International Journal of Open Publication and Exploration (IJOPE), ISSN: 3006-2853
Volume 12, Issue 1, January-June, 2024, Available online at: https://ijope.com

Integration of Blockchain Technologies with AI for Enhanced Payment Security

Pratik Badri[1], Anusha Nerella[2]

[1,2] Role: Independent Researcher

ABSTRACT

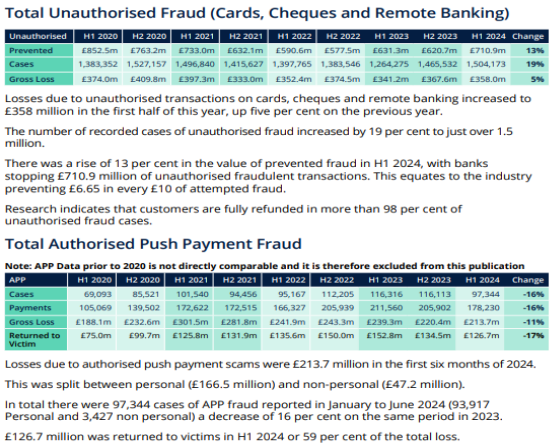
In order to enhance payment security, it is important to monitor and analyse each transaction made by the sender and the details of the payment receiver. It is too critical for a person to monitor each transaction continuously. For that reason, the organisation needs to adopt advanced technologies such as blockchain technology, artificial intelligence, and automation technologies to monitor and detect fraudulent transactions. These days people and multiple organisations are suffering through this financial fraud. This research aims to evaluate the role of blockchain and AI in enhancing payment security and to evaluate the effectiveness of integrating blockchain technology with AI. In order to develop the research a mixed method was chosen and data were collected from secondary sources. This study finds out the importance of blockchain technology and artificial intelligence to make transparent and secure transactions in the financial sector. It is important to adopt the technology after developing knowledge of the advantages and challenges of the advanced technology. This research will play an essential role in monitoring and preventing fraudulent activities during transactions and enhancing payment security.

Index Terms: Blockchain Technology, AI, banking fraud, fraudulent activities, advanced technology.

INTRODUCTION

A. Background of the study

This study focuses on preventing financial fraud and enhancing financial security by using the support of advanced technology such as blockchain technology and AI or artificial intelligence. It was noticed in 2024 that in the UK more than £570 million was stolen through payment fraud [1]. Unauthorised card fraud increased by 19% and crossed 1.5 million unauthorized cards, and unauthorized transactions increased by 5% more than the previous year [1] (Refer to Figure 1). In order to prevent these fraudulent activities and enhance payment security this research will highlight on adopting advanced technologies.



Total Unauthorised Fraud (Cards, Cheques and Remote Banking)

Unauthorised	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Prevented	£852.5m	£763.2m	£733.0m	£632.1m	£590.6m	£577.5m	£631.3m	£620.7m	£710.9m	13%
Cases	1,383,352	1,527,157	1,496,840	1,415,627	1,397,765	1,383,546	1,264,275	1,465,532	1,504,173	19%
Gross Loss	£374.0m	£409.8m	£397.3m	£333.0m	£352.4m	£374.5m	£341.2m	£367.6m	£358.0m	5%

Losses due to unauthorised transactions on cards, cheques and remote banking increased to £358 million in the first half of this year, up five per cent on the previous year.

The number of recorded cases of unauthorised fraud increased by 19 per cent to just over 1.5 million.

There was a rise of 13 per cent in the value of prevented fraud in H1 2024, with banks stopping £710.9 million of unauthorised fraudulent transactions. This equates to the industry preventing £6.65 in every £10 of attempted fraud.

Research indicates that customers are fully refunded in more than 98 per cent of unauthorised fraud cases.

