WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Analysis of Financial Fraud Detection of Credit Cards Using AI in Banking Sector.

[1]Amey Ram Nate, [2]Nisha Dipak Khenwar, [3]Prof. Dhananjay Bhavsar

Department of MBA, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune
[1]amey.nate20@vit.edu, [2]nishakhenwar30@gmail.com, [3]dhananjaybhavsar@gmail.com

ABSTRACT —

Financial fraud poses a significant challenge within the financial industry, displaying a dynamic nature with no apparent patterns. Numerous fraudulent activities, including Identity Theft, phishing schemes, credit and debit card fraud, foreclosure and loan scams, fraudulent check activities, online fraud, ransomware, and malware frauds, occur daily. These illicit practices can lead to substantial financial losses, damage to reputation, and a decline in client confidence. Exploiting technological advancements, fraudsters continually adapt to current trends. Detecting fraudulent transactions often involves utilizing data mining tools to analyze and identify anomalous activities. With the evolution of technology, Artificial Intelligence (AI) has emerged as a promising solution for the detection and prevention of financial fraud. In this research study, the author explores various measures that can be implemented using Artificial Intelligence to mitigate financial fraud risks. The study emphasizes the diverse applications of machine learning and provides examples of AI techniques that can effectively combat financial fraud.

Keywords — Fraud Detection, Artificial-Intelligence (AI), Machine-Learning (ML), Random Forest Algorithm, Credit Card , Financial Fraud, Deep Learning,

Identity Theft, Phishing Schemes, Fraudulent Activities, Fraud Prevention, Technological Advancements, Data Mining, Anomalous Activities, Risk Mitigation

Cybersecurity, Fraudsters, Transactional Data, Sentiment Analysis, Rule-based Systems, Anomaly Detection, Real-time Monitoring, Human Bias, Scalability,

Model Refinement, Interpret Ability, Regulatory Compliance, Financial Institutions, Client Confidence, Fraud Patterns.

INTRODUCTION

In the modern era, there exists a pervasive apprehension surrounding financial fraud, which can be defined in various ways. One perspective characterizes financial fraud as the exploitation of regulatory loopholes in financial product governance for illicit gains. Another definition encompasses any illicit action within the financial sector undertaken with the aim of advancing personal interests at the detriment of others or organizations. Financial fraud poses a significant challenge for entities, manifesting in diverse forms such as identity theft, credit card fraud, and money laundering.

According to a survey, a notable 65 percent of credit card or debit card owners have experienced at least one incident of credit card theft. This corresponds to approximately 151 million individuals in the United States, reflecting a substantial increase from the previous year's findings, which reported nearly 58 percent of cardholders falling victim to fraudulent activities. This research paper will predominantly delve into credit card fraud transactions, given their higher frequency compared to other fraudulent transactional activities.

1. No Card Present:

This category of credit card transactions does not necessitate the physical presence of a card during the purchase.

2. Manual or Electronic Imprints of Card:

Fraud of this nature involves extracting information from the magnetic strip of a credit card through skimming and utilizing that data for deceptive transactions.

3. Card Lost/Stolen/Misplaced:

This type of fraud occurs when the cardholder either loses their card or becomes a victim of theft.

4. Counterfeit Card Fraud:

In this scenario, the perpetrator replicates all the information from the magnetic strip, creating a counterfeit card that closely mimics the original.

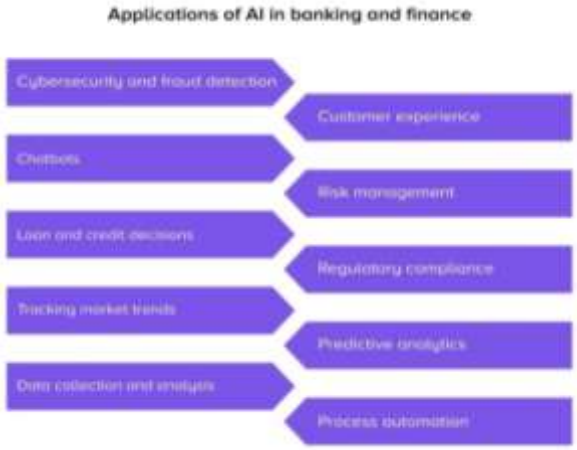
5. Application Fraud:

This form of fraud occurs when a malicious actor gains control of the software, acquires someone's login credentials, establishes a fraudulent account, and conducts transactions.

