CREDIT CARD FRAUD DETECTION USING DECISION TREE FOR TRACING EMAIL AND IP

Dr R.DHANAPAL[1] , GAYATHIRI.P[2]

[1]Professor and Head
Research Department of Computer Applications,
Eswari Engineering College, Chennai-600089

[2]Asst. Professor
Research Scholar in Manonmaniam Sundaranar University
Department of Computer Science,
Kanchi Sri Krishna College, Kanchipuram

Abstract

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Transactions completed with credit cards seem to become more and more popular with the introduction of online shopping and banking. Correspondingly, the number of credit card frauds has also increased .Currently; data mining is a popular way to combat frauds because of its effectiveness. Data mining is a well-defined procedure that takes data as input and produces output in the forms of models or patterns. In other words, the task of data mining is to analyze a massive amount of data and to extract some usable information that we can interpret for future uses. Frauds has also increased .Currently, data mining is a popular way to combat frauds because of its effectiveness. Data mining is a well-defined procedure that takes data as input and produces output in the forms of models or patterns. In other words, the task of data mining is to analyze a massive amount of data and to extract some usable information that we can interpret for future uses.

Keywords:*DecisionTree,Entropy,Gini,Hunt's Algorithm, Online Frauds, Tracing Email, Tracing IP.*

I. Introduction

Most online merchants who accept credit card payments sooner or later have to deal with the so-called carders who steal credit card information to pay for orders in online stores. This kind of illegal activity is called credit card fraud. Carders prefer "buying" goods that are delivered immediately, before their transaction is rejected. For this reason carders are mostly interested in getting access to digital items that are usually automatically delivered online. Detecting credit card fraud is not very difficult. We are talking here about manual processing of credit card payments when a merchant/customer verifies the transaction should be Legal or Fraud.Weverifythe credit cardtransaction to the following parameters of the transaction and customer contact details.

2. Types of Frauds

2.1 Offline Fraud

Most offline fraud incidences happen as a result of theft of mail, sensitive information related to customers bank or credit card accounts, stolen ATM/debit/credit cards, forged/ stolen cheque etc. customer can protect from such instances by exercising caution while receiving, storing and disposing customer account statements as well as Cheque, ATM/Debit and Credit Cards.

2.2 Online Fraud

Online fraud occurs when someone poses as a legitimate company (that may or may not be in order to obtain sensitive personal data and illegally conducts transactions on your existing accounts. Oftencalled "phishing" (An online identity theft scam. Typically, criminals send emails that look like they're from legitimate sources, but are not. The fake messages generally include a link to phony, or spoofed, websites, where victims are asked to provide sensitive personal information. The information goes to criminals, rather than the legitimate business.) Or "spoofing" (An online identity theft scam. Typically, criminals send emails that look like they're from legitimate sources, but are not (phishing). The fake messages generally include a link to phony, or spoofed, websites, where victims are asked to provide sensitive personal information. The information goes to criminals, rather than the legitimate business.) , the most current methods of online fraud are usually through fake emails, Web sites and pop-up windows, or any combination of such methods. The main objective of both offline as well as online fraud is to steal your 'identity'. This phenomenon is commonly known as "identity theft". Identity theft (A criminal activity where a thief appropriates vital information such as your name, birth date, account number, or credit card number without your knowledge) occurs when someone illegally obtains your personal information — such as your credit card number, bank account number, or other identification and uses it repeatedly to open new accounts or to initiate transactions in your name. Identity theft can happen even to those who do not shop, communicate, or transact online. A majority of identity theft occurs offline. Stealing wallets and purses, intercepting or rerouting your mail, and rummaging through your trash are some of the common tactics that thieves can use to obtain personal information.

