[1]Sina Ahmadi

Advancing Fraud Detection in Banking: Real-Time Applications of Explainable AI (XAI)

Journal of Electrical Systems

Abstract: - Technological and regulatory changes have transformed the digital footprints of the banking sector. Today, credit card transactions are providing ten times more data available for fraud detection practices than it was previously available. These larger datasets, combined with the limitations of traditional fraud detection methods, creates an opportunity to adopt Artificial Intelligence (AI) techniques. The effectiveness of AI models in the banking industry for fraud detection is proven but practitioners are slow to adopt this advancement. This was because of the concerns over transparency, trust, and the complexity of integrating these models into existing systems. This paper aims to argue in favor of Explainable Artificial Intelligence (XAI) for fraud detection in the banking sector. XAI enhances transparency, builds trust, and provides clear insights by making AI decisions interpretable and understandable, allowing users to see how and why decisions are made. This paper will explore real-time applications of XAI in the banking sector. It will also highlight the key regulatory changes necessary for effectively integrating AI techniques into banking practices. Lastly, it will encourage future researchers to investigate various aspects of XAI and its potential contribution to improving fraud detection in the banking industry.

Keywords: Artificial Intelligence; explainable artificial intelligence; banking; fraud detection; credit card.

I. INTRODUCTION

According to a Serious and Organized Crime Threat Assessment by Europol, non-cash payment fraud in banks is one of the most threatening criminal activities in the European Union [1]. In the UK in 2020, fraud losses on UK-issued credit cards from different banks totaling £567 million. Comparatively, global losses as a result of fraud totaled $32.39 billion in 2020 and are expected to cross over $40 billion by 2027 [2]. Over time, the use of online payment transactions and non-cash payments through credit cards is increasing, similarly, opportunities for perpetrators involved in fraudulent activities are increasing. To control the increasing fraud rate in the banking sector, the integration of real-time AI for detection and prevention is crucial.

A. Changing Landscape

The velocity and volume of fraud happening in the banking industry during transactions and finance management means that banks cannot rely on human expertise to identify and prevent fraudulent transactions. Fraud Management Systems (FMS) manage internal processes by automating fraud detection and decision making. FMSs working on traditional rule-based algorithms ensure that every transaction is being checked against predetermined rules. It is a satisfactory approach that enables finance managers to track inputs, modify rules, and interpret results to ensure the finance management process is free of fraud and unauthorized access. Along with advancements in the finance management processes patterns of fraud are also evolving. Perpetrators are not using simple techniques to target datasets but they are also careful and advancing to launch attacks that are difficult to predict and prevent. The changing landscape of fraud in the payment industry has brought numerous challenges that need an immediate solution. A radical change in fraud detection methods is required to prevent losses.

The United Kingdom and Europe have implemented Strong Customer Authentication (SCA), regulatory standards designed to enhance the security of customer transaction data processing [3]. One of the most important challenges linked with SCA is that the issuers receive a limited amount of data from retailers for fraud detection. To extend the amount of transaction data available for issuers a new regulatory technical standard has been introduced titled, "Authentication Enrichment" which is about 100 variables a retailer should provide to an issuer [4]. The tenfold increase in the data available for fraud detection highlights a step change in the traditional rule-based methodologies. Traditional rule-based methodologies can continue to perform transaction screenings to avoid the

[1], The University of Melbourne, Australia

sina@eml.cc

most common fraud approaches while machine learning (ML) and artificial intelligence (AI) will be integrated into screening for fraud detection and prevention.

Technological developments are revolutionizing the payment industry and the way people pay for goods and services. Contactless technology has transformed the payment system through innumerable digital payment platforms such as Apple Pay, Samsung Wallet, Google Pay, etc. These digital payment transaction platforms have heavy customer (young generations) leads. Using these payment platforms payment is being made through cards, mobile phones, and by scanning any device. These advancements in the payment industry are supporting the flexibility needed to establish the future transaction landscape. Similarly, changing payment methods and gateways need advanced fraud detection systems in place because traditional rule-based fraud detection systems are less effective in tracking fraudulent activities across devices and online databases [5].