The primary objective of virtually any credit card fraud detection method is to identify unusual behavior, promptly alert investigators, and simultaneously facilitate the seamless processing of legitimate financial transactions. Employing a fraud detection system allows for the differentiation between genuine and fraudulent transactions. In 2021, the average cost of fraud was $62, but this figure has surged to over $79 this year, marking a 27 percent increase. This rise can be attributed to a combination of heightened inflation rates and the previously noted accelerated growth in online purchases. Traditional fraud detection methods rely on rule-based systems and human expertise, which are time-consuming and occasionally inaccurate. An effective fraud detection system should swiftly and accurately identify fraudulent transactions while ensuring genuine users retain access to online payment methods.

The advancements in Artificial Intelligence (AI) present an intriguing opportunity to develop more efficient fraud prediction models. Various AI techniques, including Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP), can be applied to prevent financial fraud. This research paper is structured as follows: Section 2 provides insights into the subsets of AI currently utilized in financial fraud detection. Section 3 presents a comparative study of these AI subsets. Section 4 summarizes the research's conclusions, and Section 5 discusses future work on the proposed system.

AI Application in The Banking Sector



Cybersecurity and Fraud Detection

Daily, numerous digital transactions take place as users engage in activities like bill payments, money withdrawals, and check deposits through apps or online accounts. As a result, there is an increasing need for the banking sector to intensify its endeavors in identifying and thwarting fraud.

This is the point at which artificial intelligence in banking assumes a crucial role. AI and machine learning assist banks in identifying fraudulent activities, identifying loopholes in their systems, minimizing risks, and enhancing the overall security of online financial transactions.

An exemplary case of a bank utilizing AI for fraud detection is Danske Bank, Denmark's largest bank, which implemented a fraud detection algorithm. The deployment of this deep learning tool resulted in a 50% improvement in the bank's fraud detection capabilities and a 60% reduction in false positives. The AI-based fraud detection system also automated critical decisions while directing certain cases to human analysts for further inspection.

Author also suggested that AI is also instrumental in helping banks manage cyber threats. In 2019, the financial sector accounted for 29% of all cyber attacks, making it the most-targeted industry. Through the continuous monitoring capabilities of artificial intelligence in financial services, banks can proactively respond to potential cyber attacks before they impact employees, customers, or internal systems.

Literature Review

Kunwar' (2019) focused on AI and its impact on the contemporary world, particularly within the financial sector. The study investigates the application of artificial intelligence, addressing its challenges, opportunities, and implications for employment roles. The findings reveal that numerous financial institutions have experienced substantial benefits through the integration of various AI applications. The research concludes that across the entire value chain in financial services, encompassing processing, analytics, and investment, the prevalence of technology capable of accomplishing tasks is anticipated to increase

Patel, (2018) explained that Artificial Intelligence is rooted in two fundamental concepts. Firstly, it involves the examination of human thought processes, and secondly, it endeavors to mechanize the representation of these cognitive processes. Author also highlighted both potential loopholes and associated risks. It delves into the trans-formative impact AI has had on the banking sector, providing a comprehensive analysis of these changes .

Research Methodology

The research methodology utilized in this study was methodical and closely aligned with the specific objectives outlined in the description. Descriptive research was conducted using secondary data sources gathered from various research papers, articles, journals, and case studies. The focus of the study was on the US Banking sector, utilizing time series data spanning from 2014 to 2021 to analyze the growth and trends of AI in US. The paper delves into distinct segments of banking, including trading, lending, security, credit rating, and fraud detection. The analysis of secondary sources has facilitated an examination of the impact of artificial intelligence on the financial industry, revealing trans-formative changes in operational paradigms.

Research Problem

1. The increasing prevalence of financial fraud in the banking sector poses a significant threat to both financial institutions and their clients.

2. the integration of artificial intelligence (AI), offer promising solutions,

3. there is a critical need for a comprehensive study to investigate the effectiveness and challenges associated with utilizing AI in financial fraud detection within the banking sector.

