From Threat to Shield: How Fintech Empowers Financial Institutions in Combating Fraud

Maslinawati Mohamad[1], Noor Faiza M. Ja'afar[2*], Fatmawati Jusoh[3], Rabiatul Alawiyah Zainal Abidin[4]

[1,3]Faculty of Accountancy, Universiti Teknologi MARA, Puncak Alam Campus, Selangor, Malaysia.

[2]Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam Campus, Selangor, Malaysia, Money Laundering Research Group, Universiti Teknologi MARA, Alor Gajah Campus, Melaka, Malaysia.

[4]Faculty of Business Management, Universiti Teknologi MARA, Segamat Branch Campus, Johor, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2024.814MG0030

Received: 04 November 2024; Accepted: 08 November 2024; Published: 26 December 2024

ABSTRACT

The financial industry has significantly changed with the vast development of Fintech technology. Financial fraud has also increased with these advances, putting the financial industry at risk globally. Through the principles of financial criminology, the study illustrates some fintech technologies that can also be used as fraud-fighting tools in the financial industry. Tools including blockchain, biometrics, artificial intelligence, and machine learning were explored based on their function in preventing and detecting financial fraud. The study has found that several benefits have been brought in by the fintech tools, which can be considered as fintech solutions that contribute towards preventing and detecting financial fraud, for example, real-time monitoring and analysis of financial transactions, improved accuracy in identifying suspicious activity, enhanced customer identity verification, secure data encryption, and robust authentication protocols. Furthermore, such fintech solutions do bring extra benefits to the sustainability of financial institutions, such as better collaboration and information sharing among financial institutions and regulatory authorities, fostering a more coordinated and proactive approach to fraud prevention. This study offers useful information for financial institutions, legislators, and regulators and advances our theoretical knowledge of the revolutionary potential of fintech in fraud prevention and detection. It highlights the importance of accepting fintech as a potent weapon in the continuous fight against financial fraud.

Keywords: Fintech, financial institutions, fraud detection, fraud prevention and financial crime.

INTRODUCTION

Financial fraud will always harm institutions, especially financial institutions, causing huge financial losses, damaged reputations, and decreased public confidence. Worse, stability, credibility, and survival would also be affected. The fast development in financial technology, i.e., fintech, has increased the rate and variety of forms of financial fraud while bringing with it the most powerful solutions.

Financial fraud refers to illegal activities such as money laundering, identity theft, payment fraud, and insider trading. On average, globally, all organizations affected by financial fraud would lose at least 5% of their annual revenue, nearly USD 4.7 trillion (ACFE, 2022). In the future, the figure could go up even higher.

Hence, there is a critical need to develop stronger and more impactful methods of detecting, preventing, and mitigating fraudulent activities.

Technological advances in fintech include the use of artificial intelligence (AI), machine learning (ML), blockchain, biometrics, and data analytics for financial institutions to streamline operations, improve customer experience, and optimize risk management (Cao et. al., 2020). The benefit of these technologies has enabled financial institutions to improve their business procedures, grow their customer base and loyalty, and address contemporary challenges (Protsak & Kovalenko, 2022).

Within this context, this conceptual paper intends to explore the empowering role of fintech in combating fraud within financial institutions. The main research question leading this study is: How does fintech empower financial institutions in combating fraud? This research seeks to contribute to the existing body of knowledge in financial criminology by examining fintech's various applications and implications in fraud detection and prevention.

The importance of the study is in highlighting the positive impact of fintech in combating fraud effectively. Such information is important to financial institutions, regulators, policymakers, and stakeholders to assist them in making informed decisions regarding adopting, integrating, and regulating fintech solutions towards developing best practices and policies that harness the full potential of fintech in protecting the financial system.

In the next sections of this paper, we will explore further fintech applications in fraud detection and prevention, their challenges and limitations, and recommendations for the future directions of fintech in preventing and detecting financial fraud. Through this thorough examination, we aim to highlight how fintech could evolve from a potential threat to a strong shield against financial fraud.

