MINOR PROJECT REPORT

ON

CREDIT CARD FRAUD DETECTION BY USING MACHINE LEARNING

SUBMITTED FOR THE PARTIAL FULFILLMENT OF THE DEGREE OF

MBA in DATA SCIENCE

SEMESTER III

BY KOMAL DEV

A9920123000459(el)

Name of Supervisor

Dr, Neha Tandon
(Amity University Online)

AMITY UNIVERSITY ONLINE

DECLARATION

I, Komal Dev, Enrolment Number- A9920123000459(el), student of MBA in Data Science, Amity University Online, with this, declare that the project entitled “**Credit Card Fraud Detection By Using Machine Learning**” has been carried out independently by me under the guidance of Dr. Neha Tandon, Associate Professor, Amity University Online.

ACKNOWLEDGEMENT

I would like to express my utmost gratitude to my Guide Professor Dr. Neha Tandon for making me introduce the credit card frauds and for their unforgettable support in acquiring the knowledge. I shall be very thankful to her for her valuable input.

ABSTRACT

In the modern era, the widespread acceptance of online payment systems and internet banking has streamlined transactions globally, offering enhanced convenience and swiftness. However, the escalating prevalence of credit card transactions has also corresponded with a surge in online identity theft incidents, resulting in consequential losses for both financial institutions and consumers. This trend, observed predominantly in western economies, has also begun to manifest in developing economies like India. In response to this pressing issue, a comprehensive study has been conducted to analyze the patterns of credit card fraud within the Indian banking sector. Over a span of ten years from 2005 to 2014, this study meticulously examined secondary data to discern trends at the bank, group, and yearly levels. The findings of this investigation indicate a downward trajectory in online fraud occurrences in recent years, underscoring banks' heightened focus on security measures, detection of new fraud techniques, and development of strategies to combat them. Additionally, the study has proposed guidelines and measures to address these challenges, shedding light on innovative security approaches adopted by various banks that could be emulated by others to safeguard their online clientele. Consequently, this research contributes to mitigating the risks associated with online transactions, offering valuable insights for the banking industry at large.

TABLE OF CONTENTS

1.1 INTRODUCTION

Since 2020, identity theft and credit card fraud have surged in frequency due to the growing prevalence of digital transactions, with fraudsters employing tactics like phishing, identity theft, and unauthorized transactions using stolen card information. Despite a decrease in reported cases, these types of fraud have consistently exceeded pre-pandemic levels throughout 2023, as indicated by the latest statistics.After doubling between 2019 and 2020, reports of identity theft continued to grow in 2021, and nearly 1.4 million people were impacted. Approximately 1.1 million reports of identity theft were collected by the Federal Trade Commission (FTC) in 2022 and 1 million reports were filed in 2023.

In 2023, there were 1.036 million reports of identity theft, a decrease from 1.107 million in 2022 and 1.434 million in 2021. Among the types of identity theft, credit card fraud was the most prevalent in 2023, with 426 thousand reports, down from 448 thousand in 2022. Government documents or benefits fraud saw a significant increase of 68% in 2023, following an 85% decline in 2022. The number of reports for this type of fraud reached 102,000 in 2023 compared to 61,000 in 2022. According to a report by Javelin Strategy & Research, losses from identity theft cases amounted to $20 billion in 2022, representing a 15% decrease from the previous year's study.

The popularity of top-tier premium credit cards in India is experiencing an upswing, driven by expanding benefits and a heightened level of financial awareness, particularly among younger demographics. As of June 2022, there were over 6.78 lakh ATM transactions and roughly 12.1 crore POS transactions associated with these cards. Projections suggest a sustained upward trajectory, with an anticipated 45.3 million cards in circulation by 2028. This growth is bolstered by a diverse array of issuers, including non-banking financial companies (NBFCs) and fintech startups, which offer customized EMI (Equated Monthly Installment) options, thus further contributing to the increasing appeal of credit cards.

In 2015, the Reserve Bank of India (RBI) mandated that all new credit and debit cards issued in India should be EMV chip-enabled. EMV stands for Europay, Mastercard, and Visa, the three companies that developed the global standard for smart chip cards. EMV chip cards offer enhanced security and functionality, such as supporting offline transactions, dynamic data authentication, and tokenization.

1.1.1 Innovation & Development in the field of credit card

Year	Innovation
1946	The First Bankcard, Named Charge It, was introduced by John Biggins, a banker in Brooklyn.
1950	The Diners Club Card is the next development in the field of credit card.
1951	Franklin National Bank in New York's Starts a credit card plan.
1959	American Express Introduces the Plastic Card.
1966	Barclays Bank was the first British bank to introduce credit card known as the "Barclays card"
1966	The national credit card system was formed by the Inter Bank card Association. This Card is known as the Master card. Formerly credit cards are issued only to the local customers of the bank.
1977	Lloyds Bank introduces "Access Card."

Table 1.1

Credit Cards in India

Credit cards in India have a recent history. In the starting, a few Banks take the initiative to introduce the credit card. A few Historical steps in the development of credit cards in India is discussed below:

Year	Innovation
1961	Diners Club Card by Kali Mody introduces credit cards in India
1981	Andhra Bank and Central Bank of India has introduced the credit cards.

1988	SBI introduced its proprietary credit card
1989	ANZ Grindlays Bank came with a classic card.
1990	Citi Bank’s Mastercard became popular.

Table 1.2

Number of credit and debit card fraud incidents reported across India in 2022, by leading state

