

Exploring Bank Managers' Attitudes and Awareness of Forensic Accounting

CA Hardik Patwa, Dr. Purvi Derasari

Research Scholar, Parul Institute of Commerce, Parul University, Gujarat

Professor and Academic Head, Parul Institute of Management & Research, Parul University, Gujarat

Abstract:

This study delves into the perceptions and knowledge of bank managers regarding the field of forensic accounting in the banking industry. In an era marked by an increasing need for financial transparency and the prevention of financial malpractice, understanding the perspectives of key stakeholders, such as bank managers, is paramount. The research objectives of this study encompass two primary aspects. Firstly, it aims to investigate the perceived challenges and opportunities associated with the implementation of forensic accounting in the banking sector. This inquiry sheds light on the practical aspects of integrating forensic accounting practices into the banking industry and seeks to identify potential roadblocks and advantages. Secondly, the study endeavors to analyze the level of awareness among bank managers concerning the concept and the myriad benefits that forensic accounting brings to the table. This aspect is crucial in understanding the extent to which bank managers are cognizant of the role that forensic accounting plays in bolstering financial integrity. The sample size for this research comprised 100 bank managers. These participants were engaged through structured questionnaires and interviews to gauge their levels of awareness and understanding regarding forensic accounting. The findings of this study contribute to an enhanced comprehension of the attitudes and awareness of bank managers in relation to forensic accounting, thereby shedding light on the potential areas for improvement and integration of this critical discipline in the banking industry.

Keywords: Forensic Accounting, Financial, Fraud, Bank

I. Introduction

Forensic Accounting

Forensic accounting is a highly specialised domain within the subject of accounting that employs the principles of accounting, procedures of auditing, and investigative abilities to detect and expose instances of financial crimes and fraudulent activities. The process entails the examination of financial transactions and records with the objective of identifying potential instances of fraudulent acts, followed by the provision of evidentiary support in legal procedures, if deemed required. Forensic accounting is a fundamental instrument in the combat against white-collar crime, and it assumes a pivotal function in upholding the integrity of financial institutions. The demand for forensic accounting has witnessed a substantial surge in recent years, mostly driven by the escalating intricacy of financial transactions and the expanding reach of worldwide commercial operations. The proliferation of technology has concurrently given rise to novel opportunities for fraudulent operations and financial crimes, hence augmenting the challenges associated with their detection and prevention. Forensic accountants employ a blend of conventional auditing methodologies and cutting-edge technologies in order to examine financial crimes and instances of fraud. Forensic accounting finds application in several scenarios, encompassing fraud investigations, legal support, insurance claims, and bankruptcy proceedings. In the realm of fraud investigations, forensic accountants are tasked with the examination of financial transactions, the interrogation of witnesses, and the gathering of evidence in order to ascertain the presence or absence of fraudulent acts. Within the field of litigation support, forensic accountants play a crucial role by providing assistance in the computation of damages, the preparation of financial reports, and the provision of expert testimony during legal proceedings. Maintaining objectivity and independence is considered a crucial element in the field of forensic accounting. In order to ensure the integrity of their findings, forensic accountants are required to maintain impartiality and refrain from engaging in conflicts of interest, given that their conclusions may be utilised as evidence in legal actions. In addition, it is

imperative for them to adhere to rigorous ethical principles and uphold the principles of confidentiality, given that the material they are entrusted with frequently pertains to matters of sensitivity and confidentiality.

Forensic accounting necessitates a set of essential competencies, namely robust analytical and problem-solving aptitudes, meticulousness, and effective communication skills to convey intricate financial data to individuals without financial expertise. In addition to possessing a robust comprehension of accounting principles and auditing methodologies, forensic accountants are required to possess a comprehensive understanding of pertinent laws and regulations. Forensic accounting is a pivotal instrument in the combat against financial crime and fraud, and it assumes a vital function in upholding the integrity of financial systems. The escalating intricacy of financial transactions and the globalised nature of commercial operations have heightened the imperative for forensic accounting to an unprecedented degree. Forensic accountants play a crucial role in safeguarding the integrity of the financial system and fostering openness and accountability within the realm of business through their efforts to expose instances of financial crimes and fraud.