CONCEPTUAL FRAMEWORK

A. The overview of financial criminology and its significance towards fraud prevention

Financial criminology is a multidisciplinary field that examines financial crime, the causes, and strategies to prevent as well as to battle the issue. It sets the theoretical and empirical framework to help associated parties to understand the progression of this fraud in the financial industry. Financial crime draws on various disciplines, including criminology, economics, law, and finance, to analyze the complex nature of financial crime and develop effective prevention measures (Sahri et al., 2018).

From the perspective of fraud prevention, financial criminology has suggested the relationship between motivations, behaviours, and patterns that link to the fraud activities. It helps in identifying weaknesses in the financial system, risk analysis, and developing an intervention with a target to reduce the occurrence and effect of the fraud. With the understanding of underlying factors of criminogenic, financial institutions could implement proactive policies and strategies to detect fraud, and minimize the losses (Gotelaere & Paoli, 2022).

B. The role of technology in fraud detection and prevention.

Technology plays a very significant role in detecting and preventing fraud, enabling the financial institution to enhance their capability to detect and reduce fraud activities. Solutions provided by the latest technology has significantly increased the speed, precision, efficiency to detect fraud as compared to traditional manual approach. Moreover, automation, data analytic, and artificial intelligence (AI) have become a very much needed tools to detect patterns, anomalies, and suspicious activities that indicates fraud is happened or about to happen (Mogaji et al., 2022; Bisht et al., 2022; Couceiro et al., 2020).

C. FinTech integration into fraud prevention strategies

With its groundbreaking invention, fintech has been proven as being one of the effective strategies to combat the financial fraud. The financial institution could eventually tighten their fraud prevention measures, by benefiting from solutions provided by fintech. Fintech applications such as Artificial Intelligence, machine learning, blockchain, biometrics, and data analytics have opened up new approaches for detecting and preventing fraud. This new technology allows better real-time transaction monitoring, abnormal transaction detection, user identification authentication, and safe data encryption (Sood et.al., 2023).

D. Theoretical foundations for understanding the empowering role of fintech

To understand the role of fintech in preventing fraud, it is important to refer to several related theoretical foundations. Rational choice theory assumes that people decide to commit fraud when they believe that the risk-benefits are benefitting to them (Kuo & Tsang, 2023). Eventually, fintech can interrupt the fraud dynamic by increasing the identified risk and reducing the rewards associated with committing that particular fraud. Additionally, social control theories emphasize on the importance of monitoring, prevention as well as effective punishment to prevent fraud. Fintech has improved this aspect with the enhanced monitoring, real-time detection, and good authentication mechanism (Stojanovic et al., 2021).

FINTECH APPLICATIONS IN FRAUD DETECTION AND PREVENTION

A. Artificial Intelligence (AI) and Machine Learning (ML)

Artificial intelligence (AI) and machine learning (ML) have changed how financial fraud is prevented and detected. These technologies make use of huge data analysis, structured and structured to develop a certain pattern to identify any irregularities that indicate the existence of fraud activities (Chaquet-Ulldemolins et al., 2022; Biswas et al., 2022; Narsimha et al., 2022; Jain et al., 2021).

AI and ML technologies also offer real-time monitoring that allows financial institutions to respond to possible fraud cases more quickly, as the technologies can increase accuracy and reduce false alarms in fraud detection (Dwivedi et al., 2021). For instance, using AI-driven chatbots can guide customers on how to avoid being scammed. An anomaly detection algorithm will promptly highlight possible fraud activities whenever there are uncommon transaction patterns.

B. Blockchain Technology

Blockchain enhances the security and transparency of financial systems and its ability to automate fraud prevention and detection processes. Blockchain's decentralised and immutable feature reduces the possibilities of unauthorised access and unauthorised document alteration. Hence, it ensures the integrity and authenticity of financial documents (Balagolla et al., 2021).

