

**INTERNATIONAL JOURNAL OF LAW**  
**MANAGEMENT & HUMANITIES**

**[ISSN 2581-5369]**

---

**Volume 5 | Issue 4**

---

**2022**

© 2022 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# The Multidimensional Banking Fraud Risks: Do Banks have the Necessary Resources?

---

SUGANDHA SHARMA<sup>1</sup> AND ASHUTOSH SHARMA<sup>2</sup>

## ABSTRACT

*COVID-19 came at a time when banks were finding it difficult to handle an upsurge in fraud instances. Though banks have not yet completely grasped the significance and effects of the present environment on matters related to fraud, it appears that the banks have accepted that the outbreak might result in an increase in frauds, according to Indian banking fraud survey, deloitte, 2022, there are 78% chances that frauds might climb over the next two years. Hence, the present article aims to comprehend how banks handle fraud risk, how new operational models affect fraud risk management, and ideas on future strategic investments with special reference to India. The findings of the research article will have an impact on the discussions and debates among banks, regulators, and practitioners about how to address (and reduce) the fraud and compliance risks that are now present in the environment.*

**Keywords:** *Fraud risk management, Banking sector, Early warning signal, Artificial intelligence, Machine learning.*

## I. INTRODUCTION

Banks were attempting to cope with a growing percentage of fraud cases when COVID-19 had been announced. In combating financial crime, banks faced a three-pronged "attack": more digital transactions, constantly updating regulatory rules, and new fraud tendencies. While banks are still learning about the insinuations and influence of the present climate on difficulties relating to fraud, with 78% of people believe that frauds might climb over the next two years (Indian banking fraud survey, 2022). It suggests that banks are accepting the possibility that the epidemic could cause a spike in frauds. There has been a significant push toward digitalization and financial inclusion during the past several years, making banking highly reliant on electronic channels for both customers and banks<sup>1</sup>. This has only grown more severe throughout the epidemic and is probably going to get worse.

Without a question, the pandemic's recent developments and technology breakthroughs will have a long-term effect on the banking sector. Furthermore, it is very possible that future

---

<sup>1</sup> Author is a Faculty Associate at ICFAI University, Dehradun, India.

<sup>2</sup> Author is an Assistant Professor at Uttaranchal University, India.

modifications to the way the banking sector functions will be necessary. Some trends have led to the identification of concerns, for instance, theft of data, cybercrime, third-party induced fraud, bribery and corruption, and bogus documents<sup>2</sup>. When compared to the earlier concerns like, dangers including data theft, bribery, and corruption have now taken Centre stage. These scam schemes have becoming more prevalent noticeably. Banks must take a deliberate initiative to be proactive by uncover the primary reason behind these fraudulent threats in response to a change in these trends so that they are better prepared for the future. For banks, the rise in cybercrime and data theft might be especially concerning since it could harm customer confidence and trust<sup>3</sup>.

