SAFEGUARDING YOUR FINANCES: ONLINE BANKING AND BANKING FRAUD

Abstract

In Today's life there are so many things on internet to make our life easier, especially with the help of technology. Now day's online banking is one of them**.** Online banking is the most important and useful way for money transactions these days. Also useful for time saving of the user. On the other hand, many unauthorized and illegal activities take place, and as a result, it becomes a major trouble for the growth of the economy. One of the fraud case can misguide the users and financial loss may occur. To stop these unauthorized activities, many companies started work on these and framed data driven models which uses many machine learning algorithm as well as datasets to identify the unauthorized activities. This chapter will examine the various benefits and issues of online banking. The main objective of this chapter is to research the coverage that bank employs and observe the different fraud expectation procedures prearranged by RBI. Its objectives are to offer approaches to the observation of bank organizations towards defensive method and their responsiveness to several fraudsters. A well-built system of interior manage and good employment practices avoid fraud and take the edge off losses. The consequences indicate that lack of knowledge about updated software, technology, different kinds of mechanisms, lack of training, opposition, and low observance levels can be primary causes of banking scams. This chapter will also focus on the benefits of online banking and its future scope.

Keywords: Banking Fraud, Cause and Prevention**,** Banking Sector, Online Banking, Internet Banking, Machine Learning.

Authors

Purnima Karmakar
Research Scholar
Department of Computer Science & Engineering, Maharishi School of Engineering & Technology,
Maharishi University of Information Technology, Lucknow (Uttar Pradesh), India.
purnimakarmakar330@gmail.com

Rakesh Kumar Yadav
Research Supervisor
Department of Computer Science & Engineering, Maharishi School of Engineering & Technology,
Maharishi University of Information Technology
Lucknow (Uttar Pradesh), India.
rkymuit@gmail.com

Sunil Kumar
Research Supervisor
Department of Information Technology
Ajay Kumar Garg Engineering College,
Ghaziabad, (Uttar Pradesh), India
sunilymca2k5@gmail.com

I. INTRODUCTION

Now a day's online banking is one of the most useful technology in the world. Most of the banking transactions are done by using online banking, which is called Internet banking also. It is very helpful for those who do not want to go to the bank because maybe it takes time.

Therefore, the main purpose can be "It's time-saving". During the pandemic situation, online banking was very useful for users to pay bills online without touching the physical note. It is the easiest way that customer can check their account from anywhere in the world, anyone can money transfer from account to account, can view account statements, account balances, and so on just using an app or through the bank website. So easy to use. The main benefits of Internet banking include accessibility, rapidity, and flexibility. The login process will be as shown in Figure 1. The simplest process of login to access your account. For the same, the user just needs to fill in the required details such as login-id and password, if the details of the user match with the given details set during sign-in then the access will be granted and login will be successful. Now the user can access their account. If the user details do not match with the details the user set during the sign-in process, as per the app creator the message or pop-up can be shown to the screen as incorrect user-id or password, Now a days we are habitual with this process.

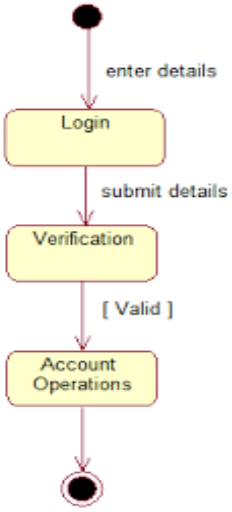

Figure 1: Login process of Internet Banking

Now online banking is not secure because it is possible for hackers to hack an account. An unauthorized user can access our personal information through hacking, when we put personal details to the main sign-in or log-in page or any other the hacker hack the details. Now a days, the most common way that hackers send links or webpages to us and when we click the same and fill in the details of our personal information the hacker gets the same information to their database. Normal user cannot differentiate the page or the link of hacking activity because the page look like same as the banking page, so the way is very easy for the hackers.

