The impact of AI-based cyber security on the banking and financial sectors

Haya saleh alrafi [1], Shailendra Mishra[2]

[1,2] Department of Information Technology, College of Computer and Information Sciences
Majmaah University Majmaah, 11952, Saudi Arabia
Emails: 441204476@s.mu.edu.sa; s.mishra@mu.edu.sa

Abstract

BD and AI are now transforming the banking and finance industry at a very fast pace, which is leading to change in the banking and finance institutions. This change is making them better, customer-oriented and financially rewarding organizations. Big data and AI have been useful in the banking and financial institutions to assess and manage the risks. Through the analysis of big amounts of unstructured data in real time, AI algorithms are capable of identifying risks. This makes it easy to put preventive measures in place to avert the risks. In addition, big data and AI have come a long way in solving the problem of fraud in banking and finance. This paper showed how big data and AI improve risk management, Cyber threat, and fraud in banking and finance by using data analysis and data pattern identification in real-time. That is why our work emphasizes the importance of implementing secure privacy and explaining the AI algorithm to eliminate ethical and Cyber security issues. Using analytical approaches, AI can identify the transactions with the help of comparison with the previous data and the behavioral characteristics related to the fraud. This approach to fraud prevention has been effective in reducing losses while at the same time improving the customer's confidence in the company. On the other hand, there are disadvantages of big data and AI such as privacy, security, and ethical issues. Measures that can be used to safeguard customer information have to be employed in order to effectively safeguard the consumer data. Furthermore, transparency and accountability of the AI algorithms are crucial in order to avoid unfair decisions.

Keywords: Artificial intelligence; cybersecurity; customers; financial products; risk-taking

1. Introduction

Banks and financial institutions have been in possession of a lot of data in recent years, and with the help of AI, they have been able to analyze this data and also automate activities that used to take a lot of time and at the same time were prone to a lot of errors [1]. Organizations have faced significant pressure to survive in highly competitive markets. They have developed solutions to cut costs, increase quality, and shorten time to market. Next-generation technologies are necessary for businesses to prosper in the new age of business transformation. Instead of focusing on a specific product or service, businesses should gather and analyse data using a platform that is future-focused. To boost acceptance rates, assure successful implementation, and reduce post-implementation risks, BD readiness and maturity levels must be assessed and measured. This is done using a concept known as maturity assessment and a corresponding tool. [2].

The banking and finance sector now has potential to analyse client behaviour, assess risks, enhance performance, and develop new financial products and services thanks to the use of big data and AI. In this research, the researcher seeks to explore how big data and AI have affected this industry by first establishing how practices in the field have evolved. It also seeks to assess the opportunities and risks of the said technologies [3]. AI is relevant to audit quality. The findings indicate that audit firms that invest in AI decrease the frequency of physical data modifications and data retrievals. This paper aims to establish the following objectives about the effect of big data and AI on banking and financial services [4].

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

AI is widely used in the field of cyber security and its importance is growing year by year. AI is applied in credit scoring, fraud detection, virus identification, spam filtering, and hacking identification. Artificial intelligence is becoming importance in reducing cyber dangers. The CS-FSM approach is the best approach that can be used in managing cyber security risks in the financial sector [14]. Thus, it becomes important for the financial institutions to know about the big data and artificial intelligence in order to survive in the ever-changing world. hese technologies can help in changing the banking and finance sector in decision making, customer satisfaction, reducing the routine work, improving the security aspects, and in providing better and new services and products in the field of banking and finance. The implication of this study will be useful to the existing and intending banks, financial institutions, policy makers and scholars to appreciate the present and future prospect of the industry [5].

The main objectives of this study are stated below:
1- The use of big data and artificial intelligence in the banking and finance industry is briefly examined in this study.
2- A critical assessment of artificial intelligence (AI) and big data in the banking and financial sector, with a focus on risk management, fraud detection, and consumer profiling.
3- Exploring big data and artificial intelligence in constructing the customer experience in the banking and financial sector.
4- Examining the use of big data and AI in improving security standards and in identifying and mitigating activities in the banking and finance sector.
5 Understanding the challenges associated with implementing big data and AI in the banking and finance sector as well as their limitations.
6-Providing recommendations to institutions, on leveraging big data and AI to enhance their operations.
The paper is organized as follows: A review of relevant work is given in part (2), the experimental setup is covered in section (3), the techniques employed in the present study are described in section (4), the findings and analysis are covered in section (5), and the possibilities for further research on the topic are discussed in section (6).