## **II. IMPACT OF COVID-19 ON BANKING SECTOR**

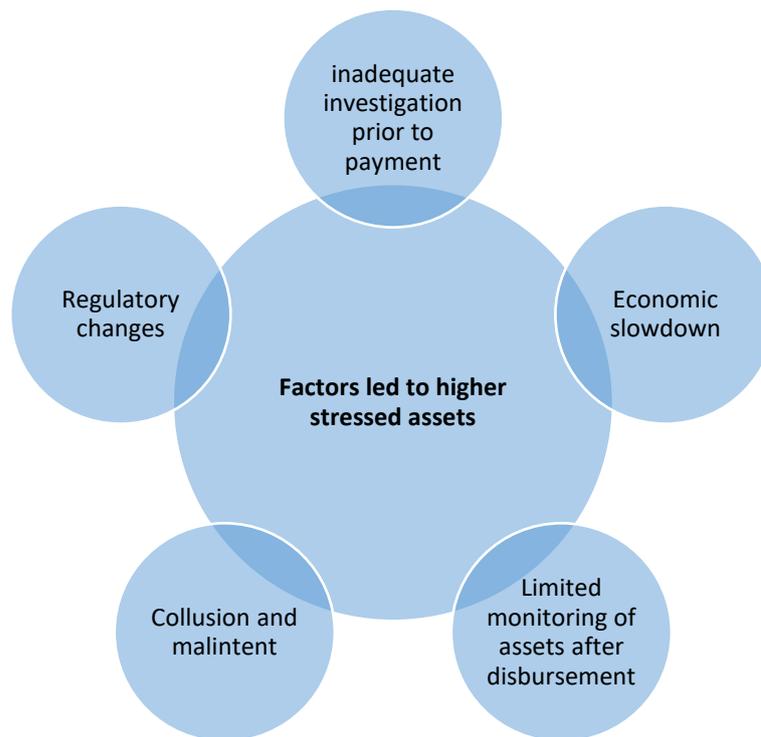
The Central Bank of India (RBI) and financial institutions were obliged to act in response to COVID-19's troublesome consequences. The Government of India and the RBI launched a wide range of steps in reaction to the pandemic and to aid in reviving the economy<sup>4</sup>. These included, to mention a few, the suspension of loan repayments, the temporary suspension of Insolvency and Bankruptcy Code (IBC) cases, and the restructuring of loans. The pandemic-related limitations required banks to adjust as well. Lockdowns and social conventions that forbid close contact with others limited bank employees' and clients' mobility, which increased use of digital platforms and other non-in-person bank facilities<sup>5</sup>. Banks required to give their workforce online accessibility to the network and data of their company since a sizable portion of bank employees worked from home. To prevent service disruptions, this compelled banks to implement considerable organizational and operational changes quickly; Is the vulnerability of all such alterations to fraud being evaluated? This is a troubling concern<sup>6</sup>.

Despite several variations being implemented at the front-end, procedures and systems may still be in place, have banks been impacted by undiscovered flaws? Due to the introduction of additional digital touchpoints for different contactless banking services and other banking-related activities, Banks must take the required actions to comprehend how these modifications would affect their capacity to detect fraud.

The government's MSMEs stimulus plan and the RBI freeze, in addition to fresh loans and loan extensions, are anticipated, according to industry analysts. While providing loans or renewing existing facilities, banks will need to exercise extra caution, weighing the strain on the account and the business's sustainability in light of the altered situation<sup>7</sup>.

In order to execute change quickly without compromising on risk management, banks will need to be nimbler given the pandemic's ongoing effects in several ways.

## **STRESSED ASSETS**



In spite of the pandemic's negative effects on some businesses, stressed assets remain a source of concern for banks. Banks should take into account a combined strategy that smears the findings of the pre-disbursement investigation to continued surveillance and spots abnormalities and red warnings in order to increase the overall efficacy of asset monitoring frameworks<sup>8</sup>. The amount of due diligence undertaken in this method must have accurate, thorough, and usable intelligence. Monitoring of Early Warning System EWS, novel fraud scenarios, and the integration of information gleaned from internal and external data sources are all necessary throughout the post-disbursement phase<sup>9</sup>.

### **III. CONTINUAL MONITORING AND FRAUD RISK MANAGEMENT AT BANKS**

Additionally, to a powerful and reliable Enterprise Fraud Risk Management (EFRM) system, a FRM function has to be successful, A bank ought to have a committed, autonomous team and a strong compliance culture. The three pillars of administration are reporting, identification, and investigation should be managed by the FRM department<sup>10</sup>. This involves establishing a reliable method for detecting fraud that incorporates information from teams working on scrutiny, credit monitoring, commercial, etc.; a pond of knowledgeable FRM generals; To prevent recurrence, scam must be reported, guidelines and processes improved, and danger registries promptly updated.

Banks can mitigate the effects of scam, therefore decreasing fatalities and preserving their

standing, with the assistance of a competent fraud risk management and monitoring department<sup>11</sup>. In addition to being able to anticipate new legislation and deal with developing fraud threats, it needs to be capable of preventing, detecting, and looking into a variety of fraud concerns.