This chapter will discuss the various issues of bank account fraud from the perception of the banking industry or financial sector. Bank account fraud is a significant challenge faced by financial institutions worldwide. The bank hierarchy in India involves unauthorized access, manipulation, or exploitation of bank accounts for fraudulent purposes. The impact is substantial, leading to financial losses for both individuals and financial institutions, as well as eroding customer trust as shown in Figure 2.

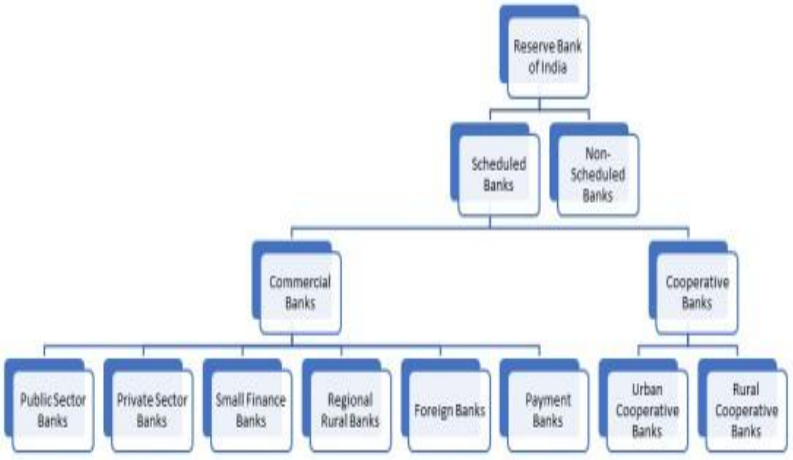

Figure 2: Bank Structure in India

As a result, the normal users facing lot of problems. Most of the user don't understand about these scam calls and messages. So need to detect these techniques very needful at any cost.

So, Detecting and preventing bank account fraud requires the development of robust strategies and technologies that can identify suspicious activities, protect customer assets and mitigate potential risks. So many ways of online bank frauds, such as Phishing scam, Malware infection and Ghost websites. Effective and efficient recognition of Internet Banking frauds is observed as a major challenge to all banks and is a rising source of concern.

II. LITERATURE REVIEW

Bank account fraud is a significant concern in today's digital age where online banking services have become increasingly popular. Researchers and scientists have conducted various studies to identify the causes of bank account fraud and develop effective measures for its detection and prevention. This literature review aims to provide an overview of the different methods used in these studies to address the issue of bank account fraud.

Palchenla Sherpa [1], study focused on detecting bank account fraud using the Computer Emergency Response Team (CERT) and legal frameworks, LAW. The researchers aimed to prevent cybercrime by understanding its nature, minimizing the damage caused, enhancing security measures, and increasing awareness among users. The study found that factors such as unemployment, insufficient banking supervision, lack of awareness about advanced tools and technology, and poor knowledge of computer system strategies contribute

to the rise in cyber fraud. The researchers recommended enforcing laws and regulations, such as Know Your Customer (KYC) protocols, to mitigate fraud

Monica Yadav [2], focused on investigating the nature of fraud in the banking sector in India, particularly related to E-banking. The researchers analyzed the impact of technological advancements and the absence of incentive mechanisms for employees. They highlighted the need for governmental control and internal control measures to prevent insider fraud. The study emphasized the importance of updated software and technology for improved security in E-banking.

Varsha Yadav[3], in this study, utilized Structural Equation Modelling (SEM), as shown in Figure 3, and regression analysis to understand users' awareness of E-banking fraud and its impact on E-banking services as shown in Figure 4.

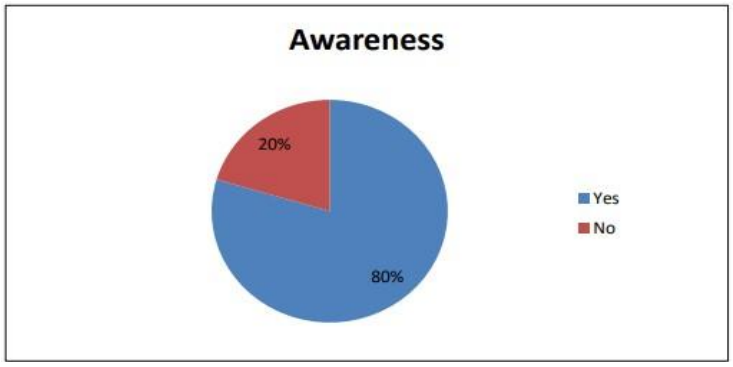

Figure 3: Structural Equation Modelling (SEM)