Objective

- To comprehensively investigate the efficiency of financial fraud detection using artificial intelligence.
- To analyze the implementation of AI techniques in identifying and preventing fraudulent activities,
- To Assess the impact of AI on enhancing security measures.
- To evaluate its overall effectiveness in mitigating financial fraud risks.
- To study seeks to provide insights into the evolving landscape of fraud detection methodologies.

Scope of the Research

Scope of the Research is based on the secondary data United States of America from the year 2014-2021, and predicting credit card fraud detection for next 6 years (2027).

Benefits & Challenges of AI-based Fraud Prevention:

Utilizing AI for fraud protection presents several advantages, such as enhanced accuracy, reduced false positives, and quicker detection of fraudulent activities. AI-powered fraud protection systems can dynamically adjust to emerging fraud trends and offer valuable insights into deceptive activities. However, there are inherent challenges associated with AI-based fraud protection. These challenges encompass the requirement for extensive datasets for effective training, the potential for biases in model outcomes, the lack of interpret-ability in the models, and susceptibility to adversarial attacks.Research Design:

Machine Learning

Machine learning functions as a subset of Artificial Intelligence (AI), enabling computers to discern patterns, identify trends, and make predictions based on data. This dynamic field has become one of the decade's leading trends, with businesses increasingly investing in machine learning to enhance their products. Unlike traditional hard coding, machine learning employs diverse computer algorithms and statistical modeling, enabling computers to perform tasks by learning from provided data, similar to human decision-making processes.

In the financial sector, particularly in fraud detection within credit card transactions, machine learning proves invaluable. By training algorithms on historical data, these models can identify fraudulent tendencies based on various characteristics like location, transaction amount, and time of day. However, the efficacy of machine learning algorithms in detecting novel fraud trends is contingent on substantial training data, and they may be susceptible to over-fitting.

In the proposed system, a Random Forest approach will be utilized to classify credit card datasets. This algorithm, associated with both regression and classification, comprises an ensemble of decision tree classifications. Unlike a single decision tree prone to over-fitting, Random Forest mitigates this risk by sampling a random portion of the training datasets for each tree. The approach has proven to be resilient against over-fitting and delivers a robust approximation of generalization errors. By selecting features from random data slices, Random Forest enhances efficiency and avoids over-reliance on specific columns.

Detecting fraudulent credit card transactions involves a binary classification of fraud activity (positive instance) and non-fraudulent activity (negative instance). Various methods, including Artificial Intelligence, data mining, fuzzy logic, and machine learning, have been explored for this purpose. The use of machine learning methods in fraud detection has evolved into a potent tool, particularly in the era of online transactions. Characteristics such as customer age, account details, and the source of the credit card contribute to the likelihood of fraudulent activity, with machine learning algorithms determining their impact based on training data.

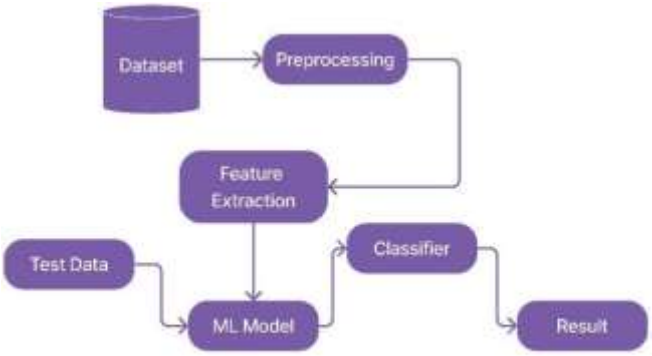


Fig 1 :- System Architecture for ML

The supervised learning approach, specifically utilizing the Random Forest algorithm, is employed to identify fraudulent transactions in credit cards, whether conducted online or offline. This approach surpasses other machine learning techniques in terms of effectiveness and precision by mitigating correlation issues and pseudo-correlating trees, thereby improving overall model performance.

The diagram illustrates the process by which the model identifies fraudulent credit card transactions. Initially, the data undergoes per-processing and cleaning. Subsequently, pertinent features are extracted to facilitate the model's learning process. The Random Forest approach in Machine Learning (ML) is rooted in collective learning, a well-established method within supervised learning. This algorithm demonstrates high reliability, as the addition of a new data point only impacts a single tree, leaving the overall model unaffected. While this enhances performance, it may marginally affect testing speed.