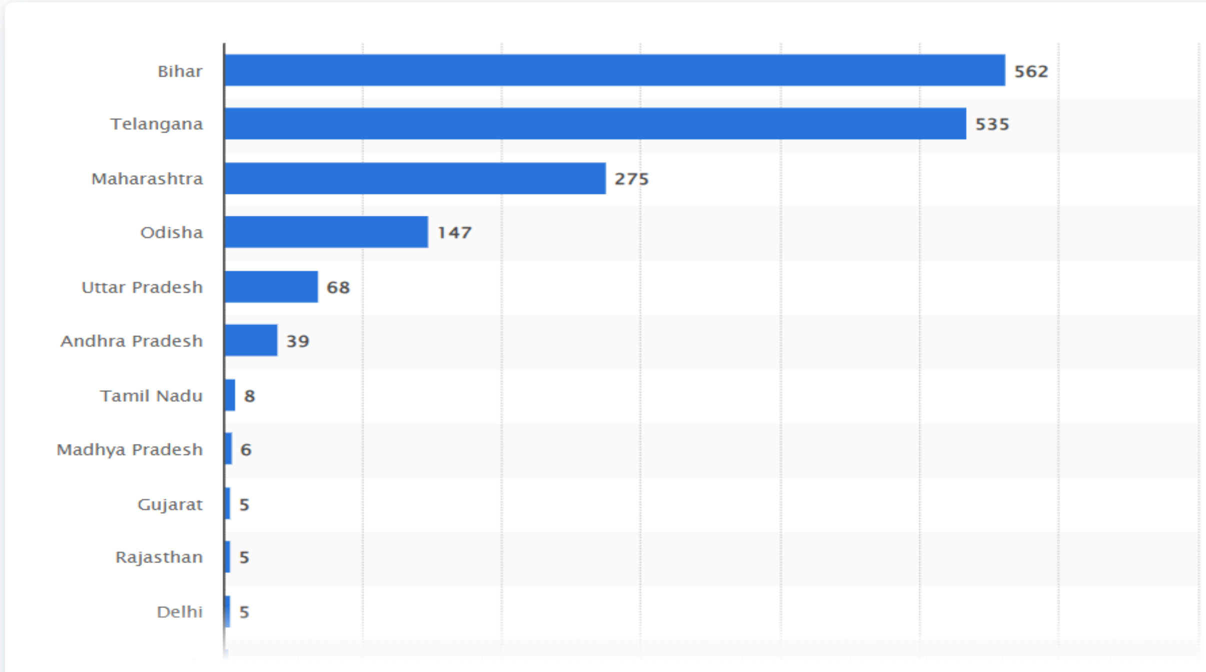


Fig 1.1

In 2022, the state of Bihar in India had the highest number of credit and debit card frauds, with approximately 562 cases registered with the authorities. The country recorded over 1.6 thousand cases of credit and debit card fraud that year. This category of crime came under the purview of Section 420 of the Indian Penal Code.

1.1.2 Credit Card Frauds

Credit card fraud, a type of identity theft, entails the illicit acquisition of someone else's credit card details to make unauthorized purchases or withdraw funds. It typically falls into two categories: application fraud and account takeover. Perpetrators can steal card information physically or electronically through hacking, leading to significant inconvenience and financial loss for victims. Unauthorized charges can accrue, potentially resulting in substantial bills and damage to credit scores. Fortunately, taking proactive measures can mitigate these risks. Vigilance over accounts and early detection of suspicious activity are paramount. Here are some prevalent forms of credit card fraud and strategies to defend against them, helping you safeguard your financial information effectively.

1.1.3 How credit card fraud happens

Credit card fraud occurs when an unauthorized person gains access to your information and uses it to make purchases. Here are some ways fraudsters get your information:

1.1.4 Types of Credit Card Fraud Businesses Are at Risk of & How to Prevent Them

The first step for reducing your risk of credit card fraud is understanding what types of credit card fraud exist. Below are six types of credit card fraud that businesses are at risk of. While this is by no means a comprehensive list, it covers the types of fraud most dangerous to your business.

1. Credit Card Skimming

Credit card skimming represents one of the card-present fraud methods. It entails the utilization of a physical device, known as a skimmer, which is covertly installed on ATMs, gas pumps, or other card readers. These devices surreptitiously capture both the credit card information and the associated PIN of unsuspecting users. Skimmers are challenging to detect as they are engineered to seamlessly blend with the card reader, making them inconspicuous to users.

How to Prevent Credit Card Skimming

While credit card skimming may not directly lead to payment fraud using stolen credit card information, it poses a significant risk to your business's reputation. The discovery of a skimmer on a card reader near or within your establishment can severely damage your reputation. To mitigate this risk, it's crucial to regularly inspect card readers for any indications of tampering. Utilizing secure card readers equipped with tamper-evident seals and encryption can enhance security measures. Additionally, securing your business perimeter, such as installing security cameras, can help deter potential skimming attempts and safeguard your customers' financial information.

2. Identity Theft

Identity theft, occasionally referred to as application fraud, is an indirect form of credit card theft. In this scheme, a fraudster utilizes an individual's personal information to establish a new credit card account and conduct transactions under their identity. Victims often only discover this type of theft upon reviewing their credit report or receiving statements for purchases they did not authorize.

How to Prevent Identity Theft

Identity theft poses a formidable challenge to prevent, especially once a fraudster successfully opens a credit card account using another person's identity, effectively deceiving the credit card issuer. However, implementing stringent measures can mitigate the risk.

One approach is to restrict purchases to verified accounts, ensuring that customers must authenticate their identity before transacting. During the identity verification process, cross-referencing identity data with public databases can help detect any disparities between the individual opening the account and the documentation they provide. This proactive verification can help thwart identity theft attempts by uncovering inconsistencies and potentially fraudulent activity.

3. Account Takeover (ATO) Fraud

Account takeover fraud is a form of credit card fraud wherein a perpetrator gains unauthorized access to someone else's account and exploits it to make purchases. This can involve using the credit card linked to the account or employing new, stolen credit card information. To evade detection, fraudsters frequently alter account particulars like email addresses and phone numbers, complicating the process for victims to identify and respond to this type of fraudulent activity.4

How to Prevent Account Takeover Fraud

Account takeover fraud can indeed be more straightforward to prevent compared to identity theft since fraudsters often rely on automated tools to breach accounts. Effective fraud prevention software can intercept and thwart these bots before they infiltrate your website or mobile app.

However, it remains prudent to remain vigilant for any signs of suspicious transaction activities that could signal credit card fraud. These might include numerous small purchases or a single large transaction that deviates from a customer's typical behavior. When such patterns are detected, it's advisable to request additional identification from the customer, such as sending a security code to their registered phone number or email address, as an added layer of verification. This proactive approach can help mitigate the risk of account takeover fraud and safeguard your customers' accounts and financial information.

4. Phishing

Phishing is an online scam tactic in which fraudsters send deceptive emails or messages, masquerading as reputable organizations, to trick recipients into divulging sensitive personal information, including credit card details. These fraudulent messages typically include links to counterfeit websites designed to mimic legitimate ones, urging individuals to engage in a fake payment process.

How to Prevent Phishing

Phishing primarily targets consumers, but it's crucial to safeguard your business from impersonation by scammers. Regularly reminding your customers not to interact with messages or click on links outside of your official communication channels can help mitigate this risk. Additionally, reinforce the message that your business will never request sensitive information via insecure channels.

Similarly, educate your employees about the potential for scammers to impersonate executives within your organization, such as the CEO or other C-level executives, in fraudulent emails seeking sensitive information. Implementing stringent spam filters and providing thorough training to your employees can help them recognize and avoid responding to suspicious emails, thereby fortifying your business against phishing attempts.