### **The requirement for a separate FRM Department in banks**

There are several benefits to having a separate FRM department that reports to the bank's ED, MD, and CEO, including, the most crucial being conveying how vital top management believes the FRM function is. The avoidance of conflicts of interest when executing FRM tasks is a second benefit. It helps with the creation of new goods and services, procedure improvement, talent expansion, etc., by carrying in appropriately qualified personnel in a separate fraud risk management department<sup>12</sup>. A separate fraud risk management department can also assist in hastening the notification of senior management of frauds, especially those with high dollar amounts, and avoiding delays in decision-making<sup>13</sup>.

However, this is crucial to establish and enforce a fraudulent behavior-free culture inside the organization's DNA in addition to aligning the FRM unit. Setting the correct tone at the top can be facilitated by senior management's active participation and monitoring. Furthermore, top management must convey this message and show the essential concentration in order to establish a zero-tolerance culture<sup>14</sup>. Additionally, in accordance with the RBI1, the CEO of the bank, the board's special committee as well as the audit committee must be responsible for managing the risk of fraud, monitoring fraud, and conducting fraud investigations<sup>15</sup>.

### **Current state of anti-fraud program's implementation**

Increased reliance on logical techniques for scam monitoring and recognition has been the pandemic's most significant effect on fraud risk management activities. The use of data analytics in FRM might signal a change in the banking sector. The epidemic has led to a workforce shortage, a rise in contactless operations and services, and remote actions, which has increased the demand for FRM solutions that focus on data analytics<sup>16</sup>. This is demonstrated by the fact that 21% of respondents said that the pandemic would also lead to changes in their goal operating model that will improve the function's capacity for remote fraud-risk management<sup>17</sup>.

### **How does bank presently identify a fraud incident?**

- Through a client grievance
- Using software (EFRMS/EWS) for transaction monitoring or internal automated data analysis.

- During routine process reviews, account audits, and reconciliations
- Through an anonymous internal complaint or whistle-blower
- During a law enforcement agency's review

### **Proactive strategy to improve fraud risk management**

The following steps were taken by the bank to reduce fraud.

- Set up seminars and trainings to improve the abilities of the employees doing fraud monitoring duties.
- Implement video KYC for onboarding new customers and KYC updates.
- Use GPS or other technologies to electronically check the assets/collateral of clients.
- Demand that vendors and consumers utilize certain software and security precautions like encryption
- Improve Case Management Solutions to quickly and efficiently respond to fraud situations
- Utilizing AI/ML and integrating external datasets, improve current Early Warning System and Fraud Monitoring Systems to accommodate modern banking environments.

### **Investing in fraud risk management to increase resiliency and hasten efficiency**

In recent years, the Indian banking sector has emphasized the need of setting up fraud monitoring units or anti-fraud cells to conduct inquiries as well as to concentrate on preclusion and the prompt identification of suspected fraudulent behavior using fraud monitoring systems, etc. Though, taking into account the rising amount and frequency of frauds as reported in the Annual Report of RBI for FY 2020–21, the ability of fraud monitoring units to prevent and identify fraud looks to have a lot of room for improvement, allowing for a more thorough and proactive approach<sup>19</sup>.

In reality, the expert group on NPAs and scams, which was established under the leadership of Shri Y. H. Malegam, presented extracts of its recommendations in January 2020, according to the RBI. The suggestions include establishing a Market Intelligence Unit (MIU) to enhance FRM and adding a credit monitoring team to the bank to give inputs and insights during client activity monitoring, sanctioning, and assessment<sup>20</sup>.

Currently, the financial statements and bank transactions of a client serve as the foundation for the attentive definitions defined for fraud monitoring systems and EWS. However, MIU's inputs will assist spot and draw attention to warning signs including the existence of shell businesses,

comments from important suppliers or clients, the rationale for a variation in management or promoters, development on building locations, and levels of activity in a manufacturing<sup>21</sup>.