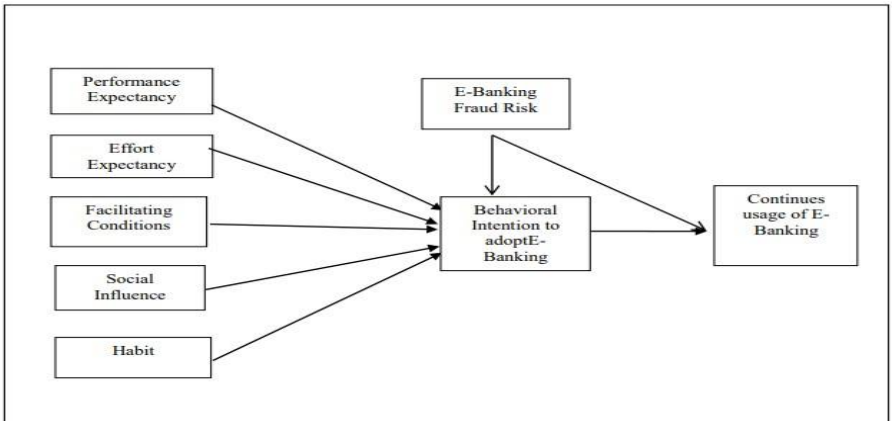

Figure 4: Research model to explain the users the role of E-banking fraud on E-banking services implementation.

This study aimed to develop models and strategies to enhance users' understanding of E-banking fraud. The researchers found that increasing awareness and implementing social, technical, and legal measures play a crucial role in preventing fraud. They recommended conducting studies with a broader demographic profile to obtain more results that are comprehensive.

According to M. J. Madhurya et al. [4] study, the researchers used some techniques like ML Algorithm, NNM (Neural Networking Model), Technique of Classification, and Clustering as the main tool. They also investigate feasible and efficient methods and try to find ways of fraud detection. They found from Diverse Disciplines and Fields, ML Algorithms, as shown in Figure 5 and AI Techniques have the ability to solve the various problems as normally processed for large volumes of data.

So, in this paper, the main factor is to analyze Different ML's performance, accuracy as well as efficiency and they found to apply the ML Algorithm and the strength.

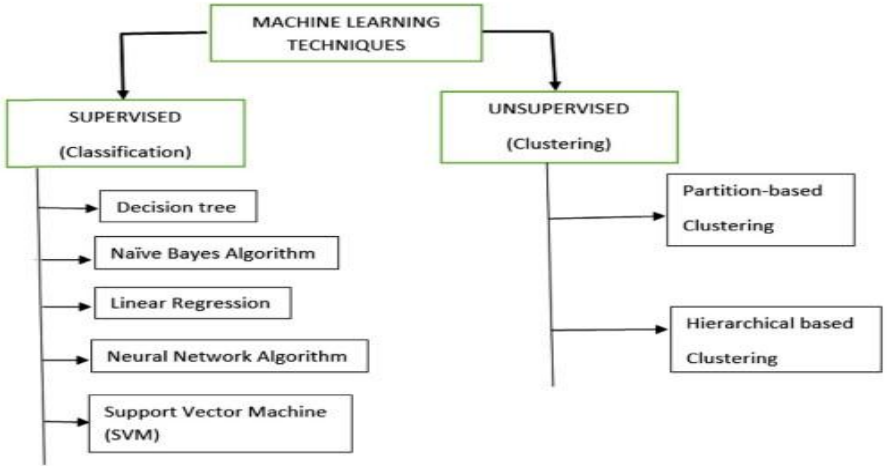

Figure 5: Classification methods of Machine Learning

Suggestion and scope: In this paper with the effective usages of these algorithms such as the method of logistic regression, classification of random forest, K-Nearest Neighbor, Naïve Bayes, Decision tree, etc. and they try to calculate the result and here they use data gathering, data cleaning, research, and visualization, train the classifier algorithm and then evaluate the result.