3. Types of Internet Fraud

3.1 Phishing Emails

Every user of the Internet should be aware about the common attempts of fraud through means like 'phishing' or 'spoofing'. 'Phishing' is an attempt by fraudsters to 'fish' for banking details. 'Phishing' attempts usually appear in the form of an email appearing to be from bank. Within the email Customer are then usually encouraged to click a link to a fraudulent log on page designed to capture your details. Email addresses can be obtained from publicly available sources or through randomly generated lists. Therefore, if you receive a fake email that appears to be from Bank, this does not mean that your email address, name, or any other information has been taken from the bank. Although they can be difficult to spot, 'phishing' emails generally Customer to click on a link which takes you back to a spoof web site that looks similar to bank's website, wherein Customer asked to provide, update or confirm sensitive personal information. To prompt you into action, such emails may signify a sense of urgency or threatening condition concerning Customeraccount. Some fake emails may also contain a virus known as a "Trojan horse" that can record Customer keystrokes or could trigger background installations of key logging software or viruses onto computer. The virus may live in an attachment or be accessed via a link in the email. Never respond to emails, open attachments, or click on links from suspicious or unknown senders. If Customer not sure if a email sent by Bank is legitimate, Report it to Bank, without replying to the email.

3.2 Counterfeit Websites

Online thieves often direct Customer/Merchant to fraudulent Web sites via email and pop-up windows and try to collect personal information. One way to detect a phony Web site is to consider how Customer/Merchant arrived there. Generally, Customer/Merchant may have been directed by a link in a fake email requesting account information. However, if Customer/Merchant can type, or cut and paste, the URL into a new Web browser window and it does not take Customer/Merchant to a legitimate Web site, or Customer/Merchantget an error message, it was probably just a cover for a fake Web site. Much more dangerous to the average Internet user is the electronic duping version of fraud. Phishing has gained a lot of media attention due to very effective emails asking a reader to click on a link and submit sensitive data, usually a social security number or bank account. These fake emails are usually written to look like they came from an official source, so reader doesn't think it's a trap. Pharming, similar to phishing, requires a reader to read or activate a web page. The scam works by using a valid website and redirecting the traffic to a bad one. Unlike phishing, which is usually sent on an email, pharming traps can be embedded into a web page, download or data stream like a movie file.

4. General Types of frauds

4.1 types of Fraud

Figure 1 Types of Fraud Statistical Report for Year 2012.

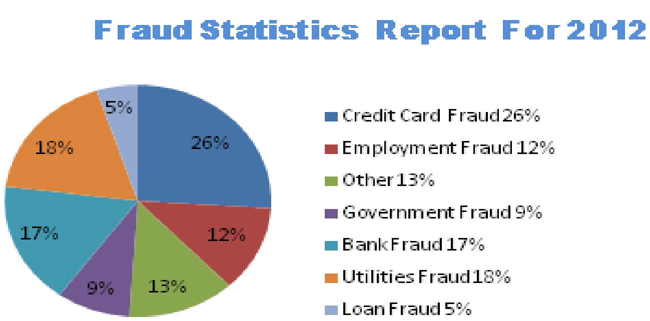
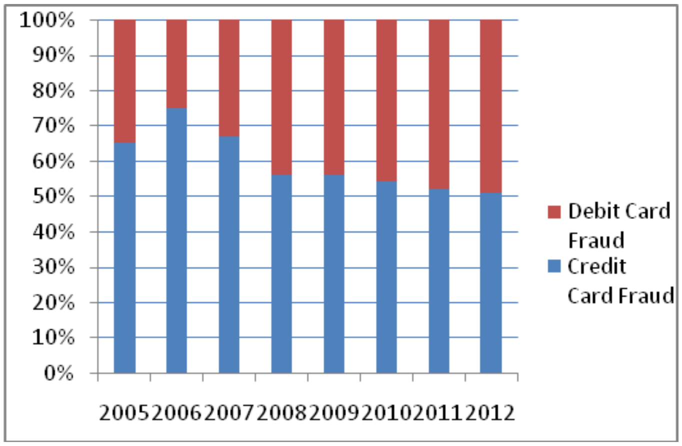


Figure 1 shows Types of Fraud Statistical Report for Year 2012. our country facing 26%of Credit Card Fraud,12% of Employment Fraud 13% of other Fraud,9% of Government Fraud,17% of Bank Fraud,18% of Utilities Fraud and 5% of Loan Fraud. Figure 2 shows both Credit and Debit Card Fraud Transaction for Year 2005 to 2012.in this figure blue can specify the Debit Card Fraudsters and red can specify the Credit Card Fraudsters. In Figure 2 year of 2005 Credit Card Fraud is Highest.