Forensic Accounting In Banking Industry

In recent years, there has been a substantial growth observed in the banking sector of India, wherein both public and private sector banks have actively engaged in competition to acquire a larger market share. The heightened intricacy of financial transactions and the global expansion of business have concurrently engendered novel prospects for fraudulent activities and financial misconduct within the banking industry. Inside this particular environment, the utilisation of forensic accounting has become a crucial instrument for the identification and mitigation of financial offences inside the banking sector. Forensic accounting assumes a pivotal function within the banking sector of India as it contributes to the preservation of financial system integrity and the identification of fraudulent practises. Forensic accountants within the banking sector are engaged in a diverse range of responsibilities, encompassing activities such as conducting investigations into fraudulent activities, evaluating risks, and performing audits to ensure adherence to regulatory requirements. Additionally, they may contribute to the formulation of anti-fraud policies and protocols, as well as deliver training sessions to bank personnel regarding the prevention of fraudulent activities. Fraud in loan disbursal is a significant concern for forensic accountants operating inside the banking industry. Loan fraud is a substantial issue in the Indian context, necessitating the indispensable involvement of forensic accountants in the identification and mitigation of such fraudulent activities. Forensic accountants are capable of conducting an analysis of loan applications and associated documentation, ascertaining the legitimacy of collateral, and detecting any indicators of potential fraudulent behaviour. The detection of money laundering is an additional domain within the financial industry where forensic accounting plays a crucial role. Money laundering is a pervasive issue on a global scale, with financial institutions frequently serving as a channel for the illicit transfer of funds. Forensic accountants employed within banking institutions employ a range of methodologies, such as data analytics and pattern recognition, to discern potentially illicit activities and subsequently communicate their findings to the appropriate regulatory bodies. Forensic accounting also serves a crucial function in assuring adherence to regulatory obligations within the financial sector. In the Indian context, banks are subjected to a multitude of rules and guidelines, which necessitate strict adherence in order to uphold the integrity of the financial system. Forensic accountants can provide support in conducting compliance audits, detecting instances of non-compliance, and proposing appropriate remedial actions to rectify these concerns.

ii. Literature Review

Bajaj and Vashisht (2020) conducted a study that investigates the utilisation of forensic accounting as a means of identifying instances of money laundering within the Indian banking sector. The authors suggest that money laundering represents a pervasive issue on a global scale, with institutions frequently serving as a medium for the illicit transfer of monies. The authors underscore the need of employing data analytics and pattern recognition techniques in order to detect and then report potentially illicit transactions to the appropriate governing bodies.

Bhattacharya and Biswas (2017) contend that forensic accounting assumes a pivotal function in the identification and mitigation of fraudulent activities inside the financial sector. The survey undertaken by the authors focused on forensic accountants in India, revealing their involvement in a diverse range of duties such as fraud investigations, risk assessments, compliance audits, and policy creation. The writers additionally underscore the significance of upholding independence and objectivity within the field of forensic accounting in order to guarantee the credibility and reliability of the findings.

Choudhury and Jha (2018) conducted a study that investigates the impact of forensic accounting on the reduction of operational risks within the banking industry of India. The authors suggest that operational risks, encompassing technology risks, human mistake, and internal fraud, pose substantial issues within the banking sector. The research indicates that the application of forensic accounting has the potential to effectively detect, evaluate, and minimise operational risks through the establishment of strong internal control mechanisms, the execution of risk evaluations, and the oversight of adherence to regulatory obligations.

In a recent scholarly investigation conducted by Kumar and Kumar (2019), an examination was undertaken to explore the significance of forensic accounting in mitigating instances of financial statement fraud within the Indian banking industry. The authors believe that forensic accounting possesses the capability to scrutinise financial accounts in order to identify any instances of anomalies or discrepancies. This study emphasises the significance of employing forensic accounting methodologies, including ratio analysis, trend analysis, and benchmarking, for the purpose of detecting instances of financial statement fraud within the banking industry.

In a separate investigation conducted by Shukla and Garg (2018), the researchers examine the application of forensic accounting techniques for the purpose of identifying instances of loan fraud within the Indian banking sector. The authors posit that loan fraud poses a substantial challenge in India, and assert that the implementation of forensic accounting might serve as a pivotal measure in identifying and mitigating such fraudulent activities. The significance of conducting a thorough analysis of loan applications and associated papers, as well as validating the legitimacy of collateral, and detecting potential indicators of fraudulent behaviour, is emphasised by the writers.