2. Related Work

Researchers focus on digital banking and customer service applications due to AI advancements. As the industry grows, so does the range of applications for banking goods and services. Mobile payments also increase convenience. AI will simplify computing and data transfers, which entails that nations must establish new systems. By automating risk identification, management, and assessment, artificial intelligence is transforming the financial industry. It is changing the financial world and promoting financial inclusion. Applications of AI in finance include fraud, accounting, credit rating, bankruptcy prediction, and forecasting. The researchers in this study explored the interaction between AI and the financial industry [6].
A further investigation examined the significance of Industry 4.0 digital technology inside the banking industry, emphasising its use in risk evaluation, risk control, real-time financial analytics, and anti-fraud mechanisms. It highlighted the need for big data and artificial intelligence technologies to create an automated personal assistant capable of making intelligent financial decisions. For risk prediction and estimate, future suggestions include digital twins, blockchain, IoT, AI, and smart contracts. Future scholars should evaluate emerging financial technologies based on their legal and regulatory environments [7].
From 2011 to 2019, the research looked at how digital finance affected 132 Chinese commercial banks' total factor productivity (TFP). The findings demonstrated that digital finance fosters effective competition and technological transfer, both of which raise TFP. The state-owned commercial banks have a negligible impact, while non-state-owned banks have a substantial effect. The association between digital finance and TFP is partially mediated by risk-taking, suggesting digital finance can improve risk management. The finance industry is undergoing a transformation driven by data, machine learning, AI, and cloud computing. The finance industry has been transformed by big data, enhanced fraud detection, offering real-time stock market insights, and precise risk analysis. Yet, ongoing hurdles like safeguarding data privacy and ensuring data quality remain. Future exploration ought to concentrate on establishing seamless pathways for companies to harness large-scale datasets effectively [8].
Machine learning techniques can detect complex datasets and improve fraud detection in Fintech systems. Feature engineering and selection significantly impact algorithm performance. Ensemble

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

approaches outperform outlier detection methods and maintain robust performance responsive to variable feature selection scenarios, outperforming outlier detection methods on synthetic datasets [9]. Machine learning has proven effective in AI systems for financial risk management, reducing losses and increasing revenues. A comprehensive analysis of its applications in financial risk management identifies task taxonomies and algorithms, highlighting challenges and emerging trends. ML has significantly impacted financial fields like securities and portfolios [10].

The study highlighted the high cost of implementing artificial intelligence in banks due to its technical components. To ensure successful implementation, employees must receive training on the technical aspects of the system. Despite the high cost, AI can reduce human error by providing accurate transaction details and timely notification of changes [11].

Fuzzy logic is being used in various aspects of the banking industry, but its full potential is yet to be realized. It is effective in resolving ambiguity and uncertainty, which are common financial analysis traits. This study contributes to identifying areas of financial research that use fuzzy logic and suggests potential applications in trading and behavioral finance. It also helps manage banking crises by identifying the most suitable fuzzy logic techniques [12]. This paper compared eight techniques of machine learning for credit card fraud detection with emphasis on categorization of imbalanced data. The findings established that LR, C5. Out of all the algorithms used, decision tree algorithm, SVM, and ANN were the most effective, with C5. Among the methods, 0, SVM, and ANN are the most effective because of the consideration of the extreme imbalance of the data [13].

Some of the advantages that come with the suggested CS-FSM paradigm powered by artificial intelligence and transforming the financial sector's cyber security include enhanced scalability, privacy, data security, risk management, and defense against attacks. From the research, it is evident that the integration of EES and KNN algorithm is efficient in identifying and preventing intrusions. There have been positive effects in the reduction of risk, privacy, and security of data. The necessity of using AI algorithms in cybersecurity solutions for banking systems has been discussed in this paper. 97.2% for scalability, 98.7% for risk reduction, 95.1 percent for treatment, and 96.1% for data protection. 94% of consumers are satisfied overall, and 4% of data security. The analytical rating of the system is 3% for attack avoidance. [14].