Total Authorised Push Payment Fraud

Note: APP Data prior to 2020 is not directly comparable and it is therefore excluded from this publication

APP	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,316	116,113	97,344	-16%
Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,902	178,230	-16%
Gross Loss	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£213.7m	-11%
Returned to Victim	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	£134.5m	£126.7m	-17%

Losses due to authorised push payment scams were £213.7 million in the first six months of 2024.

This was split between personal (£166.5 million) and non-personal (£47.2 million).

In total there were 97,344 cases of APP fraud reported in January to June 2024 (93,917 Personal and 3,427 non personal) a decrease of 16 per cent on the same period in 2023.

£126.7 million was returned to victims in H1 2024 or 59 per cent of the total loss.

Figure 1: Fraudulent activities in the UK financial sector (Source: [1])

B. Overview

Blockchain helps by offering decentralised, unbreakable ledgers which play an essential role in enhancing transparency and security [6]. On the other hand, AI or Artificial intelligence helps to detect real-time fraud and is capable of adopting security measures to prevent fraud [6]. The integration of both blockchain technology and artificial Intelligence collaboratively can monitor transactions, detect fraud, and support in preventing fraud by adopting security measures.

C. Aim and Objectives

This research aims to evaluate the integration of blockchain technology with AI and to enhance payment security, reduce fraud risk, and improve transaction reliability. 1)To find out and evaluate the liability in existing digital payment security frameworks. 2) To evaluate the role and importance of blockchain and AI in enhancing transaction security. 3) To identify blockchain technology and AI's limitations and way outs in preventing transaction fraud.

D. Problem statement

Multiple organisations and governments give high effort to develop advanced cyber security to protect financial funds but still nowadays this is one of the major challenges. The traditional fraud detection method was unable to defeat sophisticated cyber-attacks due to its rule-based system [7]. On the other hand, the centralised payment system is possible to break, manipulate, and can fail while functioning. In order to prevent the advance of cyber fraud and financial fraud it is important to develop secure, advanced, intelligent, and decentralized solutions or technology that can reduce the risk of fraudulent activities, and enhance reliability in digital platforms.

E. Scope and Significance

It is important to develop research on the importance of blockchain technology and artificial intelligence to prevent cyber fraud and financial fraud. On the other hand, this research will play an important role in guiding researchers, and banking sectors to get to know about the importance of advanced technologies and the limitations of the advanced technologies to prevent financial fraud.

LITERATURE REVIEW

A. Integration of blockchain and artificial intelligence for revolutionizing security and transparency in finance

This research highlights the integration of blockchain technology and artificial intelligence that helps to enhance security, and transparency in the financial sector and plays a role in preventing payment fraud. The immutable ledger and decentralised factors of blockchain help to conform the unbreakable transaction records, and figure out the liability in the traditional financial system [2]. AI helps to make predictive analysis, automation and machine learning, risk assessment, real-time data analysis, and decision-making while monitoring financial operations to detect fraudulent transactions and prevent them [4]. These advanced technologies introduce processes such as Anti-Money Laundering (AML) and Know Your Customer (KYC) where the organisation can store the data of customers by using blockchain [2].

With the help of AI or Artificial Intelligence organisations monitor transactions to detect suspicious activities and transactions (Refer to Figure 2). The factors and the technologies that help to reduce the dependency on intermediate, and human error automated contractual agreements, smart contracts, and blockchain play an essential role. On the other hand, AI helps to enhance the adaptability of the above-mentioned factors to market conditions [2]. This integration of Artificial intelligence with blockchain technology develops a transparent financial transaction and helps to prevent financial fraud.