Figure 2 Credit& Debit Card Fraud Statistics for 2012



5. Decision Tree

Decision Tree have become one of the most powerful and popular approaches in knowledge discovery and Data Mining, the science and technology of exploring large and complex of data in order to discover useful patterns. Decision Tree was originally implemented in decision theory and statistic or highly effective tool inother areas such as Data Mining, Text Mining, Information extraction and Machine learning. Decision Tree is a method commonly used in DataMining. Decision Tree is a classifier in the form of tree structure.

5.1. Decision tree algorithm

Decision Tree algorithm is a data mining induction techniques that recursively partitions a data set ofrecords using depth-first greedy approach (Hunts et al, 1966) or breadth-first approach (Shafer et al, 1996) until all the data items belong to a particular class. A decision tree structure is made of root, internal and leaf nodes. The tree Structure is used in classifying unknown data records. At each internal node of the tree, a decision of best split is made using impurity measures (Quinlan, 1993). The tree leaves are made up of the class labels which the data items have been group.

Fundamental Algorithm for Decision Tree

5.2 Hunt's Algorithm

Step 1: Let x_t be the set of training record from node t.

Step 2: Let y = {y_1, y_2 . . . . y_n} be theclass labels.

Step 3: If all records in xtbelong to the same class y_t

is a leaf node labeled at y_t.

Step 4: If x_t contain records that belongs more than one class

- Select attribute test conditions to partitionthe records in the smaller subset.
- Create child node for each outcome of the test.

5.3Hunt's Algorithm using Credit Card Fraud Transcation Data

Table 1 for Credit Card Fraud Transaction Data

TID	CName	Mail Type	IP Address	TransAmt	Trans Type
T1	Ezhil	Customer	117.204.23.162	Low	Fraud
T2	Ezhil	Customer	117.204.23.162	High	Fraud
T3	Raju	Customer	117.204.23.162	Low	Legal
T4	Viki	Customer	117.204.23.162	Low	Legal
T5	Viki	Merchant	61.16.173.243	Low	Legal
T6	Viki	Merchant	117.204.23.162	Low	Fraud
T7	Raju	Merchant	61.16.173.243	High	Legal
T8	Ezhil	Merchant	117.204.23.162	Low	Fraud
T9	Ezhil	Merchant	61.16.173.243	Low	Legal
T10	Viki	Customer	61.16.173.243	Low	Legal
T11	Ezhil	Customer	117.204.23.162	High	Legal
T12	Raju	Customer	117.204.23.162	High	Legal

Let x contains five attributes such as x1,x2,x3,x4,x5 and Valuesx1=TID,x2=CName,x3=MailType,x4=IPAddress,x5= TransAmt and y be the Class labels containsthe attribute TransType and values are Either Legal or Fraud. SoLegal contains y3,y4,y5,y7,y9,y10,y11,y12and Fraud Contains y1,y2,y6,y8 class labels.Raju belongs to the same class (Legal).so Rajucomes for Leaf Node or Terminal Node and Ezhil and Viki have more than one class Legal and Fraud. We canTest the condition and partition the records in to smaller subsets and create child node for each outcome of the test.

6. Split Criteria

The best split is defined as one that does the best job of separating the data into groups where a single class. Predominates in each group. Measure used to evaluate a potential split is purity. The best split is one that increases purity of subsets by the greatest amount. A good split also creates nodes of similar size or at leastdoesn't create very small nodes.

Test for choosing the best split:

- Entropy

- Information gain ratio.

- Gini

6.1 Entropy (Information Gain)

Selection of an attribute to test at each node choosing the

IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012
ISSN (Online): 1694-0814
www.IJCSI.org

most useful attribute for classifying an example. Itcan measure how well a given attribute separate the training example according to the target classification. This measure is used to select among the candidateattribute at each step while growing the tree.

General form calculating information gain,

$$\text{Entropy (S)} = - \Sigma Pi \log2 Pi$$

Where, Pi is the probability belongs to class.

1. S is a sample of training examples.
2. P is the proportion of positive and negativeexample in S
3. Log function to the base 2 is encoded in bits.

