E-Commerce Frauds and the role of fraud Detection Tools in managing the risks associated with the frauds

Article · January 2020

CITATIONS
4

READS
9,211

1 author:

Dr Padmalatha N a
Dayananda Sagar Institutions
3 PUBLICATIONS **4** CITATIONS

SEE PROFILE

International Journal of Advanced Science and Technology
Vol. 29, No. 4s, (2020), pp. 38-46

E-Commerce Frauds and the role of fraud Detection Tools in managing the risks associated with the frauds

Dr Padmalatha N A
Assistant Professor, School of Commerce and Management Studies
Dayananda Sagar University Shavige Malleshwara Hills
Kumaraswamy Layout Bangalore 560 078
Contact details: drpadmalatha-socm@dsu.edu.in

Abstract

Driven by multiple drivers, a traditionally cash based society of India is adopting digital payments at an unprecedented speed and scale. This rapid adoption has in its wake, lead to increase in the types and scale of frauds. While building business around the digital technology, companies need to proactively address the need for identification and prevention of frauds. Given the scale of transactions and the sped at which transactions get completed, mere human intervention will be futile in overcoming the looming threats of frauds. The desired objective can only be achieved by deployment of the right tools for fraud identification and tools. Formulating the right processes, specific to the sector or nature of business operations, identification of the right tool for the purpose and taking advantage of technological developments like in memory computing, collaboration across businesses, big data analysis, machine learning etc., are the key factors to consider while formulating effective fraud detection/prevention strategies. Current fraud detection techniques, however, are far from accurate, can result in significant financial loses, inconvenience and dissatisfaction to customers. In this article an attempt has been made to find the technologies to address the fraud and steps of adopting the fraud detection and prevention technology. The objectives of the research paper are to find types of e- Commerce frauds and to develop the mechanism (process) and technologies used in detection and prevention of frauds in consumer transaction.

Keywords*: Fraud detection Technology, Online business, Ecommerce*

1. Introduction

India which is traditionally a cash-based society has been adopting cashless and digital payments at an unprecedented speed and scale. From Cash on delivery as the most preferred payment method to electronic payments has been a quick journey. The adoption of electronic payments is expected to accelerate further in the future. The rapid adoption of electronic payments is driven by multiple factors –

- The push by the government agencies and regulators for digital payment,
- The unprecedented increase in the usage of smart phones
- The rapid decline in the cost of mobile data
- The penetration of e-commerce to the hinterlands of the country.

The numbers behind these key drivers of change are indicative of the scale and speed of adoption.

- As per the reports of "The Future of Internet in India", by 2020, 50% of travel transactions are expected to be online and 70% of e-Commerce transactions would take place mobile phones.
- By 2020 (NASSCOM Report), the number of online shoppers is likely to cross 175 million. Demand for International consumer products will be growing faster than the domestic supply from authorized distributors and e-commerce offerings.
- As per the reports, India has an Internet users base of about 475 million as of July, 2019.This number has crossed 627 million by the end of 2019.
- The spread of e-Commerce has led to the rise of several niche players who largely specialize their products around a specific theme. Largest e-Commerce Companies in India are Flipkart, Amazon, Myntra, Paytm, and Snapdeal.
- Payment options for online shopping in India includes billing to mobile phones and landlines, cash on delivery, cheque, debit card, direct debit in some countries, electronic money, gift cards, wire Transfer/ Delivery on Payment, etc.

ISSN: 2005-4238 IJAST

While cash based economy had frauds mainly in theft of currency notes and counterfeiting of currency notes, the cash less economy has lead to frauds of different dimensions. As per TechARC's report, ecommerce contributed to 51% of total ad fraud in India through customer acquisition, engagement and retention Reports about online frauds in India highlight (Indian Railways November,2018) how Indian Railways deactivated 1,268 user IDs on IRCTC after forfeiting 1,875 scheduled e-tickets when it conducted raids against e-ticketing fraud in over 100 cities in the country. 1,875 scheduled e-tickets worth Rs 35 lakh were forfeited. There are reports (July2018) of how 37 people were allegedly duped on OLX by fraudsters by using leaked soft copies of Aadhaar and ID cards of CISF (central Industrial Security Force) and Army Personnel. This resulted in CISF and Army Personnel receiving several calls and complaint emails- questioning the integrity of the men in uniform.