In future work, the researcher can work on the performance of other ML Techniques. ML can be tested more efficiently to detect the fraud. Using different domains and varied patterns can be used for better performance.

Tika Ram Rai [5], In this study they determined the bank fraud trouble as observed by branch and operational supervisors to identify the sources as well as prevent fraud in the banking sector as shown in Table 1. The main objective of this study is mentioned two-fold, firstly find the Bank officials' observed causes of banking frauds and second to observe bank representatives' perceived deterrent methods of banking frauds. From the documentary analysis in this review, eight important elements were categorized.

Table 1: Cause and Prevention of Banking Frauds

Causes of Banking Frauds	Preventions of Banking Frauds
X2= Information Technology & Poor database management	X1=Accounting and Internal Control
X4= Management override of control	X3= Legal System
X6= Collusion with Employees, customers, and vendors	X5= Ethical Value
X8= Dissatisfaction among employee	X7=Training to employee and awareness program to customers

Suggestion and scope: Firstly, this study was appropriately selected hence the outcome may not be generalizable and secondly in this study, the researcher used graphic statistic exclusively although a further study cross-sectional with the help of inferential statistics is recommended. But if within time the fraud cause and measures identify so we can avoid potential damage. Other major perceived fraud indicates that complicity with authorized employee, users and vendors, IT team and poor database management, awareness, legal system, internal control and ethical values.

Madan Lal Bhasin [6], here the researcher found that fraud is the worldwide phenomenon that influences in all economic sectors. In rapidly developing countries as India the fraud increasing day by day and the fraudsters now also trying to innovate new methods as hacking apps or site using technology. Main challenging aspect is making transaction free from electronic crime and no law for the same till now in the Indian banking sector. With the use of data analysis software the economic sectors can perceive the fraud.

This study conducted questionnaire-based survey for the descriptive part between stuffs of 345 banks of NCR (National Capital Region) area and for the analytical part incorporated the issues, how to integrate technology to perceive and avoid banking fraud in the banking industry. This study also examined the solution to detect fraud using technology and way to integrate the forensic approach. The researcher also uses the neural network to know about the previous bank fraud cases, to learn the various system of trends for fraud. As shown in Table 2, these are some frauds prevailing in Indian banking industry.

Table 2: Some Frauds Prevailing in India

Bribery & Corruption	Cybercrime	Multiple Funding	Counterfeit Cheques
Terrorist Financing	Data Security	Identity theft	Tunneling
Money Laundering	Loan Loss	Internet Banking Frauds	Absence of Collaterals
Tax Evasion	Fraudulent Documentation	Incorrect Sanctioning	Mobile Banking Risks

Suggestion and scope: This study indicates the limit of separation of duties, documentation, professionalism, Bank managers compliance level is low although notice that internal checks are higher than. As a global trend, customers complaints which is followed by

internal or external tip. In this fraud detection internal audit professionals can play an integral role.

III. ADVANTAGES OF ONLINE BANKING FOR SOCIETY

The benefits proposed by banking sector to the customers who choose online banking instead of visit the physical visit to the bank branch are.

1. Visibility Improvement of account balance, fund transaction and account statement, we do not need to visit bank for the banking statement, now easily we can choose the month and download the statement.

2. Easily accessible from anywhere. In today's generation most of the users are working and in week days it's almost impossible to visit bank for a particular work, so we need to take a leave from our work place only for that particular work, so using online banking we can do the transaction from our work place also, which is very convenient for all of us. Even if we are travelling then also, we can access our account.
3. Easily access at any time, 24 x 7 availability. So, not depend on bank timing as well as bank staffs availability. For an example, if we went to bank after 3:00 pm, bank staffs usually occupied with the closing work, so usually they don't do the new transaction after 3:00 pm and because of the same we need to go bank again next day for that same transaction, which is time consuming and as well as waste of time of the users.