It is crucial to make sure that the forage the monitoring team sends to the MIU is correct and up to date in order to obtain timely and pertinent findings from the MIU<sup>22</sup>. For instance, the information provided to MIU to conduct checks on suspect individuals who have obtained payments from borrowers out of the bank loan need to be predicated on the most recent information accessible with the bank. Here, data analytics may be quite important in preventing financial loss by spotting probable fraud situations earlier than would otherwise be the case. Data analytics includes not only setting up pre-established alerting criteria but also spotting irregular activity patterns that change over time. The only way to achieve this dynamism is through utilizing AI and ML techniques<sup>23</sup>.

In order to manage fraud risk more effectively in the upcoming years, banks will need to integrate cutting-edge fraud recognition systems as well as combine AI with Big Data analytics to provide warnings that are more accurate and relevant. Banks and financial institutions will be able to monitor consumers during every phase of their lifecycle, from onboarding to settlement, by integrating these capabilities with the fraud risk management methodology<sup>24</sup>.

The existing conventional techniques of fraud detection suffer from a dearth of centralized control, a lack of FRM procedures that provide enough feedback, absence of risk-based supervision, an emphasis on finding rather than prevention, etc. EWS and FRM must be combined in order to transition to a proactive, agile future and create a strong and complete system<sup>25</sup>.

### **Fostering collaboration between multiple fraud risk monitoring technologies**

Banks across the industry use a variety of systems that carry out pre-set scenarios and create warnings, which might take early warning signs in their form, probable scam alerts, or doubtful alerts, suggesting behaviors related to money laundering<sup>26</sup>. However, the majority of institutions still observe these signals separately.

To create synergy and obtain a thorough understanding of consumers and their transactions, some banks have started to combine multiple alert monitoring solutions. Incorporation of signals need not imply that one team examines all warnings produced by different gears used by banks<sup>27</sup>. In order to increase synergy, it may be necessary to revisit the alert situations listed in different systems, align the Fraud Risk Management and Early Warning Signals teams, share data with the departments responsible for monitoring and checking of credit to proactively identify danger indications, provide the AML transaction monitoring staff with insightful

feedback, and, if necessary, report to the Financial Intelligence Unit<sup>28</sup>. For banks, combining their efforts would help them reach their ultimate goal of safeguarding their consumers from potential financial loss and boosting confidence among stakeholders.

The importance of having an efficient framework for monitoring fraud has increased as a result of a rise in fraud since our previous poll. Expectations of a rise in transaction volume as a consequence of government inducement are cause for concern<sup>29</sup>. Upgrading FRM resources is required in this respect, both in terms of their capabilities and strengths. To fill its FRM function with qualified personnel and ensure the development of data analytics capabilities in crucial areas like forensic audits, market intelligence, and EWS alert evaluations, the banking sector needs to find personnel with the necessary skill sets and expertise<sup>30</sup>. This requires the banking sector to spend strategically in areas such as skill development and training.

### **EWS and FRM must be improved using AI/ML**

Customers are increasingly using digital channels for transactions, which has helped to boost transaction speed and convenience<sup>31</sup>. On the other hand, as business models have changed and the use of technology has expanded, frameworks for managing fraud risk have faced more difficult problems. Because banking technology is constantly developing, human judgement and conventional transaction warning systems are no longer useful for quickly identifying fraud<sup>32</sup>.

The number of bank transaction datasets has rapidly expanded as a result of the massive daily increase in transactions brought on by the digitization of commercial activities. It's interesting to note that this data contains a number of insightful trends that might help detect fraud in the transaction activities of a certain consumer early on<sup>33</sup>. A sophisticated data analytics tool can comb through enormous amounts of information, collect and analyze intelligence from other sources, and spot linkages that are hidden and warning signs. As a result, banks will be able to proactively spot suspected fraudulent transactions before they take place<sup>34</sup>. Fraud risk assessment and detection may be done considerably more quickly and effectively by combining human judgement with machine learning algorithms (things these datasets can teach).