While nature of frauds cover a wide spectrum of activities, the type of people who commit frauds also varies widely. Many a times the Fraud is committed by the employee acting alone, or in collusion with another party (a second employee) or a third party. Because of the availability information any person can collate the information about the company, its employees and clients in a damaging manner. A recent study by KPMG (India Fraud survey 2012), indicated that with the ever-increasing use of technology in every business, is inadvertently leading to more sophisticated and complete frauds than before.

2. The nature and implications of e-commerce frauds

Faced with enormous possibilities of frauds and the large consequences of such frauds, companies and businesses have started recognising that it is critical to assess the risks upfront and identify the possible points of frauds, instead of fighting to recover from the consequences of the frauds. Given the nature of operations, transactions and stake holders involved, any such effort has to be tool based. This research intends to assess this requirement and the trend.

Objectives of the research

- To study and analyse the types of e- commerce frauds
- To analyse the mechanisms (processes) used for fraud detection
- To analyse the technologies and the tools used for fraud detection and prevention of frauds in consumer transaction
- To formulate a framework to identify the right technologies and tools and assess the challenges in adoption of the technologies and tools

Research Methodology

This research is primarily conceptual in nature. The study tries to find the various types of factors such as types, mechanism used by organizations to prevent fraud and technologies trend related to Fraud Detection using the relevant literatures . Based on the information, the researcher has done an exhaustive study and developed the own insights. The present study is descriptive in nature.

Literature review

The article (Parr et al), mentions about the different aspects such as ways in which small business owners can combat the theft, ways of identifying week links, types of controls, types of restriction of activities. Even though author mentions that availability of tools for the specific requirement of business, the exact tools were not discussed. Machine learning as an important tool for solving business fraud is widely adopted. Automated fraud detection system is highly successful in solving the problem. Stages of machine learning and Models used were discussed in the article. (How machine learning facilitates fraud detection, 2019) . The article (Detecting financial fraud using machine learning, 2018) discusses about how to handle imbalanced data in machine learning. Depending on the data, the author has mentioned the use of techniques such as SMOTE (Synthetic Minority Over-sampling Technique), Random Under Sampler or SMOTE+ENN (Edited Nearest Neighbour) technique.

Peter Millar(2010, August 16), in his article ,"7 steps to jump start your anti-fraud program" mentions about the steps which are worth noting: Building profile of potential frauds; Test transactional data for possible indicators of fraud; Improve controls by implementing continuous auditing and monitoring; Communicate the monitoring activity throughout the organization; Provide management with

ISSN: 2005-4238 IJAST

immediate notification when things are going wrong; Fix any broken controls immediately; Expand the scope and repeat.

The key findings

Web platforms were more susceptible to frauds over app fraud because their digital teams were more likely to look at app fraud over web fraud. The web had higher chances of fake leads and keyword abuse over apps. Despite this, app fraud led to 85% of total digital ad fraud. Some of the interesting acts are:

- Video fraud is becoming more sophisticated to gain more on premium advertising channels as video consumption increases
- Both traditional and online marketers need to look at O2O (unclear if online to offline or otherwise) for ad fraud strategy.
- Companies with solutions for ad fraud are 'better equipped' to have higher user engagement because they can contain abuse

The top few fraud risks that have the potential to pose threats to businesses in India are the following:

- Data or information threat and IP infringement; Bribery and corruption
- Fraud penetrated by Senior Management
- Fraudulent disbursements (e.g. billing schemes, payroll schemes, expense disbursement schemes, check tampering);Vendor fraud or kickbacks
- Regulatory non-compliance; Theft or misuse of inventory; Misappropriation of assets(e.g. theft of cash or receipts)

Based on the research, some of the interesting observations related to ecommerce fraud types of frauds, in online industry are:

- The frauds are mainly executed by professional with knowledge - Young Professionals are potential fraudsters
- Small businesses with fewer than 100 employees are most susceptible to occupational fraud.
- Internet fraud is usually carried out by employees
- Over 90% of online fraud detection platforms use transaction rules to detect suspicious transactions.

The cost or loss due to frauds are growing significantly and indicate the enormity of the situation and the implications for the business and consumers.

- As per TechARC's report titled "India digital ad-fraud market" states that in 2018, ad fraud cost a total of $1.63 billion, contributing to 8.7% of the global fraud. The report states that Ecommerce contributed to over 51% of the total ad fraud in India, via customer acquisition, engagement and retention.
- As per the RBI reports, of more than 1.1 million people who reported fraud,21% had lost more than $63 million dollar from 2016. According to RBI data, of the total 53,334 cases of frauds during 2008-09 and 2018-19 fiscal years, involving Rs 2.05 lakh crore, a highest of 6,811 were reported by ICICI bank involving Rs 5,033.8 crore.