4. No chance of calculation mistake or manually there are chance of calculation or numeric written mistakes.

5. Profit to bank, banks gain more profit meaningfully with the use of online banking as it need less physical effort from the banking staff.

6. Using Online banking, we can set auto deduction from our account monthly; even we can set a particular date whenever we want to do the deduction. No need to visit bank physically every month. Therefore, automatically it is save the time of users as well as bank staffs.

7. Other benefits of online banking, good for the environment as it cut the usage of paper, no need to travel so can stop the pollution or step to stop the pollution.

IV. PROBLEMS AND SECURITY ISSUES IN USING ONLINE BANKING

Every day there are millions of financial transactions occur and at that time bank transaction details or information are hacked by hackers. Years ago, the evolution of attacks began that is known as phishing, where hackers create links for hacking and send them to banking users.

Recently, studied by the University of Michigan, more than 75 percent of websites related to banks have at least one design flow that holds the personal information of customers and design flows like expert users also find difficulties to detect or unlike the bugs.

The study recommended to use of SSL to avoid third-party websites like for safety purposes and secure banking.

1. **Reliability Risk**: The Internet allows us to use the services of Internet banking from anywhere in the world at any time as well as from any system, which may not be secure enough.

2. **Information Leakage**: personal information like bank account details, account holder name, and so on leakage from third-party Internet banking sites. These sites are not reliable.

3. **Transparency Issue:** The fraud can be done with a hidden method so that the user doesn't understand the process or unknowingly the user puts all the personal details into the function exactly the same details hackers need to do hacking.

4. **Poverty:** Poverty is also one of the main reasons for fraud. People cannot fulfill their needs so they do these kinds of frauds to fulfill their needs or luxuries.

5. **Entertainment:** Some people will do these kinds of things for their fun, without bothering the results of their actions.

6. **Network:** Sometimes network cannot work properly so the systems and the accounts can easily be traced. They do not have a strong network connection, updated mechanism, or better software.

7. **Careless:** People are careless about their work or an organization. They cannot take it seriously, in the way they give a chance to commit fraud.

8. **Lack of Training:** Lack of training for bank employees as well as users. Therefore, they are not aware of updated technology, mechanisms, and protected software.

V. PROPOSED WORK

To ensure the safety of our bank accounts and reduce the chances of falling victim to fraud, it is essential to follow certain steps and practices:

1. Firstly, implementing secure banking transaction methods is crucial. This includes measures such as using PIN protection to prevent external threats, password protection, and implementing SSL encryption with 128-bit encryption. It is important to safeguard passwords and avoid sharing them with anyone to maintain privacy.

2. Installing reliable antivirus and anti-spam software on our computers is another vital step. This helps protect our data from attackers and ensures secure transactions by preventing outside hacking attempts.

3. It is crucial to never share passwords or other personal information over the phone, even if the caller claims to be from the bank for verification purposes. Any suspicious links

received via email should be carefully examined using a reputable antivirus and spyware software.

4. Phishing techniques are commonly used by hackers to acquire personal credentials. Users should be cautious of emails containing links that lead to a hacker's server. When entering details into online forms, it is important to verify that the website address starts with "https://" for a secure connection. Additionally, users should look for a padlock symbol when entering passwords and ensure no one is nearby observing the password entry.

5. Enabling wireless security on modems and routers is essential to prevent attackers from intercepting sensitive data being transmitted.

6. Bank accounts should always be accessed from secure locations to avoid potential key loggers installed on unsecured computers. It is advisable to sign out of the account after each use to prevent unauthorized access.

7. Posting personal information, such as email IDs, date of birth, and phone numbers, on social network sites should be avoided. It is important to only accept friend requests from individuals known personally and refrain from using third-party apps frequently found on social sites.

8. Regularly checking bank account and credit card statements is crucial. If any unfamiliar transactions are identified, they should be reported to the bank immediately.

9. Financial institutions, like HSBC India, prioritize training staff to comply with comprehensive security protocols, ensuring secure operations of their systems.