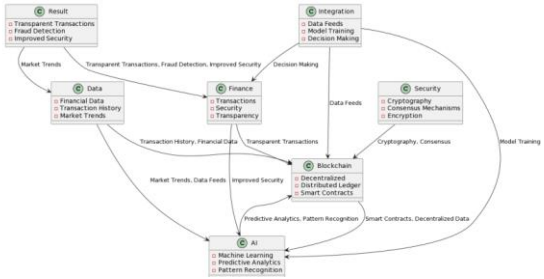


Figure 2: Blockchain and AI integration for revolutionising payment security and transparency (Source: [2])

Multiple literature highlights the theoretical benefits of integrating AI with blockchain technology in finance. The limitation is that the research does not highlight the empirical studies that focus on real-world applications and findings from the integrations. Future research needs to highlight the case studies and pilot projects that use this advanced technology and provide real-life evidence of the effectiveness of advanced technologies that help to enhance transparency and security in the financial sectors.

B. Enhancing secure financial transactions with the help of blockchain and artificial Intelligence

Some literature found that discusses the fundamental principles of blockchain technology and artificial intelligence. Blockchain helps to offer a transparent, secure, and unbreakable system that works to record transactions. On the other

hand, artificial intelligence or AI helps to process vast amounts of data to identify fraudulent activities and to prevent fraud. Studies discuss the utilisation of advanced technologies in supply chain management, the financial sector, and healthcare [3]. On the other hand, the challenges were also discussed such as regulatory uncertainties, scalability issues, and the requirement of standardisation. This study highlights collaboration the advanced technologies to develop harmless and sure processes [3].

Figure 3: Application of blockchain in business (Source: [3])

Multiple research projects have not highlighted the practical implication of the strategies on businesses, especially SMEs. SMEs always face challenges in adopting advanced technologies due to the shortfall of financial abilities. On the other hand, the literature does not highlight real-life case studies and ethical consideration factors of using advanced technologies in the financial sector.

METHODOLOGY

A. Research Design

According to the Saunders research onion, this study uses the explanatory research design to explain the implantation and integration of Blockchain technology with artificial intelligence in enhancing payment security. On the other hand, a mixed method approach is effective in evaluating qualitative case studies and real-life examples after the implication of the different technologies [9] (Refer to Figure 4). On the other hand, the quantitative method helps to analyse the statistical data and statistical findings after implementing advanced technology in the banking sector.

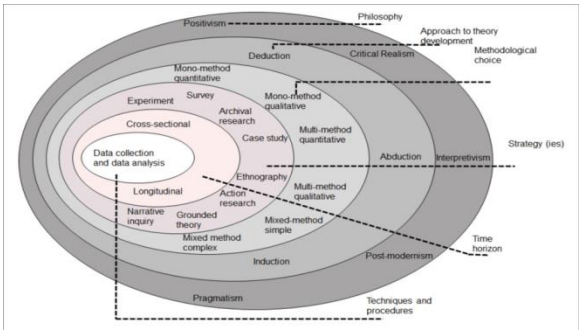


Figure 4: Saunders Research Onion [Source: 8]

B. Data collection

This study focuses on collecting secondary data through qualitative and quantitative methods. In the qualitative method, the sources of secondary data are peer-reviewed journals, and the sources of quantitative data are statistical reports from authenticated and verified sources. While collecting the data the Data Protection Act 2018 and cybersecurity factors are two ethical factors that ensure the reliability and trustworthiness of the coveted data.

C. Case studies and example

Case study 1: Technology adoption of HSBC

HSBC is one of the leading baking organizations in the UK. The company adopted AI technology to detect fraud traction. The company adopted the AI technologies offered by Ayasdi and Quantexa and as a result, the organisation achieved a reduction of 20% in fraudulent transactions with the help of AML or Anti-Money laundering detection [10]. This technology utilisation helps the bank to monitor and analyse the data of transactions, figure out suspicious activities and operations, help the bank to process complicated operations, and enhance overall payment security.

Case study 2: Technology adoption of Elliptic

Elliptic is a blockchain analytics company that is capable of managing crypto-asset compliance and able to detect fraud by monitoring transactions. The company adopted AI or artificial intelligence to identify fraudulent activities and to analyse blockchain transactions [11]. This solution developed by Elliptic helps to overcome the risks during cryptocurrency transactions and enhance payment security in the banking sector.