Deep Learning

Utilizing deep learning proves effective in identifying intricate fraud patterns within financial data. As a sub type of machine learning, deep-learning models leverage Artificial Neural Networks, employing methods such as Convolutional Neural Networks, Deep Belief Networks, Auto-encoders, Recurrent Neural Networks, and Restricted Boltzmann Machines. A fully trained Neural Network can discern unique correlations throughout the entire datasets, making it adept at detecting complex fraud patterns that may elude typical machine learning algorithms.

For instance, a deep-learning model could be trained on extensive datasets, such as social network usage, to recognize intricate patterns associated with identity theft. Deep-learning is a technique where a computer-generated model learns to perform tasks like categorization directly from images, text, or voice. These algorithms often achieve cutting-edge precision, occasionally surpassing human capabilities. The training process involves utilizing substantial labeled data and implementing neural network typologies with multiple layers.

The concept of an "Artificial Neural Network" draws inspiration from biological neural networks found in the human brain. Resembling the human brain's structure, artificial neural networks consist of interconnected neurons, referred to as nodes, at various stages of the network. These nodes emulate the connectivity found in the human brain. An Artificial Neural Network, a form of artificial intelligence, seeks to replicate the neural network structure of human brains, enabling computers to comprehend information and make decisions akin to humans. The artificial neural network is constructed by programming computers to emulate interconnected brain cells.

Generally, employing sentiment analysis can be an impactful method for detecting credit card fraud, as it provides additional information and perspectives that can be utilized to identify and prevent fraudulent activities.

Outlined below are the stages in our proposed strategy for detecting fraudulent credit card transactions using sentiment analysis:

Data Collection Methods

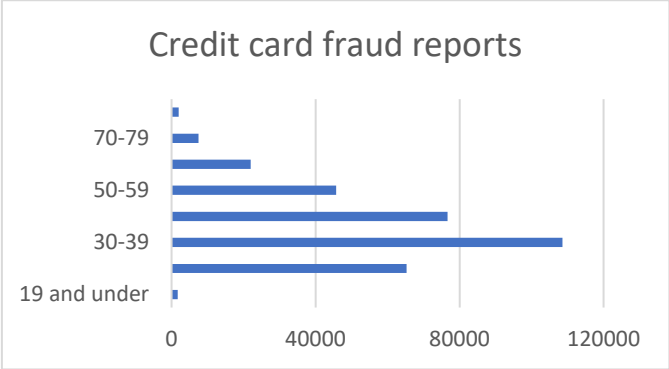
This study utilized secondary data to acquire the necessary information.

1. Data Collection

Table No. 1

Age group	Credit card fraud reports
19 and under	1,707
20-29	65,269
30-39	1,08,592
40-49	76,693
50-59	45,741
60-69	21,992
70-79	7,507
80 and over	1,954

Chart No.1

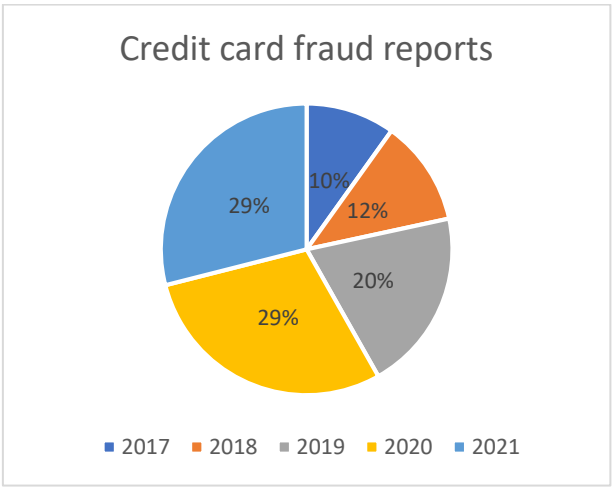


The graph clearly indicates that the highest number of reported fraud cases, reaching 108,592, occurred among individuals aged 30-39. Following closely behind are those in the age range of 40-49, with a reported total of 76,693 cases.