Traceability and transparency are other features of Blockchain that highlight its transparency and facilitate identifying and investigating fraudulent activities, such as manipulation, double spending, and identity theft. Not only that, Blockchain technology also supports smart contracts or self-executing agreements that enable quick initiative actions in response to any suspicious activities. (Dwivedi et al., 2021).

C. Biometrics and Identity Verification

Biometric technologies help significantly reduce identity theft. Through this technology, a person's identity is authenticated using their natural unique identifiers. Methods such as fingerprint authentication, facial recognition, iris scanning, and voice recognition are powerful tools to combat identity theft, as it is very difficult to imitate or manipulate a person's biometric identity (Jain et al., 2016).

D. Data Analytics and Pattern Recognition

Data analytics and pattern recognition techniques are critical to detecting and preventing fraud in financial technology. Financial institutions can identify patterns, trends, and anomalies indicative of fraudulent activity by analyzing large volumes of transactional data. These algorithms can detect suspicious transaction behaviour and uncover unusual spending patterns (Razaque et al., 2022). To cope with the imbalance in fraud detection datasets, various equalization techniques can be used, such as Random Undersampling, Synthetic Minority Oversampling Technique (SMOTE), and Generative Adversarial Networks (GAN) (Jenipher et al., 2021).

In addition, machine learning models can be used to detect fraud, including Naive Bayes, Logistic Regression, Support Vector Machine, Decision Tree, Random Forest, Gradient Boosting Tree, and Multi-layer perceptron (Tadesse, 2022). To improve fraud detection performance, control rules and community detection algorithms can be combined with machine learning models (Tadesse, 2022). Five state-of-the-art fraud detection methods are used in credit card fraud detection and prevention, including random undersampling, t-distributed stochastic neighbourhood embedding, principal component analysis, singular value decomposition, and logistic regression learning (Razaque et al., 2022).In addition, trajectory analysis can be used to detect and monitor fraud, and fraud analysis can benefit from trajectory analysis for both Big Data ecosystems and spatiotemporal data mining algorithms and techniques (Karim & Boulmakoul, 2021).

Overall, the applications of AI and ML, blockchain technology, biometrics, and data analytics in financial technology have significantly improved fraud detection and prevention measures. These technologies give financial institutions the tools to improve their monitoring capabilities, identify suspicious activity, authenticate user identities, and detect patterns indicative of fraud. Financial institutions can proactively combat fraud, protect their assets, and maintain the financial system's integrity using these fintech solutions.

CHALLENGES AND LIMITATIONS OF FINTECH IN COMBATING FRAUD

A. Ethical and Privacy Issues

There has been the fast-paced evolution and straight-forward proliferation of ch solutions, which has also, in turn, posed many important challenges in different facets of the financial industry. Technological advances in blockchain, artificial intelligence, and mobile applications have significantly improved the efficiency, availability, and quality of services offered by the banks (Awaliyah et al, 2024). On the flip side, this transformation brought regulatory responses from governments for both players of the game fintech companies and legacy institutions (Kinslin, 2024). Targeted licensing, protection and management of users' data, and risk management in relation to money laundering are the key pillars that impact on such issues as innovation and competition, compliance costs among others within the industry. While fintech uptake is influenced by performance expectancy, effort expectancy and social influence (Amnas et al, 2023), the determinant of trust is one that is critical in tech adoption decisions at the firm level (Grandhi et al, 2022). On the other hand, organizational factors such as senior management support and the competence of the organization are critical enablers of trust in fintech. Besides, the influx of new actors in the finance industry due to the introduction of fintech has also led to worries about market stability as there are some actors in the market who are now tail backed out to be so small and these are some players who should be regulated otherwise, it can cause some problems (Alam, 2022).