Current fraud detection techniques, however, are far from accurate, and can resulting significant financial loses, inconvenience and dissatisfaction to customers. With the effective use of Fraud detection technologies, losses can be reduced effectively. Today, a number of companies wanting to incorporate proactive fraud risk management in their companies at various stages in identification of fraud, identification of fraudster's relatives and close friends, collect evidence and interpretation.

3. The types of frauds, the process of detection and the tools for detection

The types of frauds carried out using electronic or digital transactions are manifold and keep evolving every day. However a careful analysis of the frauds indicates that the following are the most dominant types of frauds.

- **Identity theft:** Is the most common type of e-commerce fraud. Fraudster targets personal information such as name, addresses, e-mail addresses, credit card or account information. The personal information are used to carry out subsequent fraud.

- **Friendly Fraud:** Customers order goods or services and pay for them – preferably using a "pull" payment method like a credit card or direct debit. There are instances when they deliberately initiate a charge-back, claiming that their credit card or account details were stolen. The customers are reimbursed – but they keep the goods or services.
- **Clean Fraud:** A stolen credit card is used to make the purchase, but the transaction is then manipulated, in such a way that fraud detection function are circumvented.
- **Affiliate Fraud:** Affiliate process can be done either using a fully automated process or by getting real people to get into merchant's sites using fake accounts. This can be done by the fraudster by manipulating traffic or signup statistics.
- **Triangulation Fraud:** In this case, fraud is carried out via three ways. First, fraudster will have a fake online storefront, which offers high demand products at different process especially at extremely low prices. The user gives data related to credit card, and addresses, which is the main motive of the falsified storefront. Using the stolen credit card data and name collected, goods are collected and shipped to the original customer. The final point in the fraud triangle is making additional purchases using the stolen credit cards. Because of the unknown connect between order data and credit card numbers, it is almost impossible to connect. As a result, the fraud remains undiscovered for a longer period of time, resulting in greater damages.
- **Merchant fraud:** Merchant fraud is another method which must be mentioned. It's very simple: goods are offered at cheap prices, but are never shipped. The payments are, of course, kept. This method of fraud also exists in wholesale. It is not specific to any particular payment method, but this is, of course, where no-chargeback payment methods (most of the push payment types) come into their own.

The frauds can also be classified/analysed based on the nature of transaction and the specific instance of a process where the fraud takes place.

- Order placement Processing
  - Inflated MRP for the discounts
  - Unauthorized price change
  - Unauthorised/fake orders
  - Presence of black listed entities in the system (who tend to re-apply under a new name to register in the system) in the absence of adequate vendor due diligence
- Payment:
  - Credit/Debit Card fraud using stolen information
  - Payment gateway vulnerabilities (Hacking, Lack of authenticated credentials etc.)
  - Cash on delivery (non-receipt of payment, fraud by cash collection agent)
- System/Network Operations
  - Phishing fraud (Identity theft)
  - Intrusion/Cyber attacks (e.g. malware)
  - Pharming
  - System manipulation e.g. redemption of coupon even on cancellation of order, avail discount on expired coupons, order executed without payment)
- Returns and refunds
  - Counterfeit product returns
  - Return of used products
  - Tampering with product in order to return it
  - Customer initiates chargeback without returning the product

Pattern of Fraud as given by Association of certified Fraud examiner's Reports (ACEF), are

- Employee generated :This can be solved by background checks on employees when hiring, restrictions on employee activities, awareness in the organization
- Organization Generated: This can be prevented by having polices and procedures for using the organization's funds, Safeguarding assets and documents, promoting appropriate workflow
- Third Party generated: This can be prevented by safeguarding organization's data access, risk assessment techniques

ISSN: 2005-4238 IJAST

Based on the nature and intensity of the frauds the technology and the tool have evolved to address or overcome these specific frauds. These are used at different stages of a typical e-commerce fraud. Some of the key Fraud detection Technologies are

- **Identification of fraud:** Data across different period of time need to be analysed for identifying anomalies. However, new suppliers or new customer involved with the suspicious transactions may not be in the master data of the organization. Data analytics tools like SAP, CaseWare IDEA, etc. can be used to identify the anomalies.
- **Identification of fraudster's relatives and close friends:** The mobile phones and social networking applications such as Facebook, Twitter, WeChat, Instagram, WhatsApp provides an opportunity to observe interests, linking, lifestyle, characteristics etc. Social networking analysis tools, such as NodeXL, SVAT, Gephi, etc. could be deployed to achieve the same goal. Communication records can also be used to identify the reasons behind the crime.
- **Collection Evidence:** In a digital world, most all data are stored in cell phones, Servers, cloud systems. Forensic tools such as Encase or Helix can be the technological solutions for the same.
- **Interpretation:** In order to represent the trends tools such as Qlik, or tableau can be deployed.