Table No. 2

Year	Credit card fraud reports
2017	1,33,107
2018	1,57,745
2019	2,71,938
2020	3,93,378
2021	3,89,737

Chart No.2

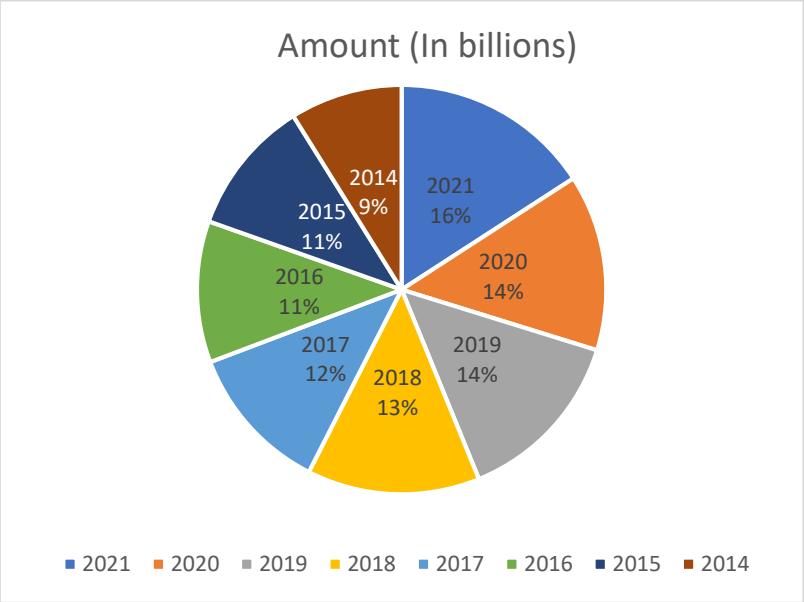


The graph highlights that in 2022, the highest number of reported fraud cases amounted to 393,378, closely followed by the year 2021, which recorded 389,737 cases. In the year 2017, a total of 133,107 cases were reported, reflecting a substantial difference compared to the more recent years.

Table No.3

Years	Amount (In billions)
2021	32.34
2020	28.43
2019	28.65
2018	27.86
2017	23.97
2016	22.8
2015	21.84
2014	18.11

Chart No.3

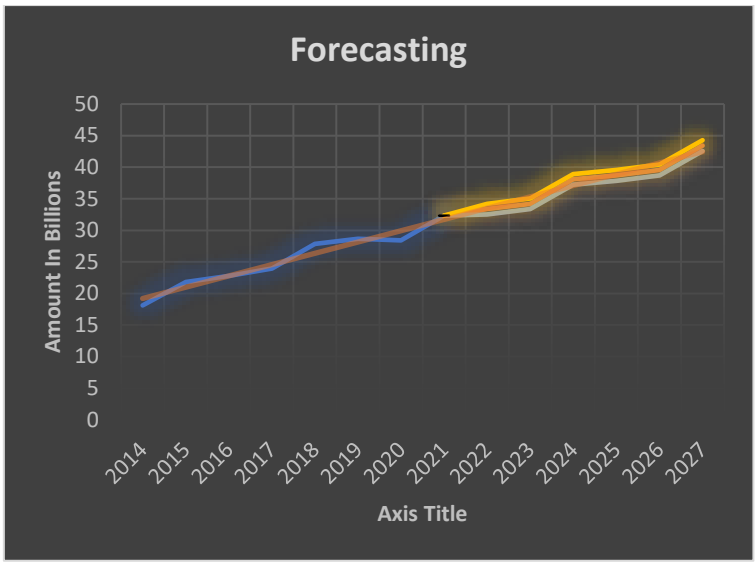


According to the provided Pie Chart, it is evident that in 2021, fraudulent activities amounted to 32.34 billion, while in 2019, the reported fraudulent amount was 28.65 billion.