10. In case of any login issues, it is recommended to contact the bank immediately rather than sending emails. Additionally, accessing online banking when internet speed and connectivity are reliable can help mitigate potential risks.

11. If a bank refuses to refund money due to fraud, losses, or any transfer-related problems, the issue can be reported to the Financial Ombudsman Service.

By following these suggested measures and guidelines, individuals can enhance the security of their bank accounts and minimize the risk of becoming victims of fraud.

VI. ANALYSIS

The studies reviewed in this literature review highlight various methods used by researchers and scientists to detect and prevent bank account fraud. These methods include utilizing CERT and legal frameworks, analyzing E-banking and governmental frameworks, employing machine learning techniques, investigating causes and prevention measures. The findings emphasize the importance of regulatory control, technological advancements, user awareness, and efficient internal controls to mitigate the risks of bank account fraud. Future research should focus on exploring advanced technologies, integrating forensic approaches, and addressing research gaps to improve fraud detection as well as avoidance in the banking industry.

VII. CONCLUSION

In the research, we proposed the implementation of a robust fraud detection solution using Logistic Regression and a large database of logged banking transactions. Logistic regression proved to be a valuable statistical model for evaluating the relationship between dependent and independent variables, allowing us to predict the likelihood of fraudulent activities based on these variables. By accurately classifying potential instances of fraud, banks, and financial institutions can take proactive measures to prevent financial losses and protect their customers.

The utilization of a large database of logged banking transactions provided a solid foundation for training and validating the logistic regression model. This extensive dataset allowed the model to learn and identify patterns and characteristics associated with fraudulent transactions. As a result, the model's ability to detect and classify fraud improved, providing enhanced accuracy in identifying potential instances of fraudulent activities within the banking system.

Implementing this fraud detection solution can significantly enhance the security and integrity of banking systems. By promptly identifying potential fraud, banks can take swift action to intervene and implement mitigation measures. This not only safeguards the interests of the institution but also ensures the financial well-being and trust of its customers. It is important to note that while logistic regression is powerful, it should be complemented by other techniques and methodologies, continuous monitoring, advanced analytics, and collaboration with industry experts to develop a comprehensive fraud prevention strategy that can effectively combat evolving fraudulent tactics.

In conclusion, the implementation of a fraud detection solution based on logistic regression, utilizing a large database of logged banking transactions, holds tremendous potential in improving the security of banking systems. By leveraging the predictive capabilities of logistic regression, banks can proactively identify and prevent fraudulent activities, thereby protecting their customers and preserving the reputation and financial stability of the institution. With continuous advancements in fraud detection technologies and ongoing collaboration among industry stakeholders, we can further enhance the effectiveness of such solutions and stay ahead of emerging fraudulent schemes.

VIII. FUTURE SCOPE OF INTERNET BANKING

In Today’s busy schedule users do not want to go bank physically, so the number of customers utilizing online banking services continues to rise. To ensure customer satisfaction and trust, it is crucial for banks to identify the modus operandi of these criminals.

It is essential for bank employees to handle accounts with utmost care and alertness, ensuring that all necessary security protocols are followed diligently. By prioritizing both technological safeguards and the human factor, the banking industry can effectively minimize the risk of fraudulent activities and protect the financial interests of their customers and commercial entities as shown in Figure 6.