5. CNP Fraud

Card-not-present (CNP) fraud encompasses all forms of credit card fraud where perpetrators conduct transactions without physically possessing the credit card. This type of fraud is prevalent and poses a significant challenge for detection and prevention. Since fraudsters can operate remotely, CNP fraud offers a relatively safe avenue for exploitation, allowing perpetrators to maintain anonymity and evade apprehension. Unfortunately, due to these factors, instances of CNP fraud often go unpunished, contributing to its persistent prevalence.

How to Prevent CNP Fraud

Indeed, CNP fraud, like account takeover fraud, often leverages automation due to its efficiency. Fraudsters use bots and automated scripts to exploit vulnerabilities, as manually identifying susceptible businesses would be time-consuming. Implementing robust payment fraud prevention software is crucial for shielding against these automated attacks.

Moreover, enhancing security measures can further fortify defenses against CNP fraud. Implementing multi-factor authentication (MFA) or requesting additional identity verification, such as card verification values (CVV), can be effective strategies. These measures serve as obstacles that impede automated bots, enhancing protection against fraudulent activities.

6. Card Cracking Fraud

When fraudsters acquire stolen credit card details, they may lack certain crucial information needed to perpetrate payment fraud. To address this gap, they employ bots to engage in card cracking, a form of brute-force attack. This tactic involves systematically cycling through various combinations on a payment platform in rapid succession, attempting to deduce the missing credit card values. Through this method, fraudsters aim to uncover the necessary details to facilitate fraudulent transactions.

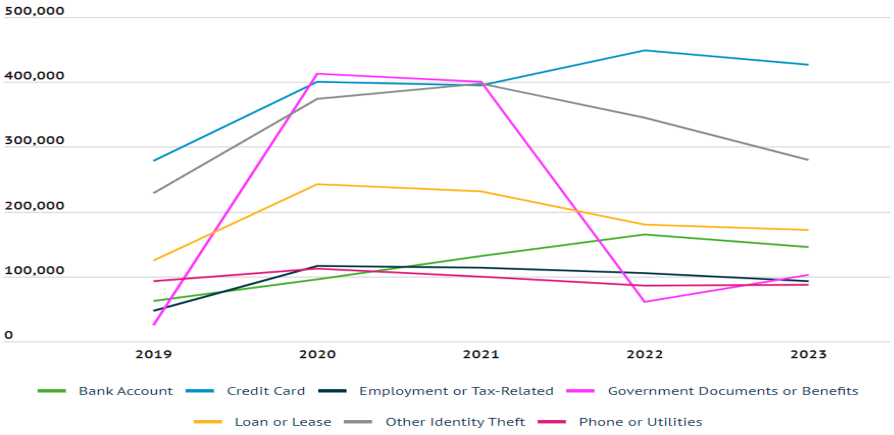
How to Prevent Card-Cracking Fraud

Indeed, leveraging fraud prevention software is a cost-effective and efficient method to counter carding attacks. With the appropriate preventative software in place, fraudster bots are effectively thwarted from even accessing your website or mobile app, let alone reaching your payment platform.

Additionally, it's imperative to bolster the security of your payment platform by implementing stringent measures. Limiting the number of payment attempts a customer can make before flagging a transaction as suspicious can help mitigate the risk of carding attacks. Moreover, integrating security measures like multi-factor authentication (MFA) and requesting card verification values (CVVs) further fortifies your defenses against fraudulent activity.

By combining robust fraud prevention software with enhanced security measures on your payment platform, you can effectively safeguard your business and customers against the threat of carding attacks

Identity theft reports by type



Data source: FTC (2024).

Fig 1.2

2. OBJECTIVES OF THIS STUDY

This project aims to identify and prevent unauthorized charges for customers by detecting fraudulent credit card transactions. This will be accomplished by employing diverse machine learning techniques, which will subsequently undergo comparative evaluation to assess their efficacy. The project will also entail a review of existing literature and methodologies to determine the most appropriate approach for distinguishing fraudulent transactions within the dataset. Furthermore, the results will be presented using graphical representations and numerical analysis.

3. Literature Review

Panigrahi, S., Kundu, A., and Sural, S., have proposed an innovative model for credit card fraud detection which is based on the combination of the three approaches i.e. rule-based filtering, Dempster- Shafer theory, and Bayesian Learning. For the computation of the initial belief regarding the incoming transactions, the author has used Dempster's rule, a rule-based component on the combined multiple evidence. The Bayesian Learning is used for updating the suspicious score by using the history database of the genuine cardholder and the fraudster cardholder.

Falaki S. O., Alses B. K., Adewale O. S., Ayeni, J.O., and Aderounmu, G. A. have suggested the probabilistic model for the detection of fraud. In these methods, the author makes the best use of the algorithms of the Baum Welsh and hybrid posterior-Viterbi. In this research paper the author concluded that after the efficient and better utilization of the parameters, the posterior-Viterbi cum new detection model performance is better than the Viterbi cum old fraud detection model.

There are several Fraud detection techniques for developed countries so Anwer, R., Baig, S., Khiyal M. S. H., Khan, A., Khanum, M. has studied those techniques and evolved the online fraud prevention system specially for developing countries. The system proposed by the author consists of multiple checks namely, Lost/ Stolen Check (LS), Credit card Validation Check (Val), Security Code Check (SC), Expiry (Exp), Multiple IP (MIP), and Repeated IP (RIP). This method is the advancement of the Address Verification System (AVS).

Ghosh S. and Reilly D. Lhas proposed a Credit card fraud detection technique with the neural network. This study on Mellon Bank showed that due to the use of neural network-based technology for detecting credit card fraud, it is possible to reduce the total credit card fraud by 20 -40 %. Shrivastava A., Kundu, A., and Sural S.they had proposed a model of fraud detection with the application of HMM. They
completely defined the stochastic process followed by the HMM. This study explained how HMM is efficient in detecting whether the transaction is fraudulent or genuine. Along this the author conducted a comparative study between the existing models of fraud detection and Hmm and established the accuracy of the system using HMM is 80 %.