Types of Fraud Detection Tools

- **Stand-alone Tools:** In order to combat frauds, new and up-to-date technology is absolutely necessary. It involves procedures to collect data, quick evaluation of the collected data, identifying activities, formulating patterns of fraudulent activities. Risk assessment analyses must also be performed to identify where the week links are. .
- **Software based tools:** Software for continuous monitoring of business transactions and for continuous monitoring of business communications
- **Assessment based tools:** These are tools used for assessment of historical transactions. These are tools for retrospective identification of fraudulent payments or other abusive activity
- **External analysis:** These are tools for analysis of public profiles, activities and public information from multiple publicly available sources for identification of unethical behaviour and are typically tools for social network analysis.
- **Analytical tools:** Technological advancements in data analytics such as link analysis, data visualization, predictive modelling and other analytic testing are usual tests to identify the anomalies.

4. Emerging Trends and framework for assessment/Adoption

The cost building processes and implementing the right tools to prevent fraud is far less expensive to business than the cost of fraud committed to business. Although obvious at the outset, this is the key understanding which has been driving the developments in the field of e-commerce. With digital transaction as the back bone, the mechanism to detect and prevent frauds is closely linked with the trends/developments in the field of Information Technology. Some of the key trends are

- It is a multi dimensional issue – involving IT, Processes and business need/environment.
- Analysis of data from multiple sources
- Real time analysis
- Tools based mechanisms
- Integration of fraud detection and prevention into the core or software/IT development
- Behavioural analysis
- Deployment of tools of big data/machine learning and Artificial Intelligence

These trends manifest in the way the fraud detection mechanisms, tools and processes are deployed and advanced within the business environments.

- **Background information as the back bone**: Once fraud is discovered, the first step was to build a basic background information understanding. In this aspect, it is necessary to comprehend a fraudster's relatives and close friends to establish his or her interpersonal relationships, then try to clarify the accomplice network. The prevalence of mobile phones and social networking apps such as Facebook, Twitter, WeChat,

ISSN: 2005-4238 IJAST

Instagram and WhatsApp provides investigators with a great opportunity to observe fraudsters' interests, lifestyle and characteristics. In addition, social networking analysis tools, like NodeXL, SVAT, Gephi, etc., could be deployed to achieve the same goal.

- **Assessment of the motives**: Social networking analysis tools and communication records could be adapted to accomplish this aim. Patterns of illicit behaviour also need to be grappled with. In this aspect, it is useful to compare different data across different periods to identify anomalies. For instance, the fact that new suppliers involved with the suspicious transactions are never presented in the company's client master data is a warning sign. Evidence of specific or unprecedented accounting subjects, such as temporary payments or account receivables factoring, are also red flags. Those anomalies could be identified via several data analysis tools like SAP, CaseWare IDEA, etc.
- **Collecting Evidence**: In a digital world, almost all data is stored on electronic devices, such as cell phones, computers, servers, cloud systems, etc. Thus, it is vital to gather digital evidence through proper devices to prevent them from being polluted, which might result in them being unable to be presented in court. In this regard, forensic tools such as Encase, FTK or Helix are certified and commonly employed by investigators.
- **Interpreting the information**: Lastly, it is requisite to summarise all the information and make an interpretation – a task which is traditionally completed by investigators. With the development of computer technology, some programmes, such as Qlik or Tableau, could be applied to comprehensively display trends and variables, so that the whole story can be seen.
- **Deployment of data Science:** Data scientists can solve fraud problem using machine learning and predictive analytics. It uses various algorithms to facilitate the machines to respond to different situations for which they have not been programmed explicitly. Advanced machine learning tools can automatically update its models to reflect the trends. With increased data set, machine learning models can pick similarities and differences between multiple behaviours. The advantages of machines for the fraud detection are speed, scale and efficiency.
- **Building multiple models:** The deployment of machine learning tools for fraud detection requires significant number of cases or large datasets to give an accurate judgement. Other challenges in this approach are high infrastructural costs, strict regulations and risk of replacing existing technology. The stages for using the machine learning fraud detection involves
  - Getting historical data
  - Building models for predicting fraud
  - Using the model for prediction.
- **Integration of systems and processes:** Even though advanced technology serves as great tool to combat fraud, the issue should be viewed as a combination of IT problem and business problem. The steps:
  - Putting a clear focus on segregation of duties(Spread and rotate financial responsibilities and financial control)
  - Offering internal and external audits (monthly profit and loss reviews, monthly balance sheet reviews)
  - Developing protocols for electronic banking transactions (e.g., limiting access, verbally confirming requests, two-step authentication process, safeguard data)