Hence, the need for advanced FMS in place has proven to be critical. Rule-based fraud detection systems were doing well in fraud detection until systems were not as complex and sensitive as they are today. To match the changing technical dynamics of the payment industry machine learning (ML) powered fraud detection systems are required.

B. Current Status

To address the challenges in the banking industry, changes in regulations, technology savvy criminal activities and to employ beneficial technological advancements researchers are exploring the opportunities to employ machine learning techniques in fraud detection. However, the adoption and integration of machine learning techniques in financial settings have been slow because banking organizations perceive ML techniques as a black-box solution that lacks transparency [6]. In the financial sector, organizations are choosy and careful because a wrong decision could be highly impactful. For example, in case of a credit card fraud, a consumer's transaction would be rejected and the credit card would be cancelled. It would result in annoyance and embarrassment for the organization and at the same time, it would impact the consumer's ability to use his financial resources to keep up with payments. The existence of these real-life cases and the impact they have on consumers and the payment industry places a stronger emphasis on industry players to integrate machine learning models and trust the process. In the finance industry, the lack of trust in machine learning models for fraud detection and prevention and the inability to integrate these models into practice is one of the biggest barriers to change.

To encounter this challenge, researchers are exploring ways in which ML models can effectively detect and prevent payment fraud and provide transparency as well as encourage adoption at a higher level. A well-known emerging technique to show transparency is Explainable Artificial Intelligence (XAI).

II. LITERATURE REVIEW AND BACKGROUND

Scholarly research surrounding XAI is limited because the majority of authors restrict themselves to committing to one definition of the XAI system. This is because it is an emerging terminology and the community of researcher’s need to agree on one definition of XAI [7].

Research by Gunning & Aha (2019) provides a holistic definition of XAI as, "Artificial Intelligence is a system with rationale that can be explained to humans, characterizing their strengths and weaknesses, and provides an understanding of how they can behave in future” [8]. This definition simply states that artificial intelligence models are explainable and interpretable.

With the ongoing debate on the exact definition of XAI, many authors and their work are underrated. Within the machine learning community, XAI models are popular research topics. Fraud detection in the finance industry lacks research focus. This explains why only one research paper published in the last 20 years discusses the application of machine learning and XAI in the context of fraud detection black boxes. The authors of this paper propose a solution to the black box issue that practitioners face when integrating machine learning models into the payment industry for fraud detection. The difficulty humans face as a result of credit card fraud explains the output they could receive in a format that humans can understand.

In the payment industry banks are facing enormous challenges when it comes to protecting online transactions and online banking databases. It is difficult to keep customer data secure while keeping the login process simple and convenient. Banks are introducing a myriad of passwords, security measures, and different communication tools that discourage customers from using online banking [9]. According to a fraud survey conducted in 2011, to reduce fraud in the banking industry it is important to detect those in real-time, analytics should be in place with an efficient rules engine [10].

According to Sakib (2018), 49 people in Bangladesh customers of non-government commercial banks have lost about $2 million when their money was withdrawn by fraud gangs from the bank using duplicate debit or credit cards [11]. Some research studies highlight that numerous customers of the government and non-government banks faced credit card fraud [12]. Another study claims that about 30% of banks are at high risk of security threats and online fraud. The study pointed out that payments through ATM and plastic card transactions are posing challenges for customers with 25% of customers facing and experiencing fraudulent activities while using online banking applications [13].

A. Credit Cards Operating Landscape

Credit card transactions proceed in two conditions: Cardholder Present (CP) and Cardholder Not Present (CNP) transactions. To proceed with CP transactions a customer would be physically present and provide the plastic card to the retailer for payment. For CNP transactions the purchase can be carried out remotely without the customer present on location through an e-commerce website. The simplicity by which a customer uses a credit card to make payments has a complex operating landscape at the backend. Multiple organizations interact to ensure a positive and smooth customer experience. Fig 1 illustrates the five organizations involved and the timing they execute their role to initiate credit card functioning.