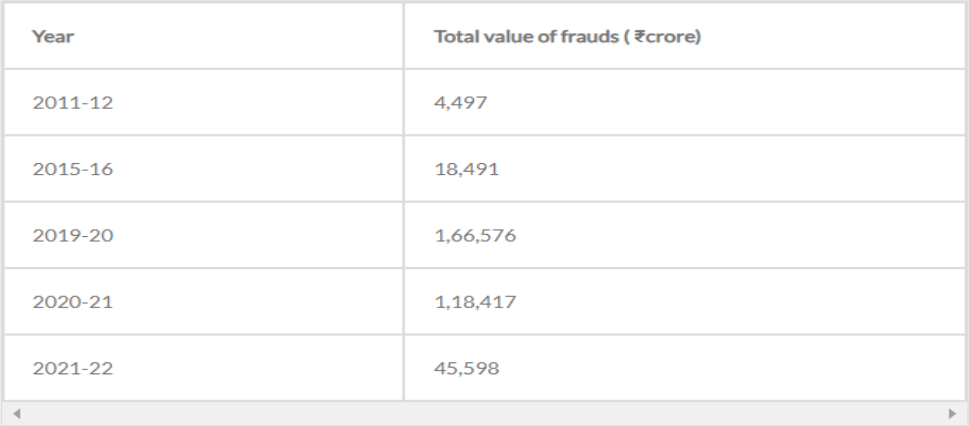
Delamaire, l., Abdou, H., and Pointon, J., have explained the types of credit card fraud and explained the various detection techniques of credit cards based on the review of existing literature.

Kadam, N., Soni, S., Puntambekar, D., and Kaul, R. have done a study to prevent customers from credit card fraud. The authors use the Concept of Data Mining and the Hidden Markov model for the detection of credit card fraud. Prakash, A., and Chandrasekar, C., have explained the concept of the Advanced Hidden Markov Model and shown the entire process of fraud detection.

4. Research Methodology

In this research paper, Descriptive statistics is used to represent the trends of credit card fraud. This study analyzes the secondary data. The India Stat Software, RBI reports, Indian Banking Association Reports, and New papers are used as the sources of the data.

4.1 Year-wise Trend of Fraud in Credit Card



Year	Total value of frauds (₹crore)
2011-12	4,497
2015-16	18,491
2019-20	1,66,576
2020-21	1,18,417
2021-22	45,598

Fig 2.1 shows the trend of credit card fraud from 2011-2022.

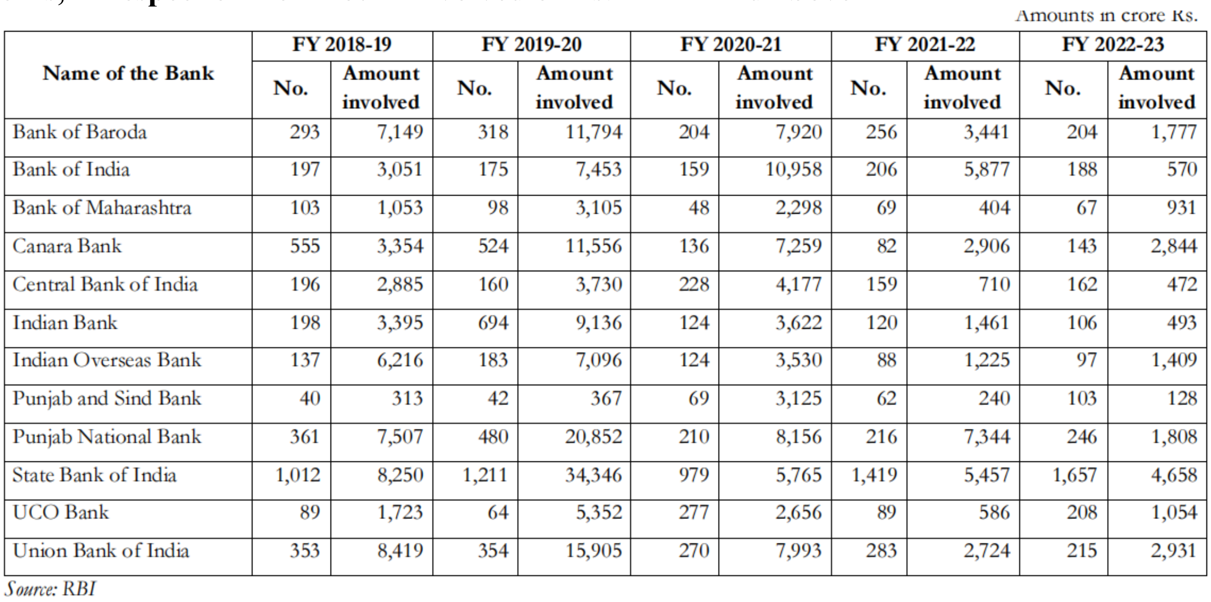
According to the latest RBI data on trends and progress of banking in India, a total of 9,053 fraud cases were reported in various banking operations in the fiscal year 2021-22, amounting to ₹45,598 crore. This figure marks a substantial increase compared to the data from 2011-12 when there were 4,091 cases of fraud totaling ₹4,497 crore. The data specifically pertains to frauds amounting to ₹one lakh and above.

Most of the reported frauds in banking transactions are related to 'advances'. Out of the total ₹45,598 crores, frauds related to advances account for ₹43,512 crore, while deposit-related frauds amount to ₹493 crore and cheque/demand drafts-related frauds are valued at ₹158 crore.

In contrast, the data from 2011-12 indicates that a vast majority of the frauds, valued at ₹3,552 crores, were related to advances, while frauds related to deposits and cheque/demand drafts were valued at ₹219 crores and ₹40 crores, respectively.

It's important to highlight that there has been a significant decline in the total value of fraud over the past two years. In the fiscal year 2020-21, the value of frauds decreased from ₹1,66,576 crore in 2019-2020 to ₹1,18,417 crore in 2020-21 and further dropped to ₹45,598 crore in the subsequent year.

4.2 Details of Frauds as reported by Public Sector banks during the last five financial years, in respect of the amount involved of Rs. 1 lakh and above



Amounts in crore Rs.

Name of the Bank	FY 2018-19		FY 2019-20		FY 2020-21		FY 2021-22		FY 2022-23	
	No.	Amount involved	No.	Amount involved	No.	Amount involved	No.	Amount involved	No.	Amount involved
Bank of Baroda	293	7,149	318	11,794	204	7,920	256	3,441	204	1,777
Bank of India	197	3,051	175	7,453	159	10,958	206	5,877	188	570
Bank of Maharashtra	103	1,053	98	3,105	48	2,298	69	404	67	931
Canara Bank	555	3,354	524	11,556	136	7,259	82	2,906	143	2,844
Central Bank of India	196	2,885	160	3,730	228	4,177	159	710	162	472
Indian Bank	198	3,395	694	9,136	124	3,622	120	1,461	106	493
Indian Overseas Bank	137	6,216	183	7,096	124	3,530	88	1,225	97	1,409
Punjab and Sind Bank	40	313	42	367	69	3,125	62	240	103	128
Punjab National Bank	361	7,507	480	20,852	210	8,156	216	7,344	246	1,808
State Bank of India	1,012	8,250	1,211	34,346	979	5,765	1,419	5,457	1,657	4,658
UCO Bank	89	1,723	64	5,352	277	2,656	89	586	208	1,054
Union Bank of India	353	8,419	354	15,905	270	7,993	283	2,724	215	2,931

Source: RBI

Table 4.1

Source: Lok Sabha Unstarred question no. 254, regarding BANK FRAUDS

4.3 Tables 5.1, 5.2, Fig 5.1, and Fig 5.2 explain the trends of credit card fraud from 2005-2004.

Table 5.1 shows the trends of credit card fraud from 2005-2004 (in numbers).