Table No. 4

Years	Amount (In billions)	Forecast Amount (In billions)	Lower Confidence Boun Amount (In billions)	Upper Confidence Bound Amount (In billions)
2014	18.11			
2015	21.84			
2016	22.8			
2017	23.97			
2018	27.86			
2019	28.65			
2020	28.43			
2021	32.34	32.34	32.34	32.34
2022		33.35879479	32.54	34.18
2023		34.20963192	33.38	35.04
2024		38.07293799	37.24	38.91
2025		38.69887012	37.86	39.54
2026		39.54970725	38.70	40.40
2027		43.41301332	42.56	44.27

Chart No.4

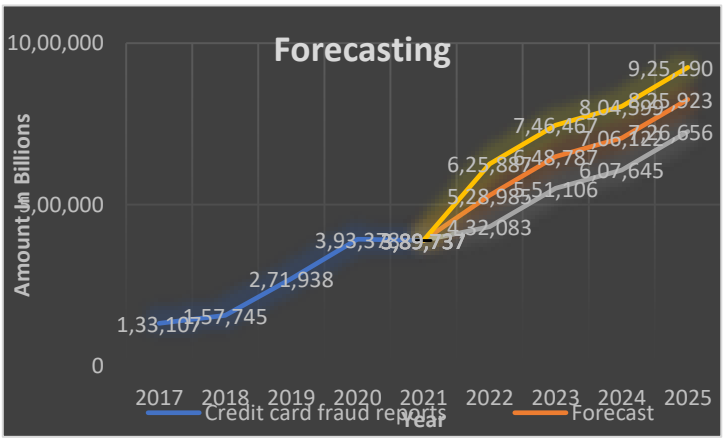


The chart illustrates a consistent upward trend in both the number of fraud cases and the corresponding amounts reported from 2014 to 2021. Projecting forward, the graph predicts a continued increase in fraud amounts, reaching 43.41 billion in the year 2027.

Table No. 5

Year	Credit card fraud reports	Forecast	Lower Confidence Bound	Upper Confidence Bound
2017	1,33,107			
2018	1,57,745			
2019	2,71,938			
2020	3,93,378			
2021	3,89,737	3,89,737	3,89,737	3,89,737
2022		5,28,985	4,32,083	6,25,887
2023		6,48,787	5,51,106	7,46,467
2024		7,06,122	6,07,645	8,04,599
2025		8,25,923	7,26,656	9,25,190

Chart No. 5



The chart clearly depicts a rising trend in both the number of fraud cases and the corresponding amounts reported between 2017 and 2021. Looking ahead, the graph forecasts a continued escalation in fraud amounts from 2022 onwards. The prediction for 2025 indicates an estimated amount of 825,923 units, with the Lower Confidence Bound at 726,656 units and the Upper Confidence Bound at 925,190 units.

2. **Pre-processing:** The data by cleaning, normalizing, and converting the text into a numerical format suitable for the sentiment analysis model. Eliminate any stop words during this process.

3. **Fraud Detection:** Fraud detection methods employ various techniques and technologies to identify and prevent fraudulent activities across different domains such as finance, e-commerce, healthcare, and more. Here are some common methods used for fraud detection:

3.1.Rule-Based Systems:

Define a set of rules that are indicative of potential fraudulent behavior.

3.2.Anomaly Detection: Identify outliers or unusual patterns in data that may indicate fraudulent activity.

3.3Machine Learning (ML) Algorithms: Train models on historical data to learn patterns of normal behavior & detect deviations.

3.4Behavior Analysis: Monitor user behavior to establish a baseline and detect deviations from the norm.

3.5Real-Time Monitoring: Monitor transactions or activities in real-time to quickly detect and respond to suspicious behavior.

Findings:

1. Enhanced Fraud Detection Accuracy:

The application of Artificial Intelligence (AI) in the banking sector for credit card fraud detection significantly enhances accuracy. Machine learning algorithms and deep-learning techniques prove effective in recognizing intricate patterns indicative of fraudulent transactions, leading to a more robust and reliable detection system.

2. Adaptability to Evolving Patterns:

AI-driven models demonstrate remarkable adaptability to evolving patterns of fraudulent behavior. Unlike traditional rule-based systems, these models can promptly adjust to alterations in fraudulent activity, ensuring a proactive approach to tackling emerging threats in the ever-changing landscape of financial fraud.

3. Overcoming Human Bias and Blind Spots:

By automating the fraud detection process, AI mitigates the impact of human biases and blind spots inherent in manually coded models. The objectivity of AI algorithms helps minimize false positives and negatives, providing a more impartial and accurate assessment of potential fraudulent transactions.