Presently, rule-based systems make up the majority of EWS and transaction monitoring systems that provide scam warnings. The transaction is flagged for additional examination when a specific threshold is exceeded, specific requirements are satisfied, or a recurring event is discovered. The amount of "wrong positives"— transactions that are flagged as perhaps suspicious yet turn out to be legitimate —is one operational problem of classic Early Warning Signals and fraud alert monitoring systems with specified thresholds/constraints<sup>35</sup>. For banks,

following up on and looking into such false positives may be an extremely time- and money-consuming task. Nevertheless, the present system may develop the capacity to identify actual abnormalities more effectively, with lower levels of false alarm, by conducting reviewing test results on a regular basis and incorporating lessons learned into monitoring systems<sup>36</sup>.

#### **IV. SUGGESTIONS**

AI approaches may be utilized to decrease false positives, identify real positives, and discover new trends in order to get better outcomes. By focusing on uncommon items based on factors the model is aware of, anomaly detection algorithms are specifically designed to spot fraudulent transactions. Implementing this use case requires involvement from the risk, compliance, and business teams in addition to intelligence acquired from outside sources.

Furthermore, banks can employ empirical studies and data segmentation to build bespoke criteria and detect traits unique to each peer group. For instance, because individuals with high net worth frequently make substantial transactions, they might need different criteria than those with smaller incomes<sup>37</sup>. The procedure of alert configuration allows banks to ascertain whether threshold levels should be raised if too many false alerts are generated or lowered if suspicious behavior is being overlooked. The manner banks carry out fraudulent checks and keep track of their operations may be changed with the use of advanced statistics<sup>38</sup>. Considering the massive amounts of data created by banks, identifying unethical activity might not be as precise as anticipated and may require longer resources and time without applying correct data interrogation tactics, properly utilizing all the information sources that are available—both external and internal<sup>39</sup>.

The existing conventional techniques of detecting fraud suffer from a dearth of centralized control, a lack of FRM procedures that provide enough feedback, a lack of risk-based monitoring, an emphasis on detection rather than prevention, etc. EWS and FRM must be combined in order to transition to a proactive, agile future and create a strong and complete system.

#### **V. CONCLUSION**

Although there has always been risk in the banking industry, institutions must immediately put strong, efficient, and effective control systems in place given the present growth in fraud tendencies. Various banks have increased their spending in upgrading their FRM frameworks, monitoring systems, and controls during the past few years; It seems, nevertheless, that their attempts have fallen short. The existing compartmentalized strategy to managing fraud risk will

no longer work. Banks should take a variety of precautions to safeguard their operations from fraudsters looking to take advantage of the epidemic while they navigate these extraordinary times.

Review the rules and situations to reflect the "new normal." This will guarantee that neither new patterns or fraud tendencies are ignored, nor that banks be overrun with notifications about clients whose behavior has considerably altered, such as payment flows that have changed significantly as a result of reconfigured supply chains. Banks need to devote attention to evaluate the efficacy, relevance, and the effectiveness of present controls in comparison to a new risk assessment in light of the numerous authorities issuing guidance globally. Banks may assist guarantee that there are connections between risk typologies and the control architecture by conducting regular, timely, and updated risk assessments.

Consider the methods and technologies employed to stop, watch for, and identify financial crime. By using innovation, the appropriate balance between risk management and effectiveness/efficiency may be achieved, through utilizing Artificial Intelligence and Machine Learning is a major problem for banks handling their regulatory requirements. Banks will be well-positioned to handle any upcoming crises if they choose to respond in a way that the public, regulators, and investors will continue to be interested in.