Years	Numbers of Frauds
2004-2005	2994
2005-2006	19252
2006-2007	16308
2007-2008	17447
2008-2009	17114
2009-2010	18925
2010-2011	6388
2011-2012	71
2012-2013	115
2013-2014	227

Fig. 1 depicts a trend wherein the number of frauds surged up to 2010, coinciding with the entry of banks and non-banking institutions into the credit card market. During this period, these entities could not effectively detect and combat the various techniques employed by fraudsters. Subsequently, there was a decline in the number of frauds from 2010 to 2014, attributable to banks becoming more cognizant of fraud detection techniques adopted by developed countries.

However, since then, there has been a slight increase in the number of frauds. This resurgence can be attributed to fraudsters' enhanced innovation and expedited tactics. Despite this recent uptick, drawing a trend line reveals an overall decreasing trend. This trend can be attributed to the heightened awareness levels among both customers and banks regarding fraud prevention measures.

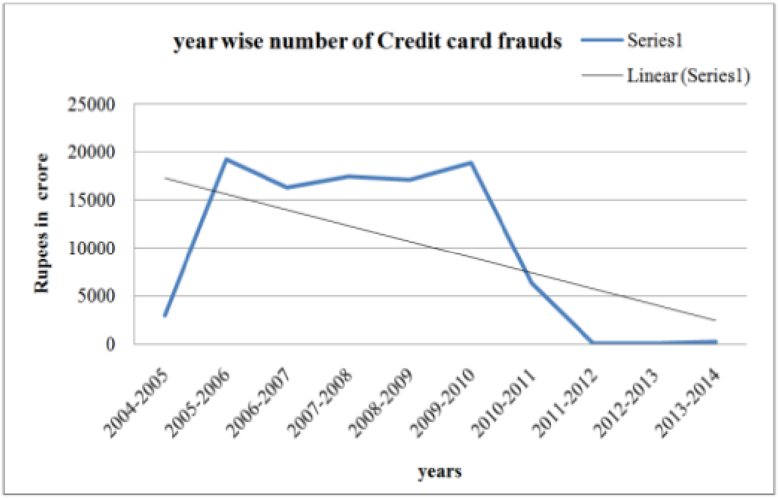


Fig 5.1

Source: Lok Sabha Unstarred Question No. 1640, dated 19.11.2010 & Lok Sabha Unstarred Question No. 1261, dated 18.07.2014.

Table 6.2: Shows the amount-wise trend of credit card frauds from 2005-2014.

Years	Amounts of frauds (Rs in Crore)
2004-2005	5.32
2005-2006	35.69
2006-2007	35.82
2007-2008	41.1
2008-2009	47.43

2009-2010	54.67
2010-2011	12.28
2011-2012	4.39
2012-2013	5.19
2013-2014	4.16

Fig. 6.2 shows the amount-wise trend of credit card fraud from the years 2005-2014. It reveals that the trend of the amount of credit card fraud is decreasing.

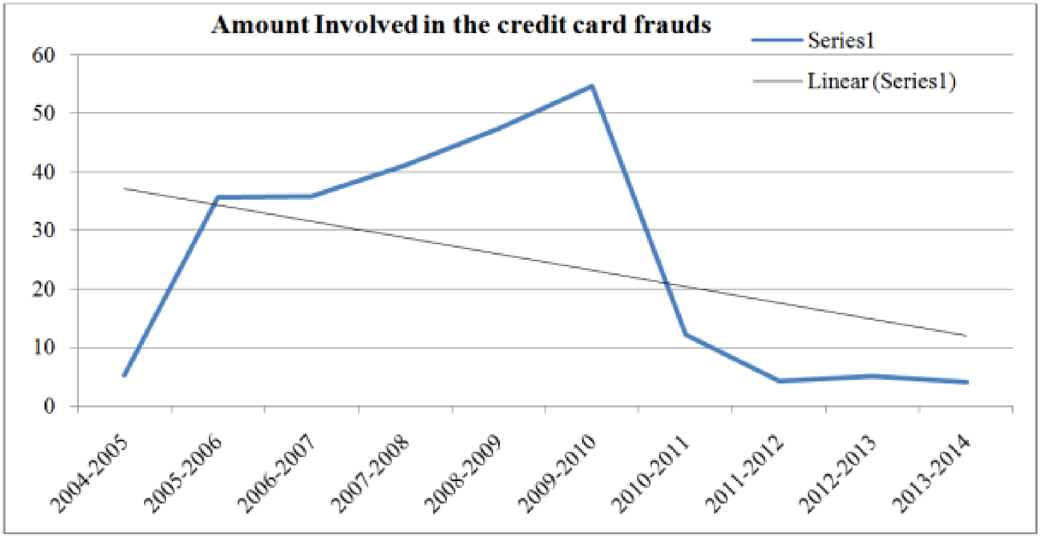


Fig. 5.2

Source: Lok Sabha Unstarred Question No. 1640, dated 19.11.2010 & Lok Sabha Unstarred Question No. 1261, dated 18.07.2014.

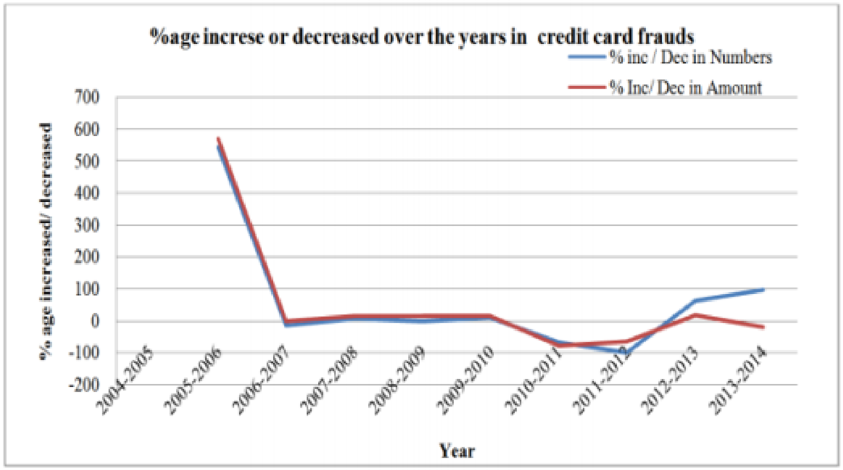
Table 5.3 gives a comprehensive picture of the frauds that increased or decreased from the years 2005-2014.