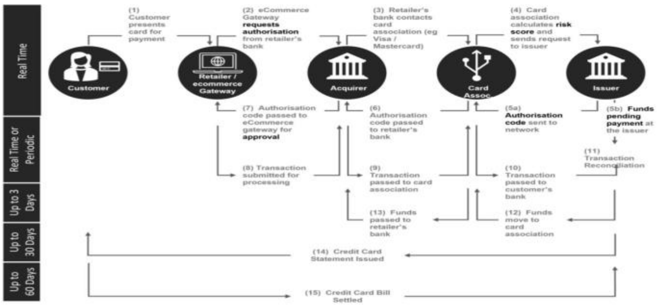

Real Time
Real Time or Periodic
Up to 3 Days
Up to 30 Days
Up to 60 Days
Customer
Retailer / ecommerce Gateway
Acquirer
Card Assoc
Issuer
(1) Customer presents card for payment
(2) eCommerce Gateway requests authorisation from retailer's bank
(3) Retailer's bank contacts card association (eg Visa / Mastercard)
(4) Card association calculates risk score and sends request to issuer
(5a) Authorisation code sent to network
(5b) Funds pending payment at the issuer
(6) Authorisation code passed to retailer's bank
(7) Authorisation code passed to eCommerce gateway for approval
(8) Transaction submitted for processing
(9) Transaction passed to card association
(10) Transaction passed to customer's bank
(11) Transaction Reconciliation
(12) Funds move to card association
(13) Funds passed to retailer's bank
(14) Credit Card Statement Issued
(15) Credit Card Bill Settled

Fig 1. Credit Card Transaction Lifecycle

The first step of the credit card transaction is when a customer provides credit card details to a retailer in exchange for a product or service. In real time the retailer asks for permission from the issuer and receives an authentication code. At this point, permission could be granted or declined based on the information provided. The response from the reader would be completed within seconds.

In case the permission is granted, the retailer will receive funds from the credit card issuer within three days. The issuer will record the transaction on the credit card statement and share the statement after thirty days of the transaction. The cardholder then fulfills the credit card payments within thirty days through the bill or using the credit card facility [14].

The goal of real-time fraud detection is to ensure that every transaction made through credit cards and online banking is free from fraud. Fraud analysis focuses on checking and confirming the authenticity of each transaction before it proceeds. The retailer, issuer, and acquirer everyone have different roles to play. These roles are similar but provide multi-dimensional views of a transaction to confirm the validity of a transaction. Table 1 shows how various individual roles contribute to providing a holistic overview of a transaction to confirm its validity.

Table 1. Organizations with their credit card fraud detection datasets

Organization	Fraud Dataset
Retailer	Previous purchases and customers

Acquirer	Transaction with every retailer linked to the bank
Cardholder	Transactions using the card brand
Issuer	Transactions from every customer using issuer cards

In real-time the role of retailers, acquirers, cardholders and issuers is equally important for fraud detection and prevention.

B. Key Challenges

Fraud Management System (FMS) that retailers are using for fraud detection poses four major challenges that complicate the fraud detection process during transactions that should be addressed to avoid operational difficulties. Four key challenges are as follows;

1) *Real-time Analysis:* Modern technology is providing hundreds of ways to improve the security infrastructure of the payment industry. It provides layers of security to protect the information of customers during a transaction. However, to show adherence to technical regulations and to deliver a smooth checkout experience to customers along with minimizing losses at e-commerce gateways Modern security features need to be processed in real-time [15].

   Fig 1 illustrates the online transaction process from steps 1 to 7.

   Retailers want to provide a hustle-free checkout experience to customers for all transactions. According to a survey, almost 20% of customers decide to abandon their shopping carts due to sticky checkout experiences [16]. The negative checkout experiences negatively affect future purchases of customers which leads to decreased overall revenue.

2) *Concept Drift:* Real-time fraud detection and analysis enables timely decision-making and prevention. In the past, fraudulent activities and the manner in which these activities used to happen had been consistent. Comparatively, modern fraud and fraudsters have been strong enough to detect and prevent. Concept drift is a term that is used to describe the changing landscapes and circumstances. Changing patterns and circumstances in the fraud catalog means existing fraud detection and prevention systems are outdated and ineffective. As a consequence fraud detection and prevention becomes less effective.

3) *Minimize False Positive:* Sometimes a model could indicate a positive result that would be known as a false positive result. To maximize positive checkout customer experiences fraud investigators should work to minimize false positives. False positives are crucial to eliminate or minimize because they create friction in the checkout process by disturbing the real-time transactions or canceling out at the same time. As a consequence, it affects the customer experience and sales volume [17]. Implementation of XAI solutions can provide transparency to highlight the reasoning behind a false positive result.