D. Evaluation metrics

In order to evaluate the effectiveness of blockchain technology and artificial intelligence it is important to use some evaluation metrics which help to find out the fraudulent activities and help to escape from fraud. Fraud Detection rate helps to measure fraud transactions. A high rate indicates improvement in preventing fraud [12]. A false positive rate helps to find out the frequency of legitimate transactions that are mistakenly marked as fraud. A low rate indicates better accuracy.
Transaction processing speed helps to evaluate the efficiency of a particular system in processing payments securely without any delay. Other metrics are system scalability, blockchain latency, data integrity score, regulatory complaint rate, and user trust and adoption rate. All these above-mentioned matrices play an essential role in monitoring transactions, identifying fraud activities., preventing the activities, and securing the transactions.

RESULTS

A. Data Presentation

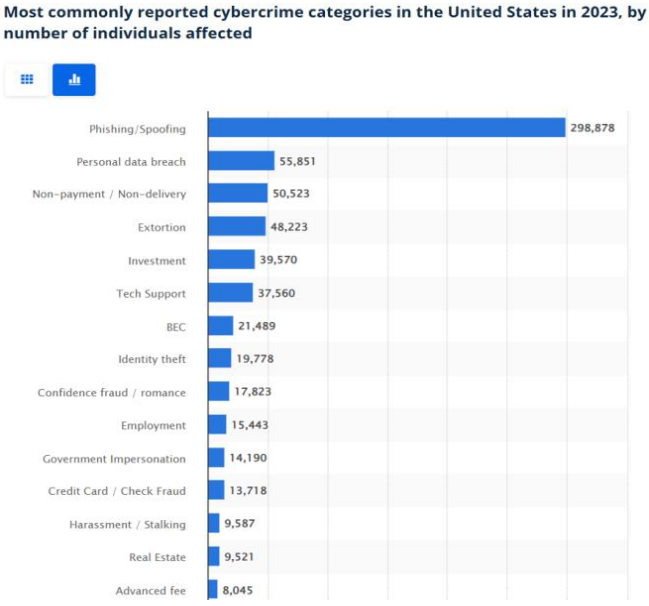


Figure 5: Cybercrime in the US in 2023 (Source: [13])

According to Figure 5, it can be evaluated that in 2023 people in the US faced multiple cybercrime challenges. Many people suffered due to the difficult fraudulent activities. It was found through a survey that in 2023, 298,878 people suffered due to phishing and spoofing issues and 55, 851 people suffered because of data breach issues [13]. In the financial sectors, while making any investment 39,570 people faced fraudulent activities, and 13,718 people faced challenges of cybercrime related to their credit card and check frauds [13]. It was also noticed that in 2023, 50,523 people faced cybercrime issues on non-payment and non-delivery related issues.

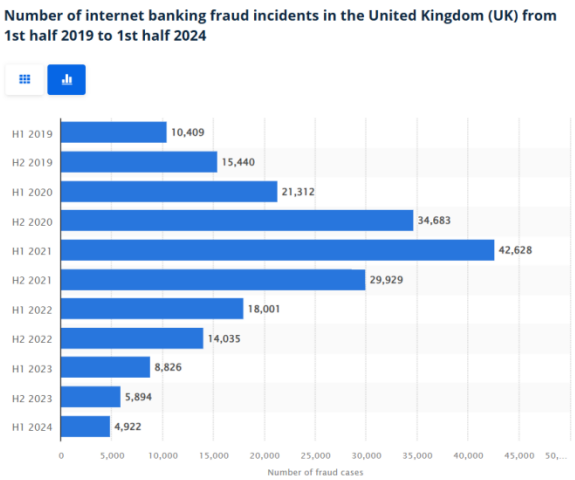


Figure 6: Internet banking fraud in the UK from 2019 to 2024 (Source: [14])

According to Figure 6, it can be evaluated that in the UK internet banking fraud will become a huge challenge from 2019 to 2023. In the first half of 2021, a total of 42,628 Internet banking frauds were detected [14]. Also, in the second half of 2020, the count was 34,683, and in the second half of 2021, the count was reduced and 29,929 fraud cases were found related to Internet banking fraud [14].