Big data refers to vast amounts of data that require specific technologies for collection, management, and analysis. Businesses must understand customer behavior and improve their products and services. The financial industry is increasingly using big data to drive wealth and financial growth. Platforms like Apache Hadoop and Spark help businesses store large amounts of data, reduce costs, and analyze sentiment. Big data can also help companies modify their product lines and ensure successful marketing campaigns [7]. The 1960s crisis prompted the growth of electronic commerce and financial services, with AI and fintech technologies transforming the banking industry and the public, paving the way for a new era [15].

3. Research Methods

Research includes issue definition and characterization, the formulation of hypotheses or suggested solutions, the collection, organisation, and evaluation of data, the justification and conclusion-making process, and the testing of the conclusions to see if they support the hypothesis. [16]. Qualitative research was conducted due to AI novelty and uncertainty. This method examines AI in finance more thoroughly and broadly. This approach is adaptable and simple to modify in response to changes in the variables and research environment. Qualitative data describes whereas quantitative data defines. McNamara and Bono [17], propose that the methodology is carefully selected to guarantee independence from the chosen method. Rather, it aims to accurately mirror the intricacies of reality. As mentioned before, AI applications in the highly regulated financial domain are still in the early stages. Therefore, in addition to reviewing academic literature, industry reports were used to validate various hypotheses and provide context. In qualitative research, just like any analytical approach, document analysis involves thorough examination and interpretation of data to uncover meaning, deepen comprehension, and cultivate insights [18]. AI applications in financial institutions of today with an outlook to the future. It has been aimed at catering to a broader audience to understand the fundamentals of AI in Financial Institutions. This is rather than focusing on AI technology application in a use case.

Quantitative research, which is what we did in this study, is the most suitable research approach for this kind of investigation. The quantitative method may cover a system of inquiry that can be applied to a population by linking distinct factors to numerical data. Through quantitative research, data may be gathered rapidly and effectively, and the findings can be directly tied to the subject of the study.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

The author's ability to support the hypothesis and results with arguments and evidence will determine the quantitative conclusion. To learn, basic empirical connections are used. This form of study relies heavily on those concepts to arrive at correct hypotheses [19].The paradigm shift in IT is transforming from programming to learning, with machine learning proving superior in many areas.[20].Machine learning (ML) involves identifying valid patterns in data, with a strong manual component for task definition, data selection, processing, and evaluation [21].Supervised learning aims to forecast a target feature based on explanatory features, such as nominal or numeric features. Deep learning is a prominent class of learning methods that uses artificial neural networks to process various types of raw data, such as texts, images, and speech.

A. Select Dataset

To carry out this analysis and verification, we will gather data from sources such as financial institutions, research papers, and industry reports. We will thoroughly examine the data to extract insights regarding the influence of data and AI on banking and finance. The findings of the study will contribute to the existing literature and provide recommendations for future studies and practice in this field.

B. Details of implementation

Data pre-processing: To maintain the quality of collected data, cleaning, integrating, transforming and handling missing values or outliers of the collected data.
Experimental design: Developing methods to assess the effects of data and AI on different spheres of banking and finance. This might entail defining what models, algorithms, and metrics are appropriate for each of the areas to be investigated.
Data analysis: Applying the right statistical and machine learning methods on the preprocessed data. This could be data analysis, predictive modelling, clustering, classification or any other analysis of relevance to the research question.
Experimental validation: Ensuring the results of data analysis through experimentation. This may involve conducting experiments, tests or comparing the models or algorithms' performance.
Impact assessment: Based on the studies, the effectiveness and efficiency of data and AI in banking and finance; Discussing the results of the study in terms of different study areas.
Ethical considerations: Analyzing the consequences that are linked to data and AI in banking and finance. These technologies are therefore not without their drawbacks and some of these include privacy, security, and biases that may be inherent in the technologies.
The data comprises 284808 records and 31 attributes. The dataset has several columns with names V1 to V28; most probably, they contain features obtained through PCA for privacy preservation purposes. Also, in the given dataset, you will have the Time column that quantifies the number of seconds between the given transaction and the first recorded transaction, the Amount column that shows the amount of the transaction, and the Class column. The Class column is represented by '0' for normal transactions and '1' for the fraudulent one.