4) *Class Imbalance:* Fraudulent transactions are affected data points that exist between the large groups of genuine transactions. According to a report by Mark Nelson, a senior vice president of Visa’s Risk Products and Business Intelligence, Visa operates at a 0.1% fraud rate for transactions [18]. The report for the states that having imbalanced datasets creates difficult difficulties to integrate machine learning models with the data because algorithms keeps an equal distribution of each class. When the most important class would be in the minority during fraud detection it would result in poor predictive performance. Scholars have highlighted several approaches to address class imbalance. One most effective techniques is under-sampling the majority class and oversampling the minority class to maintain the balance. There are a number of other techniques available that can be used to highlight terminating classes in datasets to ensure effective detection [19].

Retailers are responsible for ensuring the authenticity of customers before proceeding with online payments. Integration of artificial intelligence models in real-time helps to identify and access fraud occurrences at any given time. Fig 2 illustrates the process of fraud scoring by a retailer and highlights inputs to the risk [20].

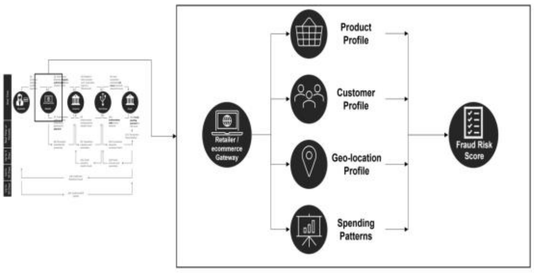


Fig 2. Illustration of the Retailer/e-commerce gateway process for fraud detection/scoring

This section provided a detailed understanding of practical constraints that occur during real-time analysis. From managing unbalanced datasets, concept drift, and minimizing false positives the section helped to understand the challenges that need immediate solutions to avoid or eliminate fraudulent activities from the banking industry. The following section will provide a detailed understanding of the problem and available solutions that can be implemented in real time in the banking industry.

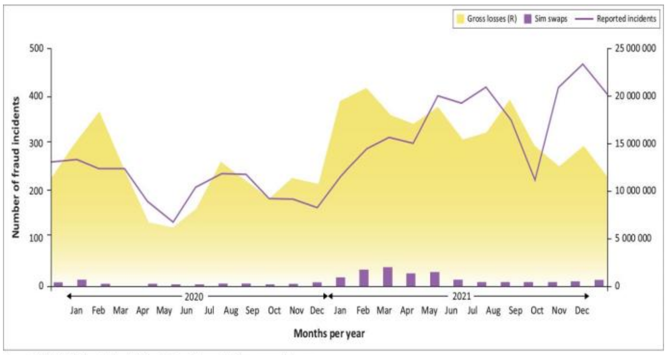
Hence, XAI lacks a research focus. This paper will address the gap by arguing in favor of XAI techniques and their ability to create change in the payment industry for fraud detection and prevention. This research will suggest how XAI can be adopted to address challenges in payment fraud detection.

The following section of the paper will highlight some literature that supports the implementation of ML techniques for fraud detection and prevention.

III. PROBLEM DEFINITION

Online banking, while offering convenience and accessibility, has also introduced new security challenges. While both customers and banks benefit from the ease of digital transactions, the risk of fraud associated with online banking and credit card usage cannot be overlooked. This dilemma poses a threat to the security and privacy of both individuals and financial institutions. The financial institutions and banking sectors are enduring yearly losses as a result of fraudulent crimes. According to the annual crime statistics, online banking fraud makes up the smallest portion of incidents compared to digital banking crimes. It is the second-highest crime, accounting for up to 45% of total losses.

Fig 3, provides yearly statistics of online banking crimes and highlights the rate of crimes increasing every year.



Source: SABRIC, 2021, *Annual crime statistics 2021*, p. 1, viewed n.d., from www.sabric.com

FIGURE 2: Online banking yearly statistics report.

Fig 3. Yearly statistics for the online banking fraud crimes [21]

The literature review and background analysis clearly show that existing fraud management systems (FMS) are outdated and ineffective at detecting and preventing online banking fraud. In the banking sector and financial institutions, additional security measures are necessary to authenticate a customer’s identity before proceeding with online transactions. XAI is an effective tool to enhance existing security protocols in the banking industry and could eliminate fraudulent activities by detecting and analyzing on time [22].