\*\*\*\*\*

**VI. REFERENCES**

- [1] Abhishek Sinha, "Fraud Risk Management in Banks: An Overview of Failures and Best Practices," *Money Laundering and Terrorism Financing in Global Financial Systems*, IGI Global.
- [2] Boateng, Akwasi A. and Boateng, Gilbert O. and Acquah, Hannah, A Literature Review of Fraud Risk Management in Micro Finance Institutions in Ghana (June 30, 2014). *Research Journal of Finance and Accounting*, Vol. 5, No. 11, 2014.
- [3] Repousis, S., Lois, P. and Veli, V. (2019), "An investigation of the fraud risk and fraud scheme methods in Greek commercial banks", *Journal of Money Laundering Control*, Vol. 22 No. 1, pp. 53-61.
- [4] Leo, Martin, Suneel Sharma, and K. Maddulety. 2019. "Machine Learning in Banking Risk Management: A Literature Review" *Risks* 7, no. 1: 29.
- [5] Zhang, Y. (2012), "Documentary letter of credit fraud risk management", *Journal of Financial Crime*, Vol. 19 No. 4, pp. 343-354.
- [6] Mwangi, S. W., & Ndegwa, J. . . (2020). The Influence of Fraud Risk Management on Fraud Occurrence in Kenyan listed Companies. *International Journal of Finance & Banking Studies* (2147-4486), 9(4), 147–160.
- [7] Alazzabi, W.Y.E., Mustafa, H. and Karage, A.I. (2020), "Risk management, top management support, internal audit activities and fraud mitigation", *Journal of Financial Crime*, Vol. ahead-of-print No. ahead-of-print.
- [8] Sunil S Mhamane, L.M.R.J Lobo, "Internet banking fraud detection using HMM", 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), pp.1-4, 2012.
- [9] Hwang, TK., Chen, WC., Chiang, WC., Li, YM. (2022). Machine Learning Detection for Financial Statement Fraud. In: Rocha, A., Adeli, H., Dzemyda, G., Moreira, F. (eds) *Information Systems and Technologies. WorldCIST 2022. Lecture Notes in Networks and Systems*, vol 469. Springer, Cham.
- [10] Arora, D., and Agarwal, R. (2009). *Banking Risk Management in India and RBI Supervision*. Retrieved on 10 September 2021, from
- [11] Association of Certified Fraud Examiners. (ACFE). (2020). *Survei Fraud Indonesia 2019*. Jakarta: ACFE Indonesia Chapter.

- [12] Clintworth, M., Lyridis, D. & Boulougouris, E. Financial risk assessment in shipping: a holistic machine learning based methodology. *Marit Econ Logist* (2021).
- [13] Dundulienė, R. Alzbutas and K. Baltrušonė, "Trade risk identification and prediction using experts' knowledge and machine learning," 2021 IEEE International Conference on Technology and Entrepreneurship (ICTE), 2021, pp. 1-5, doi: 10.1109/ICTE51655.2021.9584575.
- [14] Beatty, A., Chamberlain, S. L., Magliolo, J. (1995). Managing financial reports of commercial banks: The influence of taxes, regulatory capital, and earnings. *Journal of Accounting Research*, 33(2), 231–261.
- [15] Al Mazrouei, Fatima and Nobanee, Haitham and Nobanee, Haitham, *Machine Learning in Finance: A Mini-Review* (February 16, 2020).
- [16] Khoa, B.T., Anh, H.N., Ly, N.M., Truong, N.X. (2022). A Study on Buying Attitude on Facebook in the Digital Transformation Era: A Machine Learning Application. In: Nanda, P., Verma, V.K., Srivastava, S., Gupta, R.K., Mazumdar, A.P. (eds) *Data Engineering for Smart Systems. Lecture Notes in Networks and Systems*, vol 238. Springer, Singapore.
- [17] Bansal, A., Singh, S. (2021). Implication of Machine Learning Models Toward Education Loan Repayment Rate Analysis. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Ganzha, M., Rodrigues, J.J.P.C. (eds) *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems*, vol 203. Springer, Singapore.
- [18] <https://www2.deloitte.com/in/en/pages/finance/articles/india-banking-fraud-survey-edition-IV-2021.html>
- [19] Roy, N.C. and Basu, S. (2021), "Bank's battle against insider frauds ignitors and mitigators: an emerging nation experience", *Journal of Facilities Management*, Vol. 19 No. 4, pp. 437-457. <https://doi.org/10.1108/JFM-04-2020-0021>
- [20] Murthy, N. and Gopalkrishnan, S. (2022), "Creating a Nexus between Dark Triad Personalities, Non-Performing Assets, Corporate Governance and Frauds in the Indian Banking sector", *Journal of Financial Crime*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/JFC-05-2022-0097>
- [21] Chhabra Roy, N. and Prabhakaran, S. (2022), "Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach", *Journal*