Algorithmic bias and fairness in fintech and data analytics are pervasive components of modern finance Software-based solutions — e. g., applications for AI-driven algorithmic trading, critical infrastructures needed to operate digital. Though these technologies could provide valuable capabilities for risk management, fraud detection and investment decision making they also inherently increase the potential ethical challenges that need to be considered (Sreerama & Krishnamoorthy, 2022). For fintech, we see the increasing use of AI-enabled algorithms in credit scoring, loan approvals and investment recommendations. Nonetheless, such systems may introduce or worsen biases in ways they might generate unfair outputs for parts of the population (Sreerama & Krishnamoorthy, 2022). The "Butterfly Effect" in AI systems can compound this problem: minor biases or misbehaviors come into the system while the algorithm is being developed, leading to large and incomprehensible effects on intricate financial markets (Ferrara 2023). Addressing these issues, Explainable AI (XAI) techniques such as SHAP and LIME were proposed to achieve the detection of biases in fintech algorithms that might attribute them a potential bias (Magham, 2024). Furthermore, an important step to facilitate responsible AI adoption within financial services industry is the establishment of ethical principles and regulatory frameworks as well a mandatory collaboration between fintechs companies, insurers or banks on one hand with relevant government institutions like ethicists in order to ensure that values are considered in concrete technologies deployment covering different tracks. This provides the basis for maintaining trust and fairness in fintech applications, with data analytics becoming part of a balanced approach involving ethical considerations (Sreerama & Krishnamoorthy, 2022), while accounting for challenges such as achieving good quality of the available data [Data Quality] coupled with Cybersecurity & privacy issues.

B. Technological Limitations

Although fintech offers several benefits there are still some problems that can impair its ability to manage fraud. A major limitation is poor user interface design and insufficient technical support (Alam & Saputro, 2024). If the interface is complex, it can plausibly prevent users from interacting optimally with fintech services resulting in lower uptake and hence increased exposure to fraud incentivizing criminals. In addition, weak technological infrastructure and poor risk management processes may expose fintech platforms to cyber-attacks and privacy issues (Aloumi et al., 2024). Safety implications are especially important as they have a bearing on consumer reliance and adoption of fintech services. It should be noted that despite the promise for using AI and machine learning algorithms in fraud detection, with some studies suggesting as much as 94% accuracy of fraudulent transaction determination (Lacruz & Saniie, 2021), fintech platforms are evolving so rapidly that criminals have stepped up their game even further by making themselves more elusive. This continuous requirement for more technologically advanced and agile fraud detection methods. Finally, the use of AI for fraud detection has created issues with data security and privacy (Milovich et al. To sum up, although fintech is a new era that promises solutions to multiple potential security issues such as fraud in comparison with websites like directmale.com among others but there are still hurdles due to old technology comprising unhandy interfaces requiring technical support and suffering from cybersecurity locks all the while recurring retraining of AI models needed. As the sophistication increases, progressing beyond these abilities is a continuous cycle of investment in user-friendly design and security features based on best practices due to fraud innovations. If this gets into the wrong hands, it can cost a fortune in the future and will cause reduction in trust on technology itself (Toshihiko & Isamu 2017).

On the other hand, the novel and elaborate technological frauds act as a limiting factor for fintech. The existing technologies are not trained for such issues since this is only a fleeting problem; the frauds are always changing with time. In this case, it is necessary for the institutions of a financial nature to still aim at enhancing their systems by undertaking research and development and making improvements in fintech solutions (Saluja, 2022; Selvaraj, 2021; Toshihiko & Isamu, 2017; Roszkowska, 2020).

C. Regulatory and Legal Implications

One noteworthy aspect of recent advancements in regulations regarding fintech is that the organizations on the market now must keep within the relevant requirements and norms. This is important as such proposals were introduced for this reason, to provide protection to consumers and to enhance anti-money laundering as well as privacy law compliance. The same goes for the legal issues pertaining to the liability for false positives or negatives and legal acceptability of AI-generated evidence. Thus, under investment strategy, any use of fintech designed for fighting fraud would in practice mean the necessity for the financial institution to comply with the aforementioned regulations and legal requirements (Faccia, 2020; Dubey, 2022; Faccia, 2023; Roszkowska, 2020).