Year	%Inc/Dec in Number	% Inc/Dec in Amount
2005-2006	534.0194	570.8674
2006-2007	-15.2919	0.364248
2007-2008	6.984302	14.74037
2008-2009	-1.90864	15.40146

2009-2010	10.58198	15.2646
2010-2011	-66.2457	-77.53796
2011-2012	-98.8885	-64.25081
2012-2013	61.97183	18.22323
2013-2014	97.3913	-19.84586

Fig. 5.3 illustrates the trend of credit card fraud in terms of both amount and number, presenting the percentage increase or decrease over the years. The data reveals a consistent trend where both the amount and number of credit card frauds follow a similar pattern.

However, an anomaly is observed in the year 2013-2014, wherein the amount-wise chart shows a decrease in the amount involved in credit card frauds, while the number-wise chart indicates an increase in the number of frauds. This discrepancy can be attributed to banks' heightened focus on fraud risk management during this period, leading to stricter credit limits. Consequently, although the number of credit card frauds increased, the amount involved in these frauds decreased compared to previous years. This suggests a more proactive approach by banks in mitigating the financial impact of fraudulent activities.



Source: Lok Sabha Unstarred Question No. 1640, dated 19.11.2010 & Lok Sabha Unstarred Question No. 1261, dated 18.07.2014.

4.4 Comparison between Credit card fraud and Technological fraud

Table 5.4 compares the trends of technological fraud with the trends of credit card fraud.

Years	Credit card frauds (In Numbers)	Technologies Frauds (In Numbers)
2009-2010	18925	19787
2010-2011	6388	14271
2011-2012	71	10048
2012-2013	115	8765

Fig. 5.4 presents a comparison between credit card frauds and technological frauds, the latter comprising frauds perpetrated through the use or exploitation of technology. This category encompasses various types of fraudulent activities such as debit card fraud, credit card fraud, phishing, and fraudulent emails, among others.

The data depicted in Fig. 5.4 reveals that both credit card frauds and technological frauds exhibit a similar trend over time. This suggests a correlation between these two types of fraud, possibly indicating that advancements in technology have facilitated the proliferation of fraudulent activities across different channels.

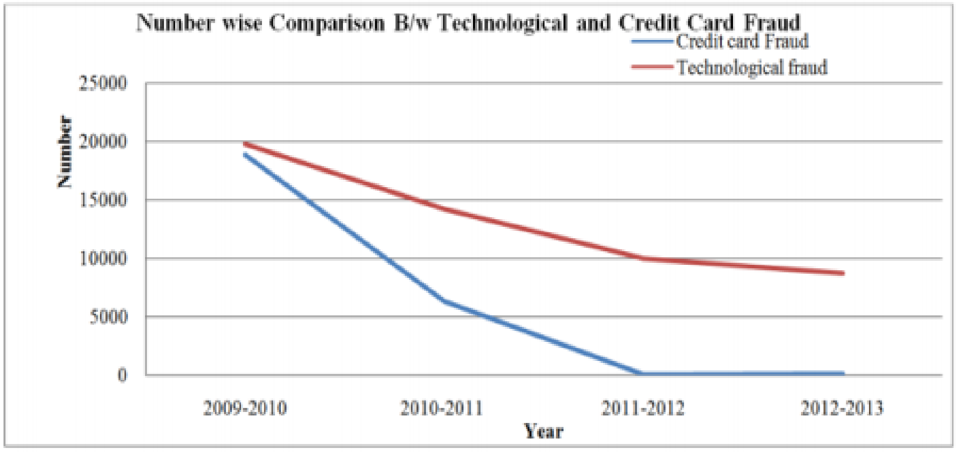


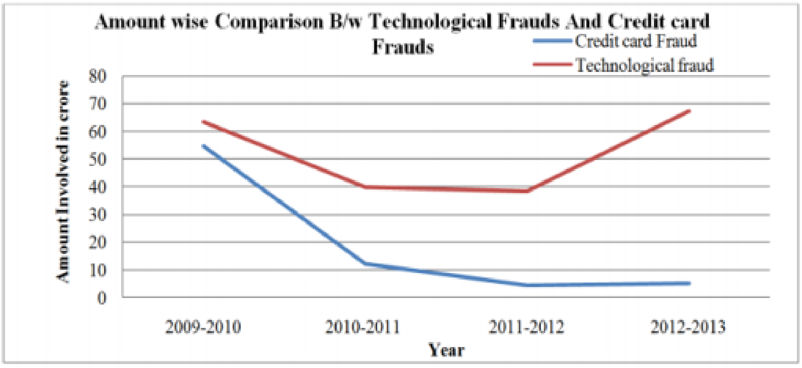
Fig . 5.4

Table 5.5 helps to make a comparison between the amount involved in credit card fraud and technological fraud.

Years	Credit card frauds (In Crore)	Technologies Frauds (In crore)

2009-2010	54.67	63.38
2010-2011	12.28	40.03
2011-2012	4.39	38.46
2012-2013	5.19	67.36

Fig. 5.5 facilitates the comparison between the amount involved in credit card fraud and Technological fraud.



Segment wise comparison

Table 5.6 reveals the comparison between public banks, private banks, and foreign banks.

Segment	2011	2012	2013
Public Bank	327	10	9
Private Bank	5274	13350	10895
Foreign Bank	3188	3908	6390

Fig. 5.6 allows for a comparative analysis of the three segments within the banking sector: Public Banks, Private Banks, and Foreign Banks. The data presented in this figure indicates that Foreign Banks and Public Banks exhibit a similar trend, while Private Banks demonstrate an opposite pattern.

This discrepancy can be attributed to the greater technological advancement of Private Banks compared to their counterparts. Notably, according to the second report of DNA, ICICI Bank was found responsible for nearly 62% of reported fraud cases (3304 out of 5319 cases) related to Phishing and KYC in the fiscal year 2010-11. This highlights the susceptibility of Private Banks, particularly technologically advanced ones like ICICI Bank, to fraudulent activities facilitated by advancements in technology.