Misra and Panda (2020) conducted a study to examine the significance of forensic accounting in upholding regulatory adherence within the Indian banking sector. The authors believe that banks operating in India are subjected to a multitude of laws and norms, and adherence to these stipulations is of paramount importance in upholding the soundness and credibility of the financial system. The significance of compliance audits is emphasised by the writers, who also propose strategies to effectively address instances of non-compliance.

Singh and Gupta (2017) conducted a study that investigates the significance of forensic accounting within the Indian banking industry for the purpose of fraud detection and prevention. The authors believe that forensic accounting possesses the capacity to conduct a thorough examination of financial transactions and accounting records, hence enabling the detection of potential hazards associated with fraudulent activities. The research indicates that the application of forensic accounting methodologies, including data analysis, interviews, and document examination, can serve as effective means to detect instances of fraudulent activities within the banking industry.

Yadav and Gupta (2019) conducted a study that examines the influence of forensic accounting on corporate governance within the Indian banking industry. This study posits that the utilisation of forensic accounting can significantly contribute to the augmentation of transparency, accountability, and integrity within the banking industry. The research indicates that the utilisation of forensic accounting has the potential to facilitate the detection and deterrence of fraudulent behaviours, fortify internal control frameworks, and augment the overall efficacy of corporate governance mechanisms within the banking industry.

iii. Research Objectives

1. To investigate the perceived challenges and opportunities associated with the implementation of forensic accounting in the banking sector

2. To analyse the level of awareness among bank managers regarding the concept and benefits of forensic accounting

Iv. Sample Size

The study's sample size consisted of 100 bank managers who were questioned in order to assess their degree of awareness pertaining to the concept and advantages of forensic accounting.

V. Data Analysis

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am aware about Frauds done by compromising credentials through Search Engines results.	-30.804	99	.000	-1.064	-1.13	-1.00
I am aware of debit/credit card frauds.	-80.688	99	0.000	-1.548	-1.59	-1.51
I am aware of fake websites offering instant payment apps.	-64.080	999	0.000	-1.394	-1.44	-1.35
I am aware of frauds using screen sharing applications or remote sharing applications.	-40.026	99	.000	-1.184	-1.24	-1.13
I am aware of identity theft.	-57.301	99	0.000	-1.363	-1.41	-1.32
I am aware of juice jacking frauds.	-4.442	99	.000	-.184	-.27	-.10
I am aware of Mobile malwares.	-44.382	99	.000	-1.259	-1.31	-1.20
I am aware of online P2P lending applications, Fake advertisements for extending loans by fraud.	-45.049	99	.000	-1.322	-1.38	-1.26
I am aware of OTP Frauds.	-117.074	99	0.000	-1.809	-1.84	-1.78
I am aware of phishing fraud.	-97.604	99	0.000	-1.635	-1.67	-1.60
I am aware of point-of-sale fraud.	-44.146	99	.000	-1.218	-1.27	-1.16

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am aware of QR code scan frauds.	-45.740	99	.000	-1.252	-1.31	-1.20
I am aware of Ransomware threats.	-69.280	99	0.000	-1.565	-1.61	-1.52
I am aware of SIM cloning frauds.	-74.233	99	0.000	-1.431	-1.47	-1.39
I am aware of SMS based fraud.	-99.126	99	0.000	-1.731	-1.77	-1.70
I am aware of the ATM card skimming process.	-93.570	99	0.000	-1.553	-1.59	-1.52
I am aware of the Denial-of-service attack frauds.	-10.011	99	.000	-.406	-.49	-.33
I am aware of the internationalized domain name IDN Homographic attacks.	-8.202	99	.000	-.330	-.41	-.25
I am aware of the online KYC verification fraud.	-67.377	99	0.000	-1.476	-1.52	-1.43
I am aware of the Trojan malwares.	-24.221	99	.000	-.914	-.99	-.84
I am aware that accessing personal email or social media on a laptop/desktop can cause cyber-attacks.	-35.071	99	.000	-1.115	-1.18	-1.05
I am aware that clicking and downloading any attachment from an unauthorized email source can cause big fraud.	-79.775	99	0.000	-1.554	-1.59	-1.52
I am aware that running an antivirus program on your laptop/ desktop keeps the machine secure.	-55.968	99	0.000	-1.407	-1.46	-1.36

One-Sample Test						
	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am aware that using any encryption tool can prevent data breach.	-42.948	99	.000	-1.242	-1.30	-1.19

Bank managers possess knowledge regarding the occurrence of phishing fraud, a deceptive practise aimed at inducing individuals to disclose confidential information, such as passwords and financial data, through the use of bogus emails or websites. This implies that banks have taken steps to provide training and education to their employees regarding the potential dangers associated with phishing attacks and the necessary preventive measures.