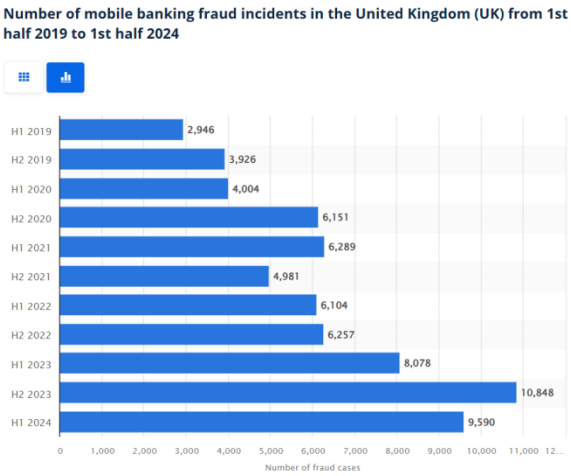


Figure 7: Mobile banking fraud in the UK from 2019 to 2024 (Source: [15])

According to Figure 7, it can be evaluated that, in the first half of 2023 8,078 fraud mobile banking cases were detected and in the second half of 2023 total of 10,848 cases were found in the UK in the first half of 2024 total of 9,590 fraud cases was found on mobile banking issues [15].

B. Findings

From the overall collected data, it can be concluded that people in developed countries like the US and the UK have faced multiple cybercrime issues over the last five to six years. It is found that in the US people face multiple types of cybercrime issues which will affect millions of people in 2023. Within the multiple cybercrime-related issues 298,878 people face challenges due to phishing and spoofing issues and 39,570 people are affected due to investment-related fraud [13]. On the other hand, it was observed that in the UK in the first half of 2021, 42,628 fraud cases were found and in the second half of 2021 the count reduced and came to 29,929 fraud cases [14]. These differences can highlight the efforts and initiatives taken by the government and the banking sectors to reduce fraud cases and to develop a transferable and secure transaction to develop the trust of people. It was also noticed from the graph mentioned in Figure 6 that in 2024 the Internet banking fraud cases will become 4,922 [14]. This number shows the achievement of the government and banking sectors. On the other hand, in the second half of 2022, a total of 6,257 fraud cases were detected on mobile banking fraud, and in the second half of 2023, it became 10,848 mobile fraud cases were found. It was noticed that in the first half of 2024, the

count became 9,590 [15]. This calculation highlights that mobile banking fraud increases every year in the UK. The government and banking sectors need to take care of the security factors in mobile banking.

C. Case study outcomes

In order to enhance fraud detection HSBC adopted AI and blockchain technology and succeeded in reducing 20% of false positives in AML (Anti-money laundering) screening. This advanced technology adoption helps to assure transaction security and develop compliance efficiency [10]. The adoption of AI and blockchain technology helps to detect suspicious activities and reduce financial fraud to offer a transparent and secure payment process to consumers.

On the other hand, Elliptic, who has special expertise in crypto asset compliance, adopted AI to analyse blockchain transactions and detect fraudulent activities. In real time the AI algorithms used by Elliptic are capable of identifying fraud activities [11]. This technology helps financial organisations to prevent crypto currency related risk and conform to high data integrity and compliance with financial regulations.