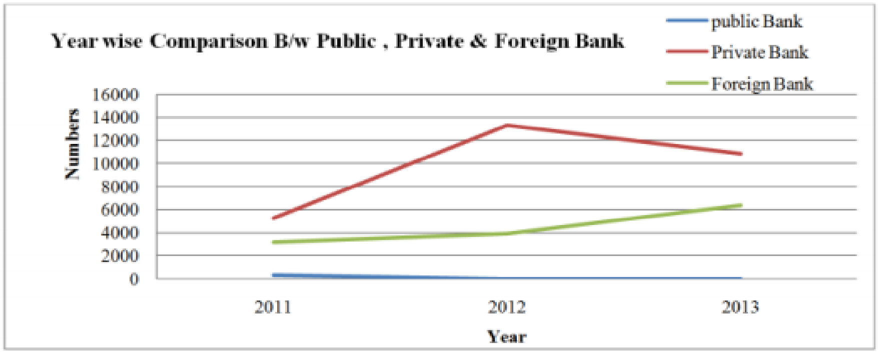
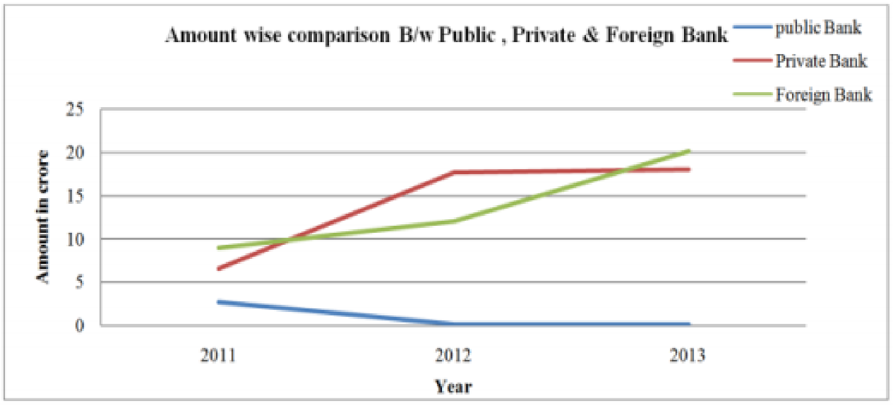


Fig. 5.6 Source: Rajya Sabha starred Question No.97, dated 04.03. 2008.
Table 5.7 reveals the comparison of amounts involved in credit card frauds between the public bank, private banks, and foreign banks.

Segment	2011	2012	2013
Public Bank	2.77	0.21	0.02
Private Bank	6.62	17.71	18.02
Foreign Bank	8.97	12.08	20.22

Fig. 5.7 makes the comparison between the amount involved in the credit card frauds among the public bank, private and Foreign Bank.



5. DATA ANALYSIS AND INTERPRETATION

Methods for preventing credit card fraud

Based on a review of the literature the following methods are useful for the prevention of credit card fraud.

5.1 A fusion of Dempster- Shafer theory and Bayesian Learning

This method employs a combination of three integrated approaches: rule-based filtering, Dempster-Shafer theory, and Bayesian learning, to differentiate between fraudulent and genuine transactions. Initially, the Dempster-Shafer rule is applied to a set of multiple pieces of evidence to establish the initial belief regarding incoming transactions. Bayesian learning then utilizes databases of genuine and fraudulent cardholders to update the suspicious score, making the Fraud Detection System (FDS) dynamic in adapting to changing behaviors. The architecture of this system is designed to be flexible, allowing for the addition of new rules or technologies at later stages as needed.

5.2 Probabilistic credit card fraud Detection system

In the online transaction method, a stepwise architecture is devised to develop a new model for credit card fraud detection. This approach involves simulating credit card transaction data, with approximately 3200 transactions simulated for training purposes and 800 transactions for assessing effectiveness, efficiency, and accuracy.

Evaluation of this method is conducted using various performance metrics, including true positive matrix, false positive matrix, accuracy, and the ROC Curve. Through optimized utilization of these performance parameters and improved algorithms, it is concluded that the probabilistic Posterior-Viterbi cum new fraud detection model outperforms the Viterbi cum old fraud detection model.

5.3 Advance Address Verification System

This method is the advancement of the address verification system. Under this method a system of multiple checks is developed namely, Lost/ Stolen Check (LS), Credit card Validation Check (Val), Security Code Check (SC), Expiry (Exp), Multiple IP (MIP), and Repeated IP (RIP).

5.4 Decision Tree

The decision tree technique for detecting and preventing fraud is notably straightforward and user-friendly. This method involves placing attribute names on the nodes and attribute values on the edges, with the leaves containing the intensity factor. Its simplicity makes it easy to implement and comprehend, making it an accessible option for fraud detection.

5.5 Clustering techniques

Cluster techniques are employed for detecting and preventing behavioral credit card fraud. These techniques utilize peer group analysis, wherein the system identifies accounts exhibiting behavior distinct from others, particularly when they repetitively display previous patterns. Such accounts are flagged as suspicious, prompting further investigation to mitigate potential fraudulent activities.

5.6 Neural Network

The neural network method is considered as the effective method for the detection & prevention of credit card fraud. A neural network usually involves a large number of processors operating in parallel that help in detecting fraudulent transactions.

5.7 Credit Verification Values

This method protects from offline credit card fraud as the physical possession of the card is necessary. It checks the 3-4 digit number embossed on the credit card. However, this technology is not useful in combating online credit card frauds such as phishing, fraudulent emails, etc.

5.8 Chip & PIN

Under this technology, new smart cards are issued by the banks. These cards consist of the EMV Chips and the PIN instead of the signature which proves that the customer is genuine.

6. RESULT AND DISCUSSIONS

The research paper provides a comprehensive examination of various methods for preventing credit card fraud, ranging from traditional techniques like Decision Trees to more advanced approaches like Neural Networks and Chip & PIN technology. These methods offer a comprehensive toolkit for detecting and preventing fraudulent activities, addressing both offline and online fraud scenarios.

The fusion of techniques, such as combining Dempster-Shafer theory and Bayesian Learning, offers a dynamic and flexible fraud detection system capable of adapting to evolving fraud patterns. Additionally, probabilistic models and advanced verification systems enhance accuracy and efficiency in identifying fraudulent transactions.

Clustering techniques offer a unique approach by detecting anomalies in transaction behavior, while neural networks leverage parallel processing to detect patterns indicative of fraud. Moreover, technologies like Credit Verification Values and Chip & PIN add layers of security to prevent unauthorized transactions.

In terms of discussion, the effectiveness of each method can be evaluated based on factors such as accuracy, efficiency, scalability, and adaptability to changing fraud patterns. Future research could focus on refining existing techniques, exploring novel approaches, and integrating multiple methods to create more robust fraud detection systems.