- of Financial Crime, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/JFC-12-2021-0274>
- [22] Boubakri, N., Cosset, J. C., Fischer, K., Guedhami, O. (2005). Privatization and bank performance in developing countries. *Journal of Banking & Finance*, 29(8–9), 2015–2041.
- [23] Kumari, P., Pattanayak, J. K. (2017). Linking earnings management practices and corporate governance system with the firms' financial performance: A study of Indian commercial banks. *Journal of Financial Crime*, 24(2), 223–241.
- [24] Pennathur, A. K., Subrahmanyam, V., Vishwasrao, S. (2012). Income diversification and risk: Does ownership matter? An empirical examination of Indian banks. *Journal of Banking & Finance*, 36(8), 2203–2215.
- [25] Thakur, J. (2021). Artificial Intelligence in Indian Banking Sector. SPAST Abstracts, 1(01). Retrieved from <https://spast.org/techrep/article/view/465>
- [26] V. Dheepa and R. Dhanapal, "Analysis of credit card fraud detection systems", *International Journal of Recent Trends in Engineering*, Vol. 2, No. 3, pp. 126-128, 2009.
- [27] "Credit Card Fraud Detection Using Hidden Markov Model" By Abhinav Srivastava, Amlan Kundu, Shamik Sural. *IEEE Transaction*, January-March 2008.
- [28] M. Syeda, Y.Q. Zhang, Y. Pan, "Parallel granular neural networks for fast credit card fraud detection", *Proceedings of the IEEE International Conference on Fuzzy Systems*, 2002, pp. 572–577.
- [29] Meha Agarwal. (2019). How will artificial intelligence change the banking industry? Retrieved from: <https://inc42.com/features/how-will-artificial-intelligence-change-the-banking-industry/> on 20.12.2019.
- [30] R.C. Chen, M.L. Chiu, Y.L. Huang, L.T. Chen, "Detecting credit card fraud by using questionnaire responded transaction model based on support vector machines", *Proceedings of the Fifth International Conference on Intelligent Data Engineering and Automated Learning*, vol. 3177, October 2004, pp. 800– 806.
- [31] Agarwal, P., 2019, March. Redefining Banking and Financial Industry through the application of Computational Intelligence. In *2019 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-5). IEEE.

- [32] Castelli, M., Manzoni, L. and Popovič, A., 2016. An artificial intelligence system to predict quality of service in banking organizations. *Computational intelligence and neuroscience*, 2016
- [33] Aashish Chandorkar, Kamal Misra, (2019). How the financial services industry in India is set for a makeover. Retrieved from : <https://www.financialexpress.com/industry/how-financial-services-industryin-india-is-set-for-ai-makeover/1723836/> on 26.12.2019.
- [34] Ashish Anantharaman, (2019). How artificial intelligence is enabling financial inclusion in India. Retrieved from:<https://yourstory.com/2019/05/artificial-intelligence-enabling-financial-inclusion> on 23.12.2019.
- [35] Ayushman Baruah. (2019). AI applications in the top 4 Indian banks. Retrieved from : <https://emerj.com/ai-sector-overviews/ai-applications-in-the-top-4-indian-banks/> on 24.12.2019.
- [36] Dhanabalan T, Subha K, Shanthi R, & Sathish A. (2018). Factors influencing consumers car purchasing decision in Indian automobile industry, *International Journal of Mechanical Engineering and Technology*, 9(10): 53–63.
- [37] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, “Credit card fraud detection using Bayesian and neural networks,” *Interactive image-guided neurosurgery*, pp.261-270, 1993.
- [38] Dhanabalan, T. & Sathish, A. (2018). Transforming Indian industries through artificial intelligence and robotics in industry 4.0., *International Journal of Mechanical Engineering and Technology*, 9(10): 835–845.
- [39] Dhanabalan, T. & Rajamohan, S. (2014). Impact of Mahatma Gandhi national rural employment guarantee scheme in Dindigul district, Tamilnadu. *International Journal of Entrepreneurship & Business Environment Perspectives*, 3(4): 1422.

\*\*\*\*\*