This section outlined the problem under discussion, based on the literature review and background analysis. The next section presents the research focus and objectives, explaining the motivation behind the study and the challenges faced.

IV. RESEARCH AGENDA

The focus of this research is to discuss real-time applications of XAI in the banking industry. Implementation of XAI in real-time would be helpful towards a step change in fraud detection and prevention. To understand existing trends on this topic, existing literature was reviewed. Articles and journals were accessed using the keywords ‘fraud in the banking industry’ and ‘credit card frauds.’ There are few types of research available that were relevant to the research focus. Relevant articles and literature were excluded from the resources to evaluate existing approaches regarding fraud detection and prevention in the banking industry.

Literature analysis supports the fact that existing research fails to highlight real-time challenges that exist in fraud detection and prevention in the banking industry. When designing AI solutions and implementing XAI models having a fraud operating environment in mind is important. It helps in the focused adoption and implementation of solutions in real time [23].

This research aims to contribute towards a step change in the banking industry by ensuring that XAI is designed and implemented by keeping the context in mind. Adherence to challenges customers are facing in real time enhances the practical use of XAI models. It would be possible only when developers would be aware of customer’s concerns about using credit cards and online banking.

V. DISCUSSION

A. XAI in fraud detection

As online banking crimes become more prevalent, real-time adaptability and responses become necessary. The integration of XAI emerged as a step-change in the banking industry. In the field of fraud detection, AI transformed manual detection systems into automatic systems. With the increasing volume and velocity of online banking and financial transactions, there was a huge need for automatic FMS that could analyze large datasets and identify fraudulent activities in real time [24]. XA-powered fraud detection systems are efficient, speedy, and scalable. AI plays a crucial role in automating the analysis of transactional data, and fraud detection process. It helps in detecting anomalies and misleading patterns that indicate the occurrence of fraud with invalid accuracy. The XAI model involves training an artificial intelligence model on labeled datasets where it learns about patterns associated with both a fraudulent and a legitimate transaction. This trained model then makes predictions about unseen datasets regarding authenticity and accuracy. Natural Language Processing (NLP) one of the facets of AI has numerous applications in fraud detection. NLP algorithms can identify and analyze textual data such as transaction descriptions and communication records to access linguistic patterns linked with fraudulent activities. By highlighting Hidden patterns of language NLP contributes to an enhanced fraud detection approach [25].

B. Effectiveness of XAI models in identifying anomalies

XAI has been effective in identifying anomalies and in fraud detection and prevention during financial services. This effectiveness originates from AI’s ability to analyze intrinsic patterns and complex datasets, and its ability to adapt to evolving threats. Through machine learning techniques and advanced algorithms, XAI has shown its effectiveness in detecting and preventing anomalies with efficiency and unprecedented accuracy. Machine Learning algorithms, those with unsupervised learning techniques are capable of identifying abnormal deviations from normal behavior within complex datasets. XAI’s ability to learn and adapt new patterns could make it effective in fraud detection and prevention [26].

There are a number of case studies that demonstrate the effectiveness of XAI In identifying nominees during financial transactions. In one case, a commercial bank has implemented a machine learning model to analyze transaction data and irregular data patterns indicating fraudulent activities. The implemented AI system successfully identified, detected, and prevented the fraudulent attempt involving compromised account information saving the bank and its customers from financial loss [27].

In another case, a bank utilized AI algorithms to analyze and track user behavior and transaction details. The XAI system implemented in real-time detected anomalies and compromised datasets, leading to the immediate removal of defective accounts and unauthorized transactions [28]. These real-life cases highlight the effectiveness of XAI's models in the detection and prevention of fraud in the banking and financial sectors.