Entropy (S) is just the average amount of informationis needed to identify the class label of a tuple S.Entropy (S) is also known as Entropy. For exampleof the credit card fraud transaction data given in Table1 there are nine instances of whichthe decision to Transtype is “Legal” and there are fiveinstances of which the decision to Transtype is “Fraud”, thenthe information gain result is:

The Entropy of each

E(S) =-9/14 x log2 (9/14) – 5/14 x log2 (5/14)= 0.940bits.

For exampleThe target class is transtype which can be legal orfraud. The attributes to collection are Tid, Cname, Transamt, IPAddress, MailTypeand TransType.detailed calculation for InformationGain (Transtype)

Entropy (Transtype) = [8/12 log2 (8/12) Legal
+ 4/12 log2 (4/12)Fraud]

=0.9185

Cname	Entropy
Ezhil	0.9709
Raju	0
Viki	0.8112
Gain	0.2486

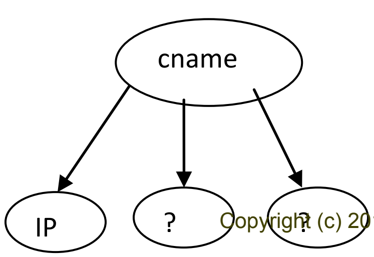
Apply the same process to the remaining attributes we get

Attributes	Gain
Email	0.01086
IP	0.1263
TransAmt	0.0568

Comparing the Information Gain of the four attributes, we see that “Cname has the Highest Value.Cname will be the Root Node of the Decision Tree. Apply the same process to the left side of the Root Node (Ezhil), we get

Entropy (Ezhil) =0.9309
Gain (Ezhil, Email) =0.0233
Gain (Ezhil, IP) =0.1387
Gain (Ezhil, TransAmt) =0.0972

The Information Gain of IP is Highest. SoIP will be the Decision Node.The decision tree look like following

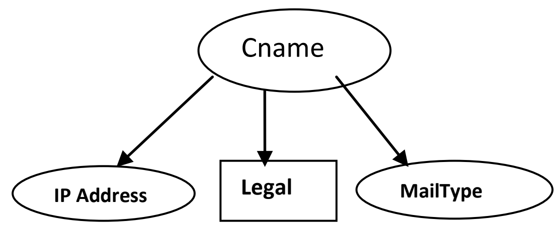


For the center of the Root Node (Raju).it is a special case. Entropy(Raju)=0.All members Raju belongs to strictly one target classification class(Legal).thus we skip all the calculation and add the corresponding Target classification value of the tree.

Apply the same process to the Right side of the Root Node(Viki) ,we get

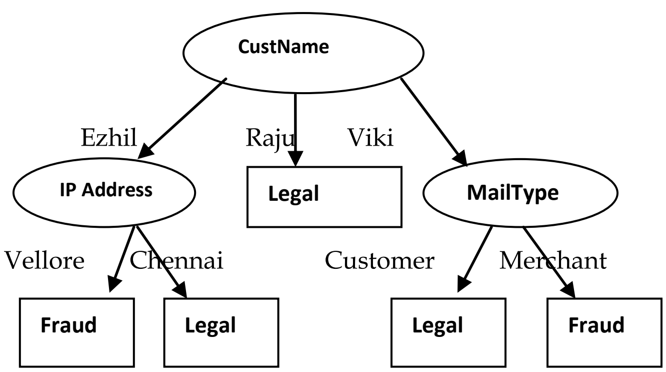
Entropy (Viki) =0.7987
Gain (Viki, mail type) =0.1089
Gain (Viki, IP) =0.0065
Gain (Viki, TransAmt) =0.0636

The Information Gain of mailtype is Highest .so mail type will be the Decision Node.the decision tree look like following



Now with IP and mail type as decision nodes. We no longer can split the decision tree based on the attributes because it has reach the Target Classification class.

The final decision tree will look like the following



6.2 Gini Index

Gini Index used in CART.Gini Index measures theimpurity of T.A does not partition a training tuples as

Gini (t) =1-ΣPi^2

When Pi Probability that a tuple in t belongs to classci is estimated|ci,t|/there let t be the training datawhere there are 9 tuples belonging to the class Transtype=”Legal” and remaining 5=”Fraud”.