Pre-processing steps:
1. Check for Missing Values: Check whether there is any form of missing values in the given dataset.
2. Feature Scaling: The Amount feature may need scaling since it is not normalized as the PCA features.
3. Data Balancing: Ensure that there exists a balance between the genuine and the fake transactions.
4. Data Splitting: Divide the given data into training and testing data set.

4. Experimental Setup

For the implementation, a desktop PC with the following hardware and software specifications: Windows 10, 8 GB RAM, Intel(R) Core (TM) i7-10700 CPU, Jupyter Notebook 7. 0. 6, and Python 3. The examples of languages that do not support Unicode by default are C, C++, and Java 5. It has been coded in the first version of the programming language and it has been executed in the second version of the interpreter. 12. In our study, we employed the use of the pandas, Scikit-Learn, NumPy, and Matplotlib libraries for data analysis and visualisation. For the visualization, the Matplotlib tool was utilized, while the NumPy tool was used for numerical computations and Panda's tool for data processing. Machine learning models for the purpose of intrusion detection in Internet of Things networks were built using Python. Due to these components, we were able to put together a strong and flexible analytic structure in a short amount of time. The framework that was required to be built had to be established before the dataset could be analyzed. This involved the act of installing python 3. 12 on a VMware Workstation and Windows 10 guest operating system.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

A. Pre-processing steps

Figure 1: Class distribution (Normal & Fraud)

There is no missing value in the given data set. The distribution of the class shows that the credit card transaction under normal class 0 is dominant with 99% while the fraudulent class 1 is only 1%. 83% normal and 0. Figure 3 shows that 17% of the transactions were fraudulent. This imbalance is common in fraud detection cases though it may cause the model to be biased. To address this, we could either use techniques like SMOTE (Synthetic Minority Over-sampling Technique) for oversampling the minority class or adjust the class weight in the machine learning algorithms.

B. Correlation matrix

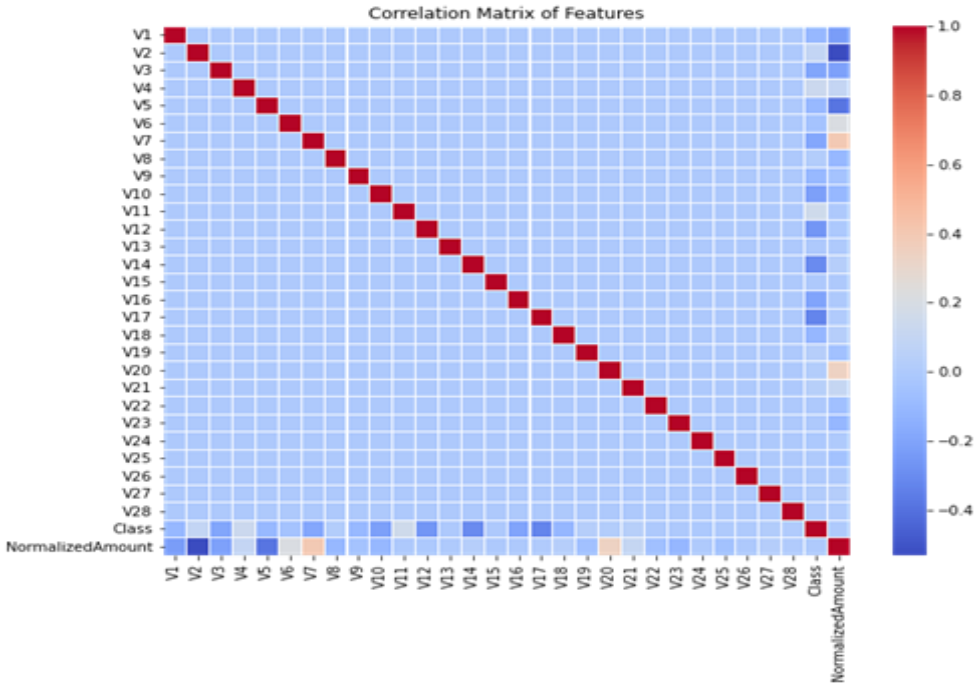

Figure 2: Heatmap

The heatmap (Figure 2) reveals varying correlations between features and the Class variable, with V11, V4, V2, V21, and V28 showing a higher positive correlation with fraud, while V12, V14, V3, V10, and V16 show a high negative correlation, suggesting their relevance in distinguishing fraudulent and non-fraudulent transactions.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