C. *Real-world applications of XAI in fraud detection*

XAI has demonstrated effectiveness in fraud detection and prevention in the finance and banking industry. The real-world applications of AI in the banking sector include its success in minimizing false positives and negatives and enabling organizations to understand the importance of AI models in detecting and analyzing fraud on time. One of the most effective applications of XAI in the real world is its ability to identify different types of fraudulent activities. AI systems possess advanced algorithms and pattern recognition that enable them to analyze vast amounts of datasets in real time, enabling them to identify abnormal behaviors indicative of fraudulent activities. For example, AI algorithms can detect anomalies during online banking transactions such as unauthorized account access, password misuse, and identity theft. It would be beneficial to implement XAI models in the banking industry because these models stay ahead of fraudsters tactics and provide banking organizations with a tool to detect anomalies on time and execute strategies to combat these anomalies [29]. Case studies from financial sectors highlight how the implementation of artificial intelligence models for fraud detection saved financial institutions from huge losses. Thus, to safeguard the integrity of financial institutions and customers it is important to replace traditional fraud management systems with advanced XAI models that are ten times more effective and accurate.

Moreover, another real-time application of XAI is minimizing false positives and negatives, which is important for making fraud detection a more convenient and transparent process. These errors can disrupt and complicate the transaction process.. XAI models have addressed this challenge by enhancing the accuracy of the process. False positives will occur when legitimate transactions are defected and declared as fraudulent which leads to inconvenience for customers and financial laws for the financial organization. False negatives will occur when a fraudulent activity goes undetected [30].

The real-world implications of XAI in fraud prevention have provided valuable lessons for organizations seeking to implement AI models for fraud detection and prevention. Some important lessons include; XAI must adapt to evolving fraud tactics and patterns to provide ultimate solutions. Regular updates are crucial to ensure the effectiveness of fraud detection models. Although AI models ensure unparalleled approaches to fraud detection, however, human insights should also be added to ensure timely detection and analysis. A collaborative approach of AI models and human expertise enhances the overall efficacy of fraud detection and prevention methods. The success of XAI in fraud detection in the banking sector depends on the quality and variety of training data. It is important to ensure that datasets are bias free, comprehensive, and transparent to enhance the accuracy of transactions. Banking institutions are advised to use AI models that provide insights into business strategy and ensure regulatory compliance [31].

D. Ethical considerations in AI-driven fraud detection

Artificial Intelligence AI played a crucial role in transforming the fraud detection process in the banking industry. To keep the process smooth and to fully integrate AI-driven fraud detection methods into the banking industry it is important to address some ethical considerations such as transparency, fairness, and regulatory compliance. It is important to ensure that the fraud detection process is free of bias and that there is transparency at every stage. To address biases financial institutions should implement measures to detect and address biases during the designing and deployment stage of AI models. This might involve representative training, regular audits, and ongoing monitoring. Financial organizations should prioritize accuracy and transparency when it comes to adopting XAI. Transparent and accurate AI models foster trust and enhance customer-provider relationships. As shown in Table 1, every individual involved in the process plays an important role in protecting organizations against fraudulent activities. Transparency is a key ethical consideration that should be prioritized to avoid ethical violations and ensure that the fraud prevention process is aligned with legal and ethical frameworks [32].

VI. FUTURE TRENDS

As online banking has become a trend thus it is at high risk. The role of XAI in this case is evolving to detect and prevent fraudulent activities during transactions. Future trends and innovations in this field involve exploring technological advancements, collaborations between regulatory bodies and financial institutions, and XAI developments. Emerging technologies would be used to integrate advanced biometric authentication tools for fraud detection. Biometrics would include fingerprints, facial biometrics, and behavioral biometrics that add extra layers of security over financial assets. AI algorithms would detect these biometrics in real time to differentiate between authorized and unauthorized users [33].

Future developments in XAI will focus on making AI models more user-friendly and interpretable. Moreover, this will include the development of interactive dashboards, and visualization tools that would be helpful to enhance the effectiveness of AI models. In future, the banking industry and financial institutions will prioritize XAI to address ethical concerns, to meet regulatory compliance, and to enhance user experience. Additionally, future trends in artificial intelligence driven fraud detection involve improved collaboration between financial institutions and banking organizations to share best practices and threat intelligence. Collaboration at large scale will enable a positive response towards emerging fraudulent trends in the financial sector. Collectively financial organizations would be able to strategize the solutions to permanently eliminate fraudulent activities during online banking and credit card transactions. Collective initiatives such as cross-institutional partnerships and information sharing platforms will play a crucial role in fortifying the financial industry against emerging threats. Having an understanding that existing fraud management systems are updated and ineffective is crucial to replace those systems with machine learning applications. Regulatory bodies can play a pivotal role in this regard to spread awareness and convince financial institutions to adopt modern AI fraud detection techniques. Regulatory bodies can collaborate with industry specialists to decide on mutual approaches to innovate fraud detection systems.