Bank managers possess knowledge regarding SMS-based fraud, a fraudulent activity that entails the transmission of deceitful SMS messages to individuals with the intention of acquiring sensitive information or executing unauthorised transactions. This implies that banks have implemented measures to educate their employees about the potential dangers associated with SMS-based fraud, as well as strategies for recognising and mitigating such risks.

Bank managers possess knowledge regarding the existence of ransomware threats, which encompass the act of infiltrating computer systems with malicious software designed to encrypt data and subsequently demanding a payment in exchange for its decryption. This implies that financial institutions have taken steps to safeguard their computer networks from ransomware attacks and possess an understanding of the potential consequences that such assaults can have on their functioning.

Bank managers has knowledge of the existence of mobile malwares, which encompass the infiltration of mobile devices with malicious software capable of extracting sensitive data or executing unauthorised financial activities. This implies that banks have implemented measures to provide training to their employees regarding the potential dangers associated with mobile malwares, as well as strategies to safeguard their mobile devices against such vulnerabilities.

Bank managers possess knowledge regarding OTP frauds, which encompass the illicit acquisition of one-time passwords (OTPs) employed for the purpose of authorising transactions, hence facilitating unauthorised financial activities. This implies that banks have adopted efforts to mitigate the occurrence of one-time password (OTP) fraud and have provided training to their employees regarding the associated dangers and preventive measures.

Bank managers possess knowledge regarding the occurrence of online KYC verification fraud, which entails the use of deceitful documents or impersonation in order to successfully navigate online KYC verification procedures. This implies that financial institutions have implemented strategies to mitigate the occurrence of fraudulent activities during online Know Your Customer (KYC) verification processes, demonstrating their recognition of the inherent dangers involved with such fraudulent behaviour.

Bank managers possess knowledge regarding fraudulent activities that exploit screen sharing or remote sharing programmes. These fraudulent activities entail the utilisation of software to illicitly access a victim's computer or mobile device, hence facilitating unauthorised transactions. This implies that financial institutions have taken steps to mitigate such fraudulent activities and possess an understanding of the potential hazards linked to remote access software.

Bank managers has knowledge of the practise of ATM card skimming, which is the illicit acquisition of ATM card information through the utilisation of skimming devices affixed to ATM machines. This implies that financial institutions have implemented measures to mitigate the occurrence of ATM card skimming and have demonstrated an understanding of the potential ramifications of such fraudulent activities on their clientele.

Bank managers possess knowledge on the occurrence of QR code scan frauds, wherein counterfeit QR codes are employed to illicitly acquire sensitive data or execute unauthorised transactions. This implies that banks have implemented measures to provide training and knowledge to their employees regarding the potential hazards associated with QR code scan fraud, as well as the strategies to mitigate such risks.

Bank managers has knowledge about a particular form of fraudulent activity known as juice jacking. This form of fraud transpires when a hacker manipulates a charging station or USB port located in a public setting, with the intention of pilfering data or implanting malicious software into the device of an unsuspecting individual.

Bank managers are cognizant of the efficacy of employing encryption solutions as a means to mitigate the risk of data breaches and safeguard confidential information against unauthorised intrusion.

Bank managers possess knowledge regarding identity theft, a sort of criminal activity involving the illicit acquisition of personal information from individuals, typically with the intention of obtaining financial benefits. Bank managers possess a comprehensive understanding of the imperative nature of implementing robust safeguards aimed at preventing identity theft and promptly detecting such occurrences.

Bank managers has knowledge about IDN Homographic attacks, a type of cyber attack that exploits the utilisation of Unicode characters to fabricate domain names that closely resemble authentic websites. Bank managers possess a comprehensive understanding of the imperative to educate both their workers and customers of various forms of attacks, and then adopt appropriate measures to mitigate their occurrence.

Bank managers are cognizant of the fraudulent activity known as a denial-of-service attack. This form of cyber-attack involves inundating a system or network with an excessive amount of traffic, so overwhelming it and impeding authorised users from gaining access. Bank managers possess a comprehensive understanding of the significance associated with implementing and maintaining effective procedures aimed at preventing and mitigating such assaults.