CONCLUSION

This research explored the role of Financial Technology (fintech) in assisting and equipping financial institutions to effectively combat fraud. The findings highlight fintech's transformational potential in combating financial crime, including applications in fraud detection and prevention, case study analysis, addressing problems and limitations, and giving empirical evidence.

There are many solutions to fraud problems provided by fintech for financial institutions: Artificial Intelligence, along with machine algorithms, has accomplished a lot in improving the element of fraud detection in finance Domi, et al., (2024); Shoetan & Familoni, (2024). With this technology, however, institutions are able to process huge amounts of data and cross check many variables for potential threats in real time with considerable ease (- et al., 2024; Shoetan & Familoni, 2024). Among all, deep learning models are exceptional in detecting sophisticated types of fraudulent activities than the manual approaches you have mentioned (Shoetan & Familoni, 2024). For example, usage of deep learning algorithms only for credit card fraud detection has made it possible to predict up to 94% of the frauds (Lacruz & Saniie, 2021). An unexpected feature, however, is that although AI and machine learning are helpful in the prevention of fraud, they themselves create problems. Certainly, the use of technology brings with it a potential risk in relation to data and fraud (Varma et al., 2022).

Next, fintech uses new advanced technologies such as AI techniques that include machine learning and blockchain to provide financial institutions with a flexible solution in reduced fraud prevention (Shoetan & Familoni, 2024). Financial Organisations, such as banks can use these tools for improving their fraud detection process which helps them in reducing operational costs and adding financial stability the whole (Gujral 2023; Varma et al., 2022). Yet institutions need to take the benefits but weigh risks and ethical issues too for responsible fraud controls using these technologies.

Some of the ways fintech can make a way for banks to benefit are: it could help supply their machine learning and artificial intelligence tools that would be used in analyzing data, pattern recognition technologies which might otherwise be ignored or undetected due fraudulent activities involving more complex patterns. On a second note, it reinforces security and transparency in recording of the transactions through deploying blockchain technology — potentially reducing risk of fraud activities. Furthermore, by improving identity verification in biometric systems there is also a potential reduction of risks related to theft. Therefore, data analytics and pattern recognition have an essential part to play in provision of trend on fraud trends for portfolio management decisions within financial institutions. This demonstrates the potential benefits of fintech such as helping banks to curb financial loss, customer trust and operational efficiency savings by enabling real time fraud prevention.

The fact that fintech can provide financial institutions with quantum computing, advanced analytics, and IoT integration to bolster their fraud prevention measures makes it imperative to highlight how beneficial it may be in this regard. However, the challenges and limitations like ethical and privacy concerns, technological limitations, as well as regulatory and legal implications cannot be overlooked. To overcome this, financial institutions, technology providers, policy makers, and regulators need to collaborate in unlocking the full potential of fintech in fighting fraud. This is vital as these institutions would highly benefit from the use of fintech.

In conclusion, fintech demonstrates significant efficacy in combating fraud, and when implemented by financial institutions, it not only enhances their defensive capabilities and safeguards their clientele, but also contributes to the fortification of a secure and robust financial system.

ACKNOWLEDGEMENT

We would like to express gratitude to the Faculty of Accountancy at Universiti Teknologi MARA (UiTM), Cawangan Selangor Kampus Puncak Alam, for the financial assistance provided under Yuran Penerbitan Artikel Jurnal Berindeks (PYPA) which has greatly facilitated the dissemination of the research findings.