VII. CONCLUSION

Technological advancement has transformed traditional banking systems with online banking and digital finance transactions that bring an inconvenience for both customers and organizations. Online banking is a convenient way to receive and send payments across locations within seconds. Continuous technological advancements are posing risks for online banking. Hundreds of customers using online banking are experiencing fraudulent activities and unauthorized access to their bank accounts due to ineffective security protocols and updated fraud management systems in place. Online banking fraud are increasing every day because of the inability of financial institutions to integrate advanced machine learning powered fraud detection and prevention models.

The comprehensive review of literature and background reveals that traditional rule-based fraud detection methods were ineffective in tracking, detecting, and preventing fraudulent activities from online banking databases. Literature research proves that artificial intelligence has not only proven to be effective in automating fraud detection processes but also enhances the accuracy and transparency of the process. AI fraud detection models in place are effectively detecting and preventing online banking fraud keeping customers and financial institutions safe from huge losses. XAI Has contributed to the establishment of an accurate and transparent fraud prevention ecosystem. Financial institutions by collaborating with the regulatory bodies can improve the integration of XAI into financial institutions to detect online transactions against anomalies and frauds. Along with artificial intelligence and machine learning tools, human intelligence is also important to achieve expected outcomes. The paper also highlights a few real-life case studies in which financial institutions successfully deployed artificial intelligence to protect organizational assets from unauthorized access and fraudulent activities. Hence, XAI is effective in fraud detection compared to FMS and traditional rule-based fraud detection systems. Explainable artificial intelligence is the need of time and in the future to interpret complex data sets would be an efficient tool.

Extensive literature review and background analysis emphasize the need for future research because existing literature is not enough to guide regarding the effectiveness of artificial intelligence models and their applications in fraud detection systems. It is recommended that future researchers explore the effectiveness of XAI In fraud detection during online transactions and credit card payments. Previous authors have covered artificial intelligence and its effectiveness in fraud detection as a whole. However, future researchers are advised to work specifically on the banking industry and the applications of XAI to prevent fraudulent activities.

COMPETING INTERESTS

N/A

FUNDING INFORMATION

N/A

AUTHOR CONTRIBUTION

N/A

DATA AVAILABILITY STATEMENT

N/A

RESEARCH INVOLVING HUMAN AND/OR ANIMALS

N/A

INFORMED CONSENT

N/A

REFERENCES

1. Europol, "Serious and Organized Crime Threat Assessment," 2021. https://www.europol.europa.eu/publications-events/main-reports/socta-report
2. UK Finance, "Fraud - The Facts, 2021," 2021. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
3. European Central Bank, "The revised payment services directive (psd2) and the transition to stronger payments transition to stronger payments security," https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
4. J. Allen, why should "You is authentication enrichment and you it?" https://www.ravelin.com/blog/what-is-authentication-enrichment-and-why-should-you-do-it.
5. The International Bank for Reconstruction and Development, "Payment systems worldwide - a snapshot," https://documents 1. World Bank. org/curated/en/115211594375402373/pdf/A-Snapshot.pdf, 2020.
6. N. F. Ryman-Tubb, P. Krause, and W. Garn, "How artificial intelligence and machine learning research impacts payment card frauds. Applications of Artificial Intelligence, vol. 76, pp. 130-197, 2018. DOI:10.1016/j.engappai.2018.07.008
7. F. Doshi-Velez and B. Kim, "A roadmap for a rigorous science o. interpretability," arXiv preprint arXiv: 1702.08608, vol. 2, p. 1, 2017.
8. D. Gunning and D. Aha, "Darpa's explainable artificial intelligence (xai) program," Al magazine, vol. 40, no. 2, pp. 44-58, 2019.
9. D. Sinanc, U. Demirezen, §. Sagiroglu et al., Explainable Credit Card Fraud Detection in image conversion. 2021. https://doi.org/10.14201/ADCAIJ20211016376
10. John, S., Anele, C., Kennedy, O. O., Olajide, F., & Kennedy, C. G. (2016). Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm. *Research Gate*. https://doi.org/10.1109/csci.2016.0224.
11. Sakib, S.: Tk 2 m stolen thru card forgery, (2019). Available https://en.prothomalo.com/bangladesh/Tk-2m-stolen-thru-card-forgery
12. Rahman, S.: Credit, debit cards: swindling on the rise. The Daily Star, 2017 [Online]. Available https://www.thedailystar.net/frontpage/credit-debit-cards-swindling-the-rise-1447729.
13. Banking services vulnerable to fraud, The Daily Star, 2017 [Online]. Available https://www. thedailystar.net/editorial/banking-services-vulnerable-fraud-1448149.
14. Gartner. Marker guide Tor online Fraud detection. 4041. Online Available: https://www.gartner.com/doc/reprints?id=1-27FWBFD0&.
15. Fisglobal. “What is credit card processing?” https://www.fisglobal.com/en-gb/insights/merchant-solutions-worldpay/article/what-1s-creait-card-processing.