Gini (transtype) =1-(9/14)2 - (5/14)2 =0.459

7 Decision Tree using Credit Card Fraud Detection

IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012
ISSN (Online): 1694-0814
www.IJCSI.org

Credit Card FraudTransaction Data Table1 contains 12 records. The Transaction table is built on the currentTransactioninformation such asTid, Cname,MailType,IPAddressTransAmt and Transtype. Instead of classifying the given transaction is either legal or fraud. The above description will be more clear and easier to understand with the help of an example table 1Transaction amount divided into two levels such as High and Low. We can find the location of the customer throughIP address.IP address traces the transaction location of the customer/merchants. Email Tracing can be divided in to two types: 1.Merchant Tracing Customer Email Address 2.Customer Tracing Merchants Email Address.

7.1MerchantTracing Customer Email

In online shopping customer can purchase the bulk of orders in some other Transaction Location.it would not necessarily mean that the customer is a carder, just be more careful when looking at other parameters of this transaction. If, however, the email address is based on a private domain name, take a look at the web site on that domain and try to decide whether it might potentially have something to do with the products ordered. Computer used to send the order, including the domain name and the IP address.

If we suspect that an order is fraudulent, we can contact the ISP of the “customer” and alert them of the fraud. Accept orders only from ISP or domain name email addresses. every fraudulent order has come through the free, web-based, or e-mail forwarding services. We are checking whether the customer is legal or fraud through customer name matching with emailid(e.g. custname: ezhil, mailid: ezhil@gmail.com) that should be Legal otherwise fraud(e.g. custname: ezhil, mailid: gai3@yahoo.com). Merchant Tracing CustomerMails are shown in Table2.

Table2 for Merchant Tracing Customer Mails

CustName	Emailid	TransType
Ezhil	**G3@yahoo.com**	**Fraud**
Ezhil	**gai3@yahoo.com**	**Fraud**
Raju	raju@gmail.com	Legal
Viki	Viki@gmail.com	Legal
Viki	Viki@gmail.com	Legal
Viki	**k_200@gmail.com**	**Fraud**
Raju	raju@gmail.com	Legal
Ezhil	**tom@gmail.com**	**Fraud**
Ezhil	ezhil@gmail.com	Legal
Viki	Viki@gmail.com	Legal
Ezhil	ezhil@gmail.com	Legal
Raju	raju@gmail.com	Legal

7.2 Customer Tracing Merchant email address

Check the domain name of the email address: whether it is a free mail service domain (e.g., @yahoo.com, @hotmail.com, @gmail.com) or a commercial web site domain name (@somecompany.com). If the email address is based on a free mail service, easiest way to find fake mail through an SMTP server. Either telnet to port 25 on a server and do the commands yourself or use a client like Outlook Express or Netscape Messenger and tell it any email addresscustomer want. There are also the times when customer has to trace down themerchant real e-mail address that was sent using a free service like Yahoo or Hotmail. There are anonymous remailers out there that would make the methods of tracing fake mail details shown in Figure 3.

Figure3 Tracing Fake Mail Details

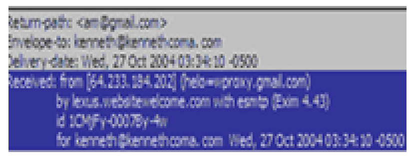


Figure3 shows email envelope is composed of a series of "Headers". These are just a series of lines of characters which precede the actual email message. Email programs such as Outlook do not normally display these Headers when displaying a message. From these Headers however, the email program is able to extract important information about the message, such as the message encoding method, the creation date, the message subject, the sender and receiver, etc. Moreover, just as a postal envelope contains an address, a return address and the cancellation stamp of the post office of origin, an email message inthese "Headers" carries with ita history of its journey to email inbox. Because of this, it's possible to determine the original IP address of the sender. Since email programs do not normally display these Headers. The Recipient's email server (POP3, Yahoo, Hotmail, etc.) receives the email message from the original sender's server. (e.g. bay15.hotmail.msn.com).

The newest 'Received:' Header at the top of the sequence of Headers now contains the IP address belonging to the email server of the sender; (e.g. gmail.com) It is not the true IP address of the sender himself.

Received: from 64.233.184.202
Bygmail.com with HTTP;
Wed, 27Oct 2004 03:34:10 GMT

The Sender sends an email message to his own email server to begin its journey to the receiver. A common Headers strings is created.

