deep Convolutional Machine Learning Method’ , European Journal of Molecular & Clinical Medicine, ISSN 2515-8260 Volume 07, Issue 02, 2020.
2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9137953/
3. https://www.ibm.com/blockchain/resources/transparent-supply/pharma/
4. https://www.leewayhertz.com/blockchain-in-pharma-supply-chain/

## 