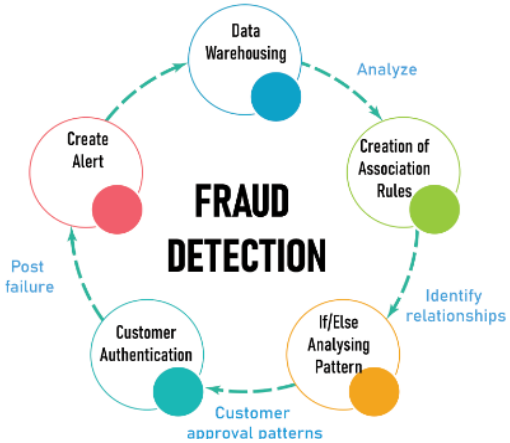

Figure 6: Way of Fraud Detection in the Indian Banking Industry

REFERENCES

[1] Palchenla Sherpa, "Legal and regulatory issues of cyber fraud in transnational banking with special reference to European Union," 2021, January, pp. 226.
[2] Monica Yadav, "Frauds in the Banking Sector a Detailed Study of Insider Risks in e-Banking and Legislative Framework in India," 2022, June, pp. 235.
[3] Varsha Yadav, "Modelling the Effect of E Banking Frauds on Customer Behavior and E-Banking Usage," 2023, February, pp.189.
[4] M J Madhuryaa , H L Gururaj , B C Soundaryaa , K P Vidyashree , A B Rajendra,"Exploratory analysis of credit card fraud detection using machine learning techniques," Vidyavardhaka College of Engineering, Mysuru, vol. 3, pp. 31-37, 2022.
[5] Tika Ram Rai, "Banking frauds: causes and preventions," JOURNAL OF BANKING, FINANCE &INSURANCE (BFIN), vol. 2, PP. 70-77, 2021.
[6] Madan Lal Bhasin,"Combatting Bank Frauds by Integration of Technology: Experience of a Developing Country," British Journal of Research.
[7] Xuting Mao, Hao Sun, Xiaoqian Zhu, Jianping Li, "Financial fraud detection using the related-party transaction knowledge graph," Procedia Computer Science 199 (2022), pp. 733–740, 2022.
[8] Mark Eshwar Lokanan, Kush Sharma, "Fraud prediction using machine learning: The case of investment advisors in Canada "Machine Learning with Applications (MLWA), vol. 8, 2022.
[9] Sarah Oliveira Pinto, Vinicius Amorim Sobreiro, "Anomaly detection approaches on digital business financial systems," Digital Business,Vol. 2, Issue 2, 2022.
[10] Mahinda Mailagaha Kumbure, Christoph Lohrmann, Pasi Luukka, Jari Porras, "Machine learning techniques and data for stock market forecasting," Expert Systems With Applications, Vol. 197, 2022.
[11] Kamal Nain Sharma, Ankit Kala, "Online Banking Frauds and Necessary Preventive Measures", ENVISION- International Journal of Commerce and Management, VOL-16, 2022.
[12] Jonathan M. Karpoff, "The future of financial fraud", Journal of Corporate Finance, vol. 66, 2021.
[13] Waleed Hilal, S. Andrew Gadsden, John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Systems with Applications, vol. 193, 2022.
[14] Sukanya Kundu & Nagaraja Rao, "Reasons of banking fraud– a case of Indian public sector banks," International Journal of Information Systems Management Research & Development (IJISMRD), Vol. 4, Issue 1, 2014.
[15] Ashu Khanna, Bindu Arora, "A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry", Int. Journal of Business Science and Applied Management, Volume 4, Issue 3, 2009.
[16] Fabrizio Carcilloa , Yann-A¨el Le Borgnea , Olivier Caelenb , Yacine Kessacib , Fr´ed´eric Obl´eb , Gianluca Bontempi, "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," 2019.
[17] Hooda N., Bawa S., Rana P., "Fraudulent firm classification: A case study of an external audit," Applied Artificial Intelligence, 32 (1) (2018), pp. 48-64.

[18] Lokanan M.E., "Theorizing financial crimes as moral actions", European Accounting Review, 27 (5) (2018), pp. 901-938.
[19] Lokanan M., Tran V., Vuong H.N., "Detecting anomalies in financial statements using machine learning algorithm: The case of Vietnamese listed firms," Asian Journal of Accounting Research, 4 (2) (2019), pp. 181-201.
[20] Perols J., "Financial statement fraud detection: An analysis of statistical and machine learning algorithms," Auditing: A Journal of Practice & Theory, 30 (2) (2011), pp. 19-50.
[21] Severina M., Peng Y., "Machine learning algorithms for fraud prediction in property insurance: Empirical evidence using real-world microdata," Machine Learning with Applications, 5 (15) (2021). Applications, 5 (15) (2021).