Bank managers possess knowledge of Trojan malwares, which are malevolent programmes that masquerade as authentic software. The individual comprehends that these forms of malicious software possess the capability to illicitly acquire sensitive information or grant unauthorised entry to a system or network.

Bank managers possess knowledge about the occurrence of debit/credit card frauds, encompassing many forms such as skimming, phishing, and other types of malicious assaults. Bank managers possess a comprehensive comprehension of the significance associated with implementing robust security protocols to safeguard their clientele's card data and promptly identify instances of deceitful conduct.

The results indicate that Bank Managers possess a high level of awareness regarding phishing schemes and the risks that accompany them. It is well acknowledged that those engaging in fraudulent activities employ diverse strategies, including but not limited to email, phone, and social media, with the intention of deceiving customers into divulging their personal information. Bank managers also implement strategies to educate their clientele of these fraudulent activities and provide guidance on exercising caution while disclosing personal information over the internet.

Bank managers has knowledge regarding SMS-based frauds and the corresponding risks they entail. It is acknowledged that those engaging in fraudulent activities employ the tactic of sending counterfeit SMS messages to unsuspecting clients, wherein they are prompted to click on hyperlinks that redirect them to deceitful websites or download hazardous software. Bank managers implement strategies to educate their clientele of fraudulent activities and provide guidance on verifying the legitimacy of SMS messages prior to engaging with any embedded links.

Bank managers has knowledge regarding the existence of ransomware attacks and the accompanying dangers they entail. The user acknowledges the concept of Ransomware as a form of malicious software that use encryption techniques to restrict access to computer data, requiring a ransom to be paid in order to regain control. Bank managers employ many strategies to safeguard their systems against such threats, including the utilisation of antivirus software and the implementation of regular data backups.

Bank managers has knowledge regarding mobile malwares and the accompanying hazards they entail. The user acknowledges the existence of mobile malwares, which are malevolent software that can be acquired and installed on mobile devices, resulting in a range of fraudulent activities. Bank managers implement strategies to educate their clientele against fraudulent activities, while also providing guidance on the installation of antivirus software and cautioning against downloading applications from unauthorised sources.

Bank managers possess a comprehensive understanding of the occurrence of OTP frauds and the inherent dangers they entail. The individual acknowledges the utilisation of One-Time Passwords (OTP) by fraudulent actors as a means to illicitly access customer accounts and carry out unauthorised transactions. Bank managers implement strategies to educate their clientele against fraudulent activities, emphasising the importance of safeguarding their One-Time Passwords (OTPs) and refraining from disclosing them to any other parties.

Bank managers has knowledge of the occurrence of online Know Your Customer (KYC) verification frauds and the accompanying hazards. It is acknowledged that individuals engaging in fraudulent activities employ counterfeit Know Your consumer (KYC) verification procedures in order to get consumer data and carry out deceitful transactions. Bank managers implement strategies to educate their clientele against fraudulent activities and counsel them to authenticate the legitimacy of Know Your Customer (KYC) verification procedures prior to disclosing any personal details.

Bank managers has knowledge of the utilisation of screen sharing programmes or remote sharing services for fraudulent purposes, as well as the inherent hazards involved with such activities. It is acknowledged that those engaging in fraudulent activities can exploit these applications as a means to infiltrate client systems and carry out deceptive transactions. Bank managers implement strategies to educate their clientele on fraudulent activities and recommend that they evaluate the legitimacy of screen sharing or remote sharing software prior to granting access.

Bank managers has knowledge regarding ATM card skimming techniques and the accompanying hazards. It is widely acknowledged that those who engage in fraudulent activities employ skimming devices to illicitly get client ATM card data, then utilising this information to carry out unauthorised transactions. Bank managers implement strategies to provide education to their clientele regarding fraudulent activities, emphasising the importance of exercising caution when utilising automated teller machines (ATMs) and promptly reporting any dubious transactions.

Bank managers has knowledge of the occurrence of fraudulent activities via QR code scanning and the inherent hazards linked with such practises. It is acknowledged that those engaging in fraudulent activities employ counterfeit QR codes as a means to illicitly get client data and carry out deceitful transactions. Bank managers implement strategies to educate their clientele against fraudulent activities and provide guidance on the importance of verifying the legitimacy of QR codes prior to scanning them.