D. Comparative Analysis

Table 1: Comparative Analysis

Sources	Focus	Findings	Gap
[2]	This paper focuses on the usefulness of blockchain technology and AI in ensuring transparency and security in the financial sector.	This study discusses who possesses advanced technology such as blockchain ensures data integrity and highlights the effects of AI. This research highlights that AI helps in predictive analysis and helps to monitor financial transactions. The collaboration of advanced technologies supports streamlining KYC and AML processes, works in detecting fraudulent activities, and develops smart contracts.	It is found this research does not highlight the ethical and regulatory implications of adopting this advanced technology which is essential for future research.
[3]	This paper focuses on the IBAI framework or integrated blockchain and artificial intelligence framework to develop transparency and security in financial transactions.	This study discusses a blockchain decentralized process that helps to store unbreakable data and discusses the utilization of AI's predictive analysis to monitor and detect real-time fraudulent activities and risk assessment. This research finds that the integration of advanced technologies helps to improve transparency and security in the financial sector.	This research discusses the challenges of blockchain technologies and AI models but does not make any in depth analysis on the way out to overcome the challenges. Also not discuss the real-life example of the technology implications in the financial sectors.
[4]	This research focuses on predictive analysis and machine learning to overcome risk and develop agility.	This research finds that predictive analysis and machine learning help in risk assessment, demand forecasting and inventory management.	This research does not highlight and not discuss the limitations of adopting the technology for SMEs (Small, and medium-sized entrepreneurs)
[5]	Focus on the importance of AI frameworks, serverless computing and AI-as-a-service models.	Finding out that the main challenges are in data privacy, system interoperability, AI bias and regulatory compliance offers a comprehensive understanding of scalability factors.	This study does not highlight real-life examples and does not discuss the SMEs who are facing these challenges.

(Source: self-developed)

This comparative analysis highlights the findings, focus, and gaps of the above-mentioned literature used in the literature review section. This analysis helps to understand the findings of the efficient researchers who study the importance and effectiveness of advanced technologies.

DISCUSSION

A. Interpretation of Results

The discussed sources focus on the importance of blockchain technology and Artificial intelligence in enhancing security and transparency in the financial sector. All the research discusses the effectiveness of advanced technologies in monitoring transactions, detecting financial fraud, and preventing fraudulent activities. It is clear from above mentioned discussion that Blockchain technology helps to store the data of customers which is critical to breaking security [16]. On the other hand, AI helps monitor, detect, and prevent fraudulent activities during transactions. It is also found that developed countries like the US and the UK have faced challenges of cyber surety and financial fraud issues for the last 6 years and are working on overcoming the challenges.

B. Practical Implications

Advanced technologies like blockchain technology and AI are used by the financial sector to prevent financial fraud. It was noted that HSBC adopted the AI technologies offered by Ayasdi and Quantexa and as a result, the organisation achieved a reduction of 20% in fraudulent transactions with the help of AML or Anti-Money laundering detection [10]. On the other hand, Elliptic adopted blockchain technology and Artificial intelligence to identify fraudulent activities and to analyse blockchain transactions.

C. Challenges and Limitations

It is found from the overall discussion that there is limited research on the research topic that discusses real-life examples. Several researchers have not discussed the banking organisations that are using advanced technologies and real-life examples to discuss the advantages and disadvantages of using AI and blockchain technology. It can evaluate that multiple literatures discuss the definition, utilisation, importance, and challenges but without focusing on real-life examples.

This study adopts the mixed method approach to analyse the findings. This research uses secondary sources like statistical data, and peer-reviewed journals and authenticates a verified source to evaluate the effectiveness of implementing blockchain technology and artificial intelligence. The limitation of this research is that it does not collect any primary data to understand the opinions and experiences of professionals who use the advanced technologies and have knowledge of the practical experience of using the advanced technologies.

D. Recommendation

From the overall discussion, it can be evaluated that before adopting the advanced technologies the financial organisations need to study both the importance and challenges of the technologies. Also, financial organisations develop risk mitigation strategies to overcome the risk of AI and Blockchain technology from cyber threats and data breach issues.

CONCLUSION AND FUTURE WORK

It can be concluded that AI and blockchain technology play an essential role in offering transparent and secure transactions in the financial sector. The advanced technologies help to reduce financial fraud through the unbreakable data storage features of blockchain and the mentoring, detecting, and preventing activities of artificial intelligence. In banking sectors and any kind of financial transactions and payment-related concerns, this advanced technology helps to secure the data and transactions process of customers.