4. Limitations of Traditional Machine Learning Models:

While traditional machine learning models exhibit competence in recognizing typical fraud patterns, they are constrained by the limitations of human-designed features and may struggle with unforeseen scenarios. The study underscores the necessity for continuous model refinement and adaptation to evolving fraud techniques.

5. Effectiveness of Deep Learning Techniques:

Deep-learning techniques, designed for handling multivariate, high-dimensional data, prove to be particularly effective in fraud detection. The ability to analyze comprehensive contextual information, such as entire paragraphs of transaction details, enhances the model's confidence in accurately assessing the potential risk associated with specific terms or patterns.

6. Scalability for Large Datasets:

The research affirms that AI, especially deep-learning approaches, is well-suited for handling large datasets common in the banking sector. The scalability of these techniques enables the integration of data from various sources, facilitating a more comprehensive analysis and improving the overall effectiveness of fraud detection mechanisms.

7. Practical Implications for Banking Security:

Implementing AI-based fraud detection systems has practical implications for enhancing banking security. The findings highlight the importance of leveraging AI technologies to fortify financial institutions against the growing sophistication of credit card fraud, thereby safeguarding both the institution and its customers.

8. Recommendations for Future Research:

The study suggests avenues for future research, emphasizing ongoing exploration into the development of AI models capable of addressing novel fraud scenarios. Additionally, continuous efforts to enhance interpretability and transparency of AI models in the financial sector are crucial for building trust and facilitating regulatory compliance.

Conclusion:

In conclusion, this study delving into the application of Artificial Intelligence (AI) in the banking sector for the detection of financial fraud in credit card transactions has revealed valuable insights and implications. The intersection of AI and financial fraud detection proves to be a promising avenue, offering enhanced capabilities for identifying and preventing fraudulent activities in the dynamic landscape of the banking industry.

The examination of machine learning algorithms showcased their adeptness at discerning patterns indicative of fraudulent transactions. The quick adaptability to evolving patterns of fraudulent behavior makes AI a powerful tool in safeguarding financial systems. However, it is crucial to acknowledge the inherent limitations associated with human coding, such as biases and potential blind spots in the model.

The incorporation of deep-learning techniques emerged as a significant advancement, particularly in handling large and intricate datasets. The ability to analyze multivariate, high-dimensional data, and the contextual understanding brought by deep learning contribute to more robust fraud detection capabilities.

This research emphasizes the importance of comprehensive data pre-processing, including sentiment analysis, to provide additional layers of information for a more nuanced understanding of transactional data. By integrating sentiment analysis findings with other fraud detection strategies like anomaly detection, the model's efficacy can be significantly improved.

As we move forward, the collaborative integration of AI technologies and traditional fraud detection methods presents a holistic approach to fortifying the resilience of financial systems against emerging threats. Continuous refinement and adaptation of AI models based on evolving fraud patterns, coupled with ongoing vigilance and innovation, will be essential for maintaining the integrity and security of credit card transactions in the banking sector.

References:

1) https://www.kaggle.com/code/meet3010/credit-card-fraud-detection-using-cnn/notebook

2) https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/

3) https://www.security.org/digital-safety/credit-card-fraud-report/#:~:text=According-

4) https://www.ravelin.com/insights/machine-learning-for-fraud-detection

5) Gupta, Shalini, and R. Johari. ”A New Framework for Credit Card Transactions Involving Mutual Authentication between Cardholder and Merchant.” International Conference on Communication Systems and Network Technologies IEEE, 2021:22-26

6) Bolton, Richard J., and J. H. David. “Unsupervised Profiling Methodsfor Fraud Detection.” Proc Credit Scoring and Credit Control VII (2020): 5–7.

7) Drummond, C., and Holte, R. C. (2019). C4.5, class imbalance, and cost sensitivity: why under-sampling beats oversampling. Proc of the ICML Workshop on Learning from Imbalanced Datasets II, 1–8.

8) Quah, J. T. S., and Sriganesh, M. (2020). Real-time credit card fraud detection using computational intelligence. Expert Systems with Applications, 35(4), 1721-1732.