VI. Conclusion

Based on the empirical evidence, it can be inferred that bank managers possess a commendable degree of cognizance regarding diverse fraudulent activities and security vulnerabilities that have the potential to impact their operational processes. The individual possesses knowledge regarding many fraudulent activities, including but not limited to juice jacking, identity theft, internationalised domain name (IDN) homographic attacks, denial-of-service assaults, and debit/credit card fraud. The individuals are cognizant of security protocols that can effectively mitigate the risk of data breaches, including the utilisation of encryption mechanisms.

The degree of consciousness among bank managers plays a pivotal role in establishing effective strategies to limit the risks associated with frauds and threats. Financial institutions that place a high emphasis on employee training

and awareness initiatives are more inclined to cultivate a robust security culture, hence enhancing their ability to safeguard the organisation and its clientele efficiently.

In light of the results, it is recommended that banks persist in allocating resources towards employee training and awareness initiatives in order to ensure that their personnel remain well-informed regarding the latest security dangers and fraudulent activities. This measure will assist financial institutions in improving their security stance and upholding client confidence, which is of paramount importance for the prosperity of banks.

One of the primary issues lies in the perpetual evolution of fraudulent activities and security concerns. Fraudsters consistently seek novel methods to exploit weaknesses, necessitating banks to consistently adapt and enhance their security measures in order to maintain a competitive edge.

One further obstacle is to the necessity of striking a harmonious equilibrium between security protocols and client satisfaction. The implementation of robust security measures is vital in mitigating fraudulent activities; nonetheless, it is noteworthy that such procedures may inadvertently cause difficulty to clients. Financial institutions are faced with the challenge of striking a harmonious equilibrium between ensuring security measures and facilitating user-friendly access to accounts and services, hence minimising any unnecessary inconvenience experienced by clients.

Simultaneously, banks have the potential to utilise technology as a means to augment their security protocols. One such use involves the utilisation of machine learning algorithms to identify atypical patterns of activity, which may serve as potential indicators of fraudulent conduct. Biometric identification technologies, such as facial recognition and fingerprint scanning, offer enhanced security and increased convenience for users to access their accounts.

Overall, the results indicate that bank managers possess a satisfactory level of cognizance regarding frauds and security risks. However, it is imperative for banks to persistently allocate resources towards employee training and awareness initiatives in order to remain abreast of evolving dangers. Banks have difficulties in effectively managing the trade-off between security measures and client experience. However, there exist prospects for utilising technology to augment their security stance. In order to uphold client, trust and safeguard against potential losses, banks must adopt a cautious and adaptable stance towards fraud prevention and security measures.

References

1. Bajaj, M., & Vashisht, A. (2020). Forensic Accounting: A Tool for Detecting Money Laundering in Indian Banking Industry. *International Journal of Accounting Research*, 8(2), 1-6.
2. Bhattacharya, S., & Biswas, P. (2017). Forensic Accounting: Role in Detecting and Preventing Fraud in the Banking Sector. *International Journal of Research in Commerce, IT and Management*, 7(2), 1-6.
3. Choudhury, R. K., & Jha, S. K. (2018). The Role of Forensic Accounting in Mitigating Operational Risks in the Indian Banking Sector. *International Journal of Research in Commerce, IT and Management*, 8(3), 15-21.
4. Kumar, A., & Kumar, M. (2019). The Role of Forensic Accounting in Preventing Financial Statement Fraud in the Indian Banking Sector. *International Journal of Scientific Research and Management*, 7(9), 225-231.
5. Misra, R. K., & Panda, A. (2020). Forensic Accounting and Its Role in Ensuring Compliance in the Indian Banking Sector. *International Journal of Accounting and Finance*, 10(2), 138-150.
6. Shukla, M., & Garg, A. (2018). Role of Forensic Accounting in Detecting Loan Fraud in Indian Banking Industry. *Journal of Commerce and Accounting Research*, 7(2), 31-36.
7. Singh, P., & Gupta, V. (2017). The Role of Forensic Accounting in Detecting and Preventing Fraud in the Indian Banking Sector. *International Journal of Engineering and Management Research*, 7(3), 166-171.
8. Yadav, R., & Gupta, A. (2019). Impact of Forensic Accounting on Corporate Governance in the Indian Banking Sector. *International Journal of Recent Technology and Engineering*, 8(2S), 2155-2160.