8. IP Address

Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address. IP addresses consist of four numbers separated by periods (also called a 'dotted-quad') and look something like 127.0.0.1.Since these numbers are usually assigned to internet service providers within region-based blocks, an IP address can often be used to identify the region or country from which a computer is connecting to the Internet. An IP address can sometimes be used to show the user's general location. Because the numbers may be tedious to deal with, an IP address may also be assigned to a Host name, which is sometimes easier to remember. Hostnames may be looked up to find IP addresses, and vice-versa. At one time ISPs issued one IP address to each user. These are called static IP addresses. Because there is a limited number of IP addresses and with increased usage of the internet ISPs now issue IP addresses in a dynamic fashion out of a pool of IP addresses (Using DHCP). These are referred to as dynamic IP addresses. This also limits the ability of the user to host websites, mail servers, ftp servers, etc. In addition to users connecting to the internet, with virtual hosting, a single machine can act like multiple machines (with multiple domain names and IP addresses).

8.1 Customer IP address

Check the customer's IP address. Firstfind the administration section "Orders" of shop. There are quite a few online services that automatically retrieve detailed information about the domain owner or the company who owns the server with the specified IP address. Find out where the server with the customer's IP address is located. If the country of the server is not the same as the country specified in the order shipping address, the transaction validity would be liable to Fraud.

8.2 IP Tracing & IP Tracking (117.204.23.162)

Trace an IP address we can easily find the Location of the customer/merchant, we can get detailed information on any IP Address anywhere in the world. Results include detailed IP address location, name of ISP, net speed/speed of internet connection, and more.

Figure4 Tracing IP address

117.204.23.162 IP address location & more:	
My IP address [?]:	117.204.23.162 [Whois] [Reverse IP]
My IP country code:	IN
My IP address country:	India
My IP address state:	Tamil Nadu
My IP address city:	Velluru
My IP address latitude:	12.9333
My IP address longitude:	79.1333
My ISP [?]:	BSNL
My Proxy:	None / Highly Anonymous
Organization:	BSNL
Local time in India:	2012-05-05 20:10

In this following figure4 shows the detail information about customer/merchant make transaction from where and which location .we easily find the location of the customer/merchant through IP Address. So figure4 shows the IP Address (117.204.23.162) and the transaction locationis Vellore in Tamilnadu and ISP is BSNL.it can give all information details of IP location ,city ,state, time and ISP. .

Conclusion

In this Paper Presents a Credit Card Fraud Detection using effective algorithm for Decision Tree Learning. Although focus on the Information Gain based Decision Tree Learning in this paper estimating the best split of Purity Measures of Gini, Entropy and Information Gain Ratio to test the best classifierAttribute. In this Technique we simply find out the Fraudulent Customer/Merchant through Tracing Fake Mail and IP Address. Customer /merchant are suspicious if the mail is fake they are traced all information about the owner/sender through IP Address. It can find out the Location of the customer and Trace all details. Decision Tree is Most Powerful Technique in Data Mining Decision Tree is vital part of Credit card Fraud Detection.

Acknowledgments
The Author Gradually Acknowledges the Support of Kanchi Sri Krishna College and the Department of Computer Science

References

[1] Jon T.S. Quah, M. Sriganesh, "Real-time credit card fraud detection using computational intelligence", Expert Systems with Applications, 35(4), pp.1721-1732, 2008.

[2] Suvasini Panigrahi, Amlan Kundu, Shamik Sural, A.K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning", Information Fusion, 10(4), pp. 3630-3640, 2009.

[3] Quinlan, J.R. 1986. Induction of Decision trees. Machine Learning

[4] J. Han, M. Kamber, Data Mining: Concepts and Techniques, Elsevier Inc. (2006).

[5]. H. Witten and E. Frank, Data Mining: Practical Machine Learning Tools and Techniques, 2nd Decision Tree Edition, Elsevier Inc., 2005.

[6].Kass G. V., An exploratory technique for investigating large quantities of categorical
Data. Applied Statistics, 29(2):119-127, 1980.