REFERENCES

1. Alam, N. (2022). *FinTech regulation—A key to financial stability* (pp. 9–24). springer. https://doi.org/10.1007/978-3-031-11954-5_2
2. Alam, A., & Saputro, I. A. (2022). A qualitative analysis of user interface design on a Sharia fintech application based on the Technology Acceptance Model (TAM). *Jurnal TAM (Technology Acceptance Model)*, *13*(1), 9.
3. Aloumi, D., Malik, S., Alkhaldi, A., & De Pablos, P. O. (2024). Factors influencing consumer interactions with fintech services (pp. 239–258). igi global. https://doi.org/10.4018/979-8-3693-5673-9.ch010
4. Amnas, M. B., Parayitam, S., Selvam, M., Raja, M., & Santhoshkumar, S. (2023). Understanding the determinants of fintech adoption: integrating UTAUT2 with Trust Theoretic Model. *Journal of Risk and Financial Management*, *16*(12), 505. https://doi.org/10.3390/jrfm16120505
5. Association of Certified Fraud Examiners (ACFE). (2020). Report to the nations 2020 global study on occupational fraud and abuse. Retrieved from https://www.acfe.com/report-to-the-nations/2020/
6. Awaliyah, T., Hartaty, S., Felani, F., Judijanto, L., & Safitri, N. (2024). The impact of financial technology innovation on banking service transformation: A case study in the fintech industry. *Global International Journal of Innovative Research*, *1*(3), 306–313. https://doi.org/10.59613/global.v1i3.47
7. Balagolla, E., Fernando, W.N., Rathnayake, R., Wijesekera, M., Senarathne, A., & Abeywardhana, K.Y. (2021). Credit card fraud prevention using Blockchain. 2021 6th International Conference for Convergence in Technology (I2CT), 1-8.
8. Bisht, D., Singh, R., Gehlot, A., Akram, S.V., Singh, A., Montero, E.C., Priyadarshi, N., & Twala, B. (2022). Imperative role of integrating digitalization in the firm's finance: A technological perspective. Electronics.
9. Biswas, A., Deol, R.S., Jha, B.K., Jakka, G., Suguna, M., & Thomson, B.I. (2022). Automated banking fraud detection for identification and restriction of unauthorised access in financial sector. 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 809-814.
10. Cao, L., Yuan, G., Leung, T., & Zhang, W. (2020). Special Issue on AI and FinTech: The Challenge Ahead. *IEEE Intell. Syst.,* 35, 3-6.
11. Chaquet-Ulldemolins, J., Gimeno-Blanes, F.J., Moral-Rubio, S., Muñoz-Romero, S., & Rojo-álvarez, J.L. (2022). On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): *Nonlinear Analysis through Interpretable Autoencoders. Applied Sciences*.
12. Couceiro, B., Pedrosa, I., & Marini, A. (2020). State of the art of artificial intelligence in internal audit context. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 1-7.
13. Dubey, B. (2022). Role of fintech in financial reporting and audit fraud prevention and safeguarding equity investment. International Journal of Science and Research Archive, 2022, 07(02), 559–565.
14. Dwivedi, Y. K., Rana, N. P., Janssen, M., Lal, B., Williams, M. D., & Clement, M. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy. International Journal of Information Management, 56, 102211.
15. Faccia, A. (2023). National payment switches and the power of cognitive computing against fintech fraud. Big Data Cogn. Comput., 7, 76.
16. Faccia, A., Moçteanu, N.R., Cavaliere, L.P., & Mataruna-dos-Santos, L.J. (2020). Electronic money laundering, the dark side of fintech: an overview of the most recent cases. *Proceedings of the 2020 12th International Conference on Information Management and Engineering*.
17. Ferrara, E. (2023). The butterfly effect in artificial intelligence systems: implications for AI bias and fairness. https://doi.org/10.48550/arxiv.2307.05842
18. Grandhi, L. S., Wells, M., Grandhi, S., & Wibowo, S. (2022, December 7). The role of organizational factors and trust on fintech adoption in Indian financial organizations. https://doi.org/10.1109/snpd54884.2022.10051816
19. Gotelaere, S., & Paoli, L. (2022). Prevention and control of financial fraud: A scoping review. *European Journal on Criminal Policy and Research,* 1-21.