Overall, the research provides valuable insights into the diverse range of methods available for preventing credit card fraud and highlights the importance of implementing comprehensive fraud prevention strategies to safeguard financial transactions effectively.

7. CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion:

In conclusion, this research paper has provided a thorough exploration of various methods for preventing credit card fraud. By reviewing existing literature and methodologies, as well as analyzing trends in fraud incidents, the paper has shed light on the evolving landscape of fraud detection and prevention.

The study has demonstrated the effectiveness of a range of techniques, from traditional decision trees to more advanced neural networks and probabilistic models. Each method offers unique strengths in detecting and mitigating fraudulent activities, providing a multifaceted approach to fraud prevention.

Moreover, the research has highlighted the importance of staying proactive and adaptive in the face of evolving fraud tactics. As fraudsters continue to innovate, financial institutions and businesses need to leverage cutting-edge technologies and techniques to stay ahead of the curve.

7.2 Recommendations:

Based on the findings of this research paper, the following recommendations are proposed:

1. Integration of Multiple Techniques: Financial institutions and businesses should consider integrating multiple fraud detection techniques, such as neural networks, clustering, and advanced verification systems, to create more robust and comprehensive fraud prevention strategies.

2. Continuous Monitoring and Analysis: It is essential to establish continuous monitoring and analysis of transaction data to identify emerging fraud patterns promptly. Real-time monitoring allows for immediate intervention and mitigation of fraudulent activities.

3. Investment in Technology: Organizations should prioritize investment in technology infrastructure and resources to support sophisticated fraud detection systems. This includes leveraging artificial intelligence, machine learning, and big data analytics to enhance detection capabilities.

4. Customer Education and Awareness: Educating customers about common fraud tactics, phishing scams, and best practices for protecting their financial information can help mitigate the risk of fraud. Providing regular updates and reminders about security measures can empower customers to safeguard their accounts effectively.

5. Collaboration and Information Sharing: Collaboration between financial institutions, regulatory bodies, and law enforcement agencies is crucial for sharing information and intelligence about emerging fraud trends. Establishing robust networks for information sharing can strengthen collective efforts in combating fraud.

By implementing these recommendations, organizations can enhance their resilience against credit card fraud and better protect their customers from unauthorized transactions. Ultimately, proactive measures and collaboration are key to staying ahead of fraudsters and maintaining trust in financial transactions.

8. BIBLIOGRAPHY

[1] Panigrahi, S., Kundu, A., and Sural, S., "Credit Card fraud detection: A fusion approach using ", Elsevier Information Fusion, 10, 4, February 2009, pp. 354-363.
[2] Falaki S. O., Alses B. K., Adewale O. S., Ayeni, J.O., Aderounmu, G. A., “Probabilistic credit card fraud detection System in online transaction”, International Journal of Science Engineering and its Application, Vol 6, No 4, October 2012, pp 69-78.
[3] Anwer, R., Baig, S., Khiyal M. S. H., Khan, A., Khanum, M., “Online Credit card fraud prevention system for Developing Countries”, International Journal of Reviews in Computing, pp. 62-73
[4] Kathirvel, K., “Credit card Frauds and Measures to Detect and Prevent Them”, International Journal of Marketing, Finance & Management Research, Vol 2, No 3, March 2013, pp. 172-179
[5] Balan,Popescu, “Credit card Fraud”, The Annals of The “Stefan cel Mare” University of Suceava. Fascicle of the Faculty of Economics and Public Administration. Vol 11, No 1(13)2011, pp. 81 -85.
[6] Ramaki A. A. H., Asgari, R., Ebrahimi, R., “ Credit card Fraud Detection based On Ontology Graph”, International Journal of Security, Privacy and Trust Management, Vol 1, No 5, October 2012, pp 1-12.
[7] Ghosh S., Reilly D. L., “Credit card fraud Detection with a neural network”, Proceedings of Twenty Seventh Annual Hawaii International Conference on System Science: Information system: Decision Support and Knowledge-based System, Vol 3 pp. 621-630.
[8] Shrivastava A., Kundu, A., Sural S., “Credit card Detection with Hidden Markov Model”, IEEE transaction on Defendable and Security Computing. “Vol 5,, No 1, January – March 2008
[9] Delamaire, l., Abdou, H., Pointon, j., “Credit card fraud and detection technique: a review”, Banks and Banks System, Vol 4, No 2, 2009, pp. 53-68
[10] Kundu, A., Panigrahi, S., “BLAST- SSAHA Hybridization for credit card fraud detection”, IEEE Transactions on Dependable And Secure Computing, Vol 6, No. 4, October-December 2009, pp. 309-315.
[11] Kadam, N., Soni, S., Putambekar, D., “Credit card fraud Detection based on Profile and Previous transaction”, Indian Journal of Research, Vol. 2, No. 3, March 2013, pp.1-3.
[12] Suman, “Survey Paper on Credit Card Fraud Detection ”, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 3, No 3, March 2014.
[13] Prakash, A., Chandrasekar, C., “A Parameter optimized approach for improving credit card fraud detection.”, International Journal of Computer Sciences, Vol. 10, No1, January 2013, pp. 360- 366.
[14] Kumar, R., Raj, S., “Design & Analysis of Credit card fraud detection based on HMM”, International Journal of Engineering & Innovative Technology, Vol. 2 No. 3, September 2012, pp.
332- 334.
[15] Dheepa, V., Dhanapal, R., “Analysis of credit card fraud detection methods”, International Journal of Recent Trends in Engineering, Vol. 2, No. 3, November 2009. pp. 126-128.
[16] Dheepa, V., Dhanapal, R., “Behavioral-based Credit Card Fraud Detection Using Support Vector Machines”, ICTACT journal on Soft Computing, Vol 2, No 4, July 2012, pp. 391-397.
[17] Shabbir, S., A., Kannadasn, R., “An effective Fraud Detection System Using Data Mining technique”, International Journal of Scientific & Research Publication, Vol. 3, No. 5, May 2013, pp. 1-4.

[18] Chaudhary, K., Yadav, J., Mallick, B., "A review of fraud detection Techniques: Credit card", International Journal of Computer Applications, Vol 45, No. 1, May 2012, pp. 39-44.
[19] Ingole, A., Thool, R. C., "Credit card Detection using Hidden
Markov Model And its performance", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 6, June 2013, pp. 626-632.
[20] Chaudhary, K., Mallick, B., "Exploration of Data Mining Techniques In Frauds Detection: Credit Card", International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 3, pp. 1765-1771.