16. Baymard Institute. “Main reasons why consumers in the United States abandoned their orders during the checkout process in 2021. “https://www.statista.com/statistics/1228452/reasons-for-abandonments-during-checkout-united-states”
17. Ethoca. “Solving the CNP false decline puzzle; Collaboration is key”. https://hs.ethoca.com/solving-the-cnp-false-decline-puzzle-collaboration-is-key
18. M. Nelson. “Outsmarting fraudsters with advance analytics.” httos://usa.visa.com/visa-evervwhere/security/outsmarting-fraudsters-with-advanced-analytics.html.
19. N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyeroiole: minority over-sampling technique. Journal of artificial intelligence research, vol. 16, pp. 321-357, 2002.
20. Ravelin, "Retail eCommerce Fraud and Payments Survey," https://102,2 2elin
21. Phiri, J., Segooa, M., & Lavhengwa. Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, *26*(1). https://sajim.co.za/index.php/sajim/article/view/1763/2689
22. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: a recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060
23. I. Sadgali, N. Sael, and F. Benabbou. "Adaptive model for credit card fraud detection”. 2020.
24. Wang, L., Zhang, Z., Zhang, X., Zhou, X., Wang, P. and Zheng, Y., 2021. A Deep-forest based approach for detecting fraudulent online transaction. In Advances in computers (Vol. 120, pp. 1-38). Elsevier.
25. Shahbazi, Z. and Byun, Y.C., 2021. Blockchain-based event detection and trust verification using natural language processing and machine learning. IEEE Access, 10, pp.5790-5800.
26. Bouchama, F. and Kamal, M., 2021. Enhancing Cyber Threat Detection through Machine Learning-Based Behavioural Modelling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), pp.1-9.
27. Chhabra Roy, N. and Prabhakaran, S. Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. Aslib Journal of Information Management, 75(2), pp.246-296.
28. Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O. MASTERING COMPLIANCE: A Comprehensive Review of Regulatory Frameworks in Accounting and Cyber security. Computer Science & IT Research Journal, 5(1), pp.120-140.
29. Mohanty, B. and Mishra, S. Role of Artificial Intelligence in Financial Fraud Detection. Academy of Marketing Studies Journal, 27(S4). https://www.abacademies.org/articles/role-of-artificial-intelligence-in-financial-fraud-detection.pdf
30. Ayo-Farai, O., Olaide, B.A., Maduka, C.P. and Okongwu, C.C. Engineering Innovations in Healthcare: A Review of Developments in the USA. Engineering Science & Technology Journal, 4(6), pp.381-400.
31. Buhrmester, V., Münch, D. and Arens, M., 2021. Analysis of explainers of black box deep neural networks for computer vision: A survey. Machine Learning and Knowledge Extraction, 3(4), pp.966-989.
32. Felzmann, H., Fosch-Villaronga, E., Lutz, C. and Tamò-Larrieux, A., 2020. Towards transparency by design for artificial intelligence. Science and Engineering Ethics, 26(6), pp.3333-3361.
33. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M.L., Herrera-Viedma, E. and Herrera, F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion, p.101896.