[7].Kearns M. and Mansour Y., A fast, bottom-up decision tree pruning algorithm with near-optimal generalization, in J. Shavlik, ed., 'Machine Learning:

[8].Proceedings of the Fifteenth International Conference', Morgan Kaufmann Publishers, Inc., pp. 269-277, 1998.

[9].Kearns M. and Mansour Y., On the boosting ability of top-down decision tree learning algorithms. Journal of Computer and Systems Sciences, 58(1): 109-128, 1999.Kohavi R.

[10].Duncan M D G. 1995. The Future Threat of Credit Card Crime, RCMP Gazette, 57 (10): 25–26.

[11].P Chan, W Fan, A Prodromidis & S Stolfo. 1999. Distributed data mining in credit card fraud detection, IEEE Intelligent Systems, 14(6): 67–74.

[11].Maguire S. 2002. Identifying Risks during Information System Development: Managing the Process, Information Management & Computer Security, 10(3): 126–134.

[12].2002. Card Fraud Facts 2002, APACS (Administration) Ltd, Association for Payment Clearing
Services (APACS), April 2002.

[13] P. Cunningham, N. Nowlan, S.J. Delany, and M. Haahr, "A case-based approach in spam filtering that can track concept drift", In Proceedings: The ICCBR‟03 Workshop on Long-lived CBR Systems, Trondheim, Norway, 2003

[14] K. Wei, A naïve Bayes spam filter, Faculty of Computer Science, University of Berkely, 2003.
B. Kamens, Bayesian filtering: Beyond binary classification. Fog Creek Software, Inc., 2005.

[15]Dr.R.Dhanapal, Gayathri Subramanian, Jobin M Scaria. "Customer Retention Using Data Mining Techniques". International Journal of Computer Applications, Vol. 11, No.5, pp. 32 - 34, 2010.

[16]V.Deepa, Dr.R.Dhanapal, D.Remigious. "A Novel Approach to Credit Card Fraud Detection Model". International Journal of Computing, Vol. 2, Issue 12, pp. 94 – 96, 2010.

AUTHORS BIOGRAPHY

First Author Dr.R.Dhanapal obtained his PhD in Computer Science from Bharathidasan University, Tamil Nadu, India. He is currently Professor & Head, Research Department of Computer Applications, SRM Easwari Engineering College, Affiliated to Anna University Chennai, Tamil Nadu, India. He has 25 years of teaching, research and administrative experience his includes 21 years of Government Service. Besides being Professor, he is also a prolific writer, having authored twenty one books on various topics in Computer Science. His books have been prescribed as text books in Bharathidasan University and Autonomous Colleges affiliated to Bharathidasan University. He has served as Chairman of Board of Studies in Computer Science of Bharathidasan University, member of Board of Studies in Computer Science of several universities and autonomous colleges. Member of standing committee of Artificial Intelligence and Expert Systems of IASTED, Canada and Senior Member of International Association of Computer Science and Information Technology (IACSIT), Singapore and Member of International Association of Engineers, Hongkong. He has Visited USA, Japan, Malaysia, and Singapore for presenting papers in the International conferences And to demonstrate the software developed by him. He is the recipient of the prestigious 'Life-time Achievement' And 'Excellence' Awards instituted by Government of India. He served as Principal Investigator for UGC and AICTE, New Delhi funded innovative, major and minor research projects worth of 1.7 crore especially in the area of Intelligent Systems, Data Mining and Soft Computing. He is the recognized supervisor for research programmes in Computer Science leading to Ph.D. and MS by research in several universities including Anna University Chennai, Bharathiar University Coimbatore, Manonmaniam Sundaranar University Tirunelveli, Periyar University Salem, Mother Teresa University Kodaikanal and many Deemed Universities. He has got 63 papers on his Credit in international and national journals. He has been serving as Editor In Chief for the International Journal of Research and Reviews in Artificial Intelligence (IJRRAI) United Kingdom and serving as reviewer and member of editorial in edited peer reviewed national and international Journals including Elsevier Journals

.**Second Author** P.Gayathiri is Research Scholar in Manon Maniam Sundaranar University .She Received her MSc Degree in Kanchi Sri Krishna College and did her MPhil from Bharathidasan University. She is working in Kanchi Sri Krishna College as Assistant Professor. She has Published 4 International and National Conferences. Her Areas of Interest Data Mining and Mat lab.