5. Framework for assessment and suggest possibilities of adoption

Thanks to the evolution of technology, fraud investigators can now conduct a thorough and complete audit of entire populations of transactions in a relatively short period. However what is critical is the use of the right technology for the purpose.

- **Nature of data to the right tool:** The business transactions of an enterprise and the source of information span multiple sources of data and multiple types of data. The data sources can be real time, offline or sourced from third parties. The data could be structured or/unstructured. So

understanding the source of data, the size of data and the nature of data and using this understanding to select the right tool is the key step in adoption of fraud detection tools.

- **High performance computing redefines the possible**: Today's high-performance analytics can rapidly analyze massive amounts of data using technologies such as grid computing, in-database analytics and in-memory analytics. Fraud analysts can now rapidly test multiple methods to determine which models work best. Speedier model development/testing means better models get deployed sooner, giving institutions more agile response to the flash fraud and zero-day threats that can manifest in online channels. The different types of models required for analysis, the ready availability of the models and the speed of analysis required to be carried out are the other set of parameters to be used for determining the tools or in building the system for fraud detection.
- **The need for data storage and size/growth of data:** Analytical insights can be delivered to visual interfaces and automated workflow systems. Imagine arming your investigative team with visualizations that clarify where to look, along with supporting detail about threats as they are developing, rather than days or weeks later. This makes the ability to analyse large sized data and analyse quickly almost in real-time and throw up insights or actionable outputs, as the key parameter for selection of a tool/system. For example tools like Hadoop brings high-performance data storage and processing to the fraud-fighting arsenal, operating on large clusters of commodity hardware. Hadoop makes it fast and affordable to support analytics processes that can find anomalies in millions of records.
- **Hybrid analytical techniques deliver richer insights:** By combining analytical approaches, one can detect and prevent more fraud with fewer false positives, protecting the firm while preserving the quality of the customer experience. This becomes an essential requirement while selecting or adopting a tool for fraud detection. Some of the key features of a hybrid model are:
  - Hybrid models can use firm's data at the core, consolidating data both internally and externally with a consortium model to create an even more predictive model.
  - The systems can detect variances that could indicate identity theft or malware.
  - Neural network models use machine learning to interactively learn from the data without human intervention, so the algorithms become smarter and more accurate with every iteration.
- **Behavioural analytics:** When it comes to white collar crimes like the ones seen in e-commerce transactions, behavioural analytics transcend rules-based systems: Fraudsters can easily out-manoeuvre rules-based systems, so it's essential to have adaptive analytics that can detect unknown risks and new ways of trying to break the bank. The features for adaptive analytics and ability to model behavioural patterns is one of the key developments being adopted in fraud detection/prevention. Some of the key features of this are:
  - A behavioural analytics approach captures behavioural patterns from every source and evaluates that information every time a transaction is scored.
  - Process to build a deep profile of the historical norm for an account, card holder, customer, merchant, POS terminal, device, web session, etc.
  - The more profiles available, the richer the understanding of whether a payment transaction or new product application is legitimate.
  - Identifying potentially fraudulent behaviour before a payment is made or a customer's account is compromised or a fraud is committed
- **Investigative workflow becomes more efficient:** Firms need to become more efficient in detecting, triaging and building investigations on suspicious activity. Deployment of an integrated work flow with key steps for investigation with different degrees of certainty/probability is another possibility. The fraud solution for such a requirement would have the following features:
  - Stage the data so transactions can be bridged to associated accounts and those accounts to parties – and if applicable, to households, corporate parents or other networked entities.
  - Aggregate work items for a subject, rather than require analysts to review separate work items. This reduces the number of widgets to be worked and gives analysts a more complete view of subject behaviour.