20. Gujral, R. K. (2023). Determinants of fintech and internet of things for technological disruption: A new-age sustainable and comprehensive outlook. *RESEARCH REVIEW International Journal of Multidisciplinary, 8*(3), 141–149. https://doi.org/10.31305/rrijm.2023.v08.n03.016
21. Jain, A. K., Ross, A., & Prabhakar, S. (2016). An Introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
22. Jain, A., Purwar, A., & Yadav, D. (2021). Credit card fraud detection using K-Means and Fuzzy C-Means. Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies.
23. Jenipher, V.N., Dafni Rose, J., Sabharam, M., & Nithin, M.S. (2021). Learning algorithms with data balancing in credit card fraud detection application. 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 1-6.
24. Karim, L., & Boulmakoul, A. (2021). Trajectory-based modelling for fraud detection and analytics: foundation and design. 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), 1-7.
25. Kinslin, D. (2024). Impact of regulations on fintech firms/banking and non-banking financial services (pp. 371–428). https://doi.org/10.4018/979-8-3693-3803-2.ch015
26. Kuo, C., & Tsang, S. S. (2023). Detection of price manipulation fraud through rational choice theory: evidence for the retail industry in Taiwan. *Security Journal,* 36(4), 712-731.
27. Lacruz, F., & Saniie, J. (2021, May 14). Applications of machine learning in fintech credit card fraud detection. https://doi.org/10.1109/eit51626.2021.9491903
28. Magham, R. (2024). Mitigating bias in ai-driven recruitment: The role of explainable machine learning (XAI). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(5), 461–469. https://doi.org/10.32628/cseit241051037
29. Narsimha, B., Raghavendran, C.V., Rajyalakshmi, P., Reddy, G.K., Bhargavi, M.S., & Naresh, P. (2022). Cyber defence in the age of artificial intelligence and machine learning for financial fraud detection application. International Journal of Electrical and Electronics Research.
30. Protsak, K., & Kovalenko, T.O. (2022). FinTech and Commercial Banks: The Development Trends and Specifics of Cooperation. *Business Inform* 1(528), 131-137.
31. Razaque, A., Frej, M.B., Bektemyssova, G., Amsaad, F.H., Almiani, M., Alotaibi, A., Jhanjhi, N.Z., amanzholova, S., & Alshammari, M. (2022). Credit card-not-present fraud detection and prevention using big data analytics algorithms. Applied Sciences.
32. Roszkowska, P. (2020). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. Journal of Accounting & Organizational Change, 17(2), 164-196.
33. Sahri, Z., Shuhidan, S.M., & Sanusi, Z.M. (2018). An Ontology-Based Representation of Financial Criminology Domain Using Text Analytics Processing. *International Journal of Computer Science and Network Security*, VOL.18 No.2, February 2018
34. Saluja, S. (2022). Identity theft fraud- major loophole for fintech industry in India. *Journal of Financial Crime*, 6(2), 18-29.
35. Selvaraj, N.A. (2021). The essence of cybersecurity through fintech 3.5 in preventing and detecting financial fraud: A literature review. *Electronic Journal of Business and Management*6 Issue 2, 2021 pp. 18-29
36. Shoetan, P., & Familoni, B. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*, *6*(4), 602–625. https://doi.org/10.51594/farj.v6i4.1036
37. Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of System Assurance Engineering and Management*, *14*(6), 2120-2135.
38. Sreerama, J., & Krishnamoorthy, G. (2022). Ethical considerations in AI addressing bias and fairness in machine learning models. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (Online)*, *1*(1), 130–138. https://doi.org/10.60087/jklst.vol1.n1.p138

39. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors,* 21(5), 1594.
40. Tadesse, T. (2022). Combining control rules, machine learning models, and community detection algorithms for effective fraud detection. 2022 *International Conference on Information and Communication Technology for Development for Africa* (ICT4DA), 42-46.
41. Toshihiko, O., & Isamu, T. (2017). Enhancing fintech security with secure multi-party computation technology. *NEC Technical Journal*, 11(2).
42. Varma, P., Rupeika-Apoga, R., Nijjer, S., Grima, S., & Sood, K. (2022). Thematic analysis of financial technology (Fintech) influence on the banking industry. *Risks*, *10*(10), 186. https://doi.org/10.3390/risks10100186