This research will play an essential role in guiding future researchers to study the importance and effectiveness of using blockchain technology and artificial intelligence. Also, will guide how to collaborate both of the technologies in the financial sector. This research also highlights real-life examples which can enhance the understanding of future researchers and banking organisations.

REFERENCES

[1] Rane, N., Choudhary, S. and Rane, J., 2023. Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. Available at SSRN 4644253.
[2] Xuan, T.R. and Ness, S., 2023. Integration of Blockchain and AI: exploring applications in the digital business. Journal of Engineering Research and Reports, 25(8), pp.20-39.
[3] Aljohani, A., 2023. Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. Sustainability, 15(20), p.15088.
[4] Prosper, J., 2021. Scalable AI Architectures for E-Commerce and Retail. https://www.researchgate.net/profile/James-Prosper-2/publication/389730113_Scalable_AI_Architectures_for_E-

Commerce_and_Retail/links/67d00dd3d75970006507aab7/Scalable-AI-Architectures-for-E-Commerce-and-Retail.pdf

[5] Potla, R.T., 2023. AI in fraud detection: Leveraging real-time machine learning for financial security. Journal of Artificial Intelligence Research and Applications, 3(2), pp.534-549. https://www.researchgate.net/profile/Ravi-Teja-Potla/publication/389057213_AI_in_Fraud_Detection_Leveraging_Real-Time_Machine_Learning_for_Financial_Security/links/67b3688696e7fb48b9c5a51b/AI-in-Fraud-Detection-Leveraging-Real-Time-Machine-Learning-for-Financial-Security.pdf

[6] Saunders, "Research onion (Saunders et al., 2019, p. 108).," *ResearchGate*, 2019. https://www.researchgate.net/figure/Research-onion-Saunders-et-al-2019-p-108_fig1_349083776

[7] M. A. S. Toyon, "Explanatory Sequential Design of Mixed Methods research: Phases and Challenges," *International Journal of Research in Business and Social Science (2147- 4478)*, vol. 10, no. 5, pp. 253–260, Aug. 2021.

[8] W. Hilal, S. A. Gadsden, and J. Yawney, "A Review of Anomaly Detection Techniques and Applications in Financial Fraud," *Expert Systems with Applications*, vol. 193, no. 1, p. 116429, Dec. 2021, doi: https://doi.org/10.1016/j.eswa.2021.116429.

[9] Chintale, P. (2023). DevOps Design Pattern: Implementing DevOps best practices for secure and reliable CI/CD pipeline (English Edition). Bpb Publications.

[10] Nerella, A. (2024). Leveraging Quantum Machine Learning to Optimize High-Frequency Trading Strategies in US Treasuries and Forex Markets. International Journal of Information and Electronics Engineering, 14(4), 20-28.

[11] Venna, S. R. (2024). Next-Generation Regulatory Operations: Trends in AI, Data, and Automation. Available at SSRN 5270687.

[12] Yugandhar, M. B. D. (2023). Automate Social Sharing with Meta platform, Google feed, Linkedin feed, Google News, Fb, Instagram, Twitter. International Journal of Information and Electronics Engineering, 13(4), 7-15.

[13] Bucha, S. DESIGN AND IMPLEMENTATION OF AN AI-POWERED SHIPPING TRACKING SYSTEM FOR E-COMMERCE PLATFORMS.

[14] A. Petrosyan, "U.S. most frequently reported cybercrime by number of victims 2022," *Statista*, Aug. 29, 2023. https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/Petrosyan, "UK mobile banking fraud H1 2023," *Statista*, 2024. https://www.statista.com/statistics/1426193/uk-mobile-banking-fraud-incidents/

[15] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Future Internet*, vol. 14, no. 11, 2022, doi: https://doi.org/10.3390/fi14110341.