ISSN: 2005-4238 IJAST

  - Present the most meaningful information. Why are there events on this subject? Who are the players in these transactions? What is normal for them? Does this merit further investigation?
  - Automatically assemble alerts from multiple monitoring systems, prioritize higher-risk activities and auto-assign alerts to investigators based on the firm's unique rules and requirements.
  - A well-designed fraud solution will reduce queries to source systems, increase efficiency and provide governance through automated workflow for dual controls for investigation and filing of regulatory reports.
- **Financial institutions become crime-fighting partners**: The institutions especially in the financial sector are not isolated enteritis. It is important to partner with other entities to make the fight against frauds, more efficient and effective. Another key feature of the tools deployed for fraud detection and prevention is the ability of the tool to facilitate such collaboration. Establishing proactive intelligence units that source negative news events, referrals, case data, social media, consortium data and cyber events to detect previously unknown risks is facilitated by such tools. Deploying in-memory data architectures that enable sophisticated analyses such as global search, text mining, visualization, and network analysis to piece together clues from masses of disparate data is a key trend in the field.

6. Recommendations

Ecommerce frauds are becoming sophisticated and customers are consistently challenged by the sophistication of frauds. Degree of sophistication tends to be sectoral in nature. While some like IT, ITES and Financial services are more prone and vulnerable for frauds than the others; no entity is immune from frauds. Understanding the modulus operandi of the frauds and suggesting is not easy. Some of the suggestions are:

- **Stronger authentication**: Given the millennial generation's demand for convenience and frictionless commerce, the biggest challenge will be authenticating users without impeding the customer journey. Innovative fraud operations will find ways to tighten controls without inconveniencing users, perhaps through some combination of biometrics, near field communications and analytics.
- **More data for richer profiles:** Models and signatures will incorporate more data, such as from biometrics, consortia, interface devices, digital voice recordings and other novel sources. Information sharing among merchants and institutions will become more prevalent and efficient. We will continue to see convergence of cyber data with behavioural profiles for enhanced fraud detection.
- **High-performance fraud solutions**: Real-time prevention will be faster and scale to higher transaction throughput. More firms will implement fraud solutions that can correlate billions of daily transactions and enrich that data with business context and threat insights across the enterprise. In so doing, they will create smarter data that can be analyzed in many different combinations and peer groups – across products and organizational entities – to find anomalous behavior that could look innocuous in local context.
- **Usage of Integrated packages**: Expert System package FCI(Financial Crime Investigator), a package by Anthem Corporation, helps to identify fraud detection in purchase or in contracts. The user can write the query for fraud indication and then match the indicators to profiles of specific fraud schemes. The program generates detailed work plans, including further databases and on-line searches, designed to confirm or exclude each suspect scheme. These work plans also include information about what documents to review and what to look for, as well as who to interview and what to ask.

7. Scope for Further Research

The present study identifies various types of ecommerce frauds which is affecting any business organization. In order to combat business fraud effectively, it is important identify the prominent one which is the scope for further study. A number of fraud detection and prevention tools are available in

the industry and the research can be extended to identify the tool best suited to the challenges faced by a particular industrial/business ector to take care of the fraud.

8. Conclusion

In modern business, transactions takes place through a variety of payment channels such as credit /debit card, smartphones, kiosks, etc. At the same time fraudsters are becoming adept at finding weak links in the business transactions. Hence, detecting frauds is essential for any business. And, fraud detection is possible for banks and commercial industry with the advancement of technology. With the availability of increasing processing power, advancement in statistical modelling, ability to capture and store voluminous data organizations are adopting technology to detect fraud.

Bibliography

[1] Arbinder Singh, EY, "Changing face of fraud in India,
[2] Cindy Parr, CFE, is a senior auditor with Whittaker Cooper Financial Group, Certified Public Accountants and Consultants
[3] Keith M(2015, Feb 25), "How technology is shaping the fight against fraud", Inc.com , 22-Jan - 2020
[4] Kuo Ming Huang(2017, February), Fraud Prevention and Detection- Focus on the technological trend, Financier
[5] Rafael Piere, January 17,2018, Detecting financial fraud using machine learning: Winning the war against imbalanced data, Data Science
[6] Stu Bradley, David Sewart(n.d.) , "Five trends in fraud solution.", SAS
[7] (n.d.), How machine learning facilitates fraud detection, Maruthi Techlabs, Pvt Ltd., 2019
[8] Future of Internet in India, NASSCOM Report , 2020
[9] Indian Fraud Survey(2012), KPMG India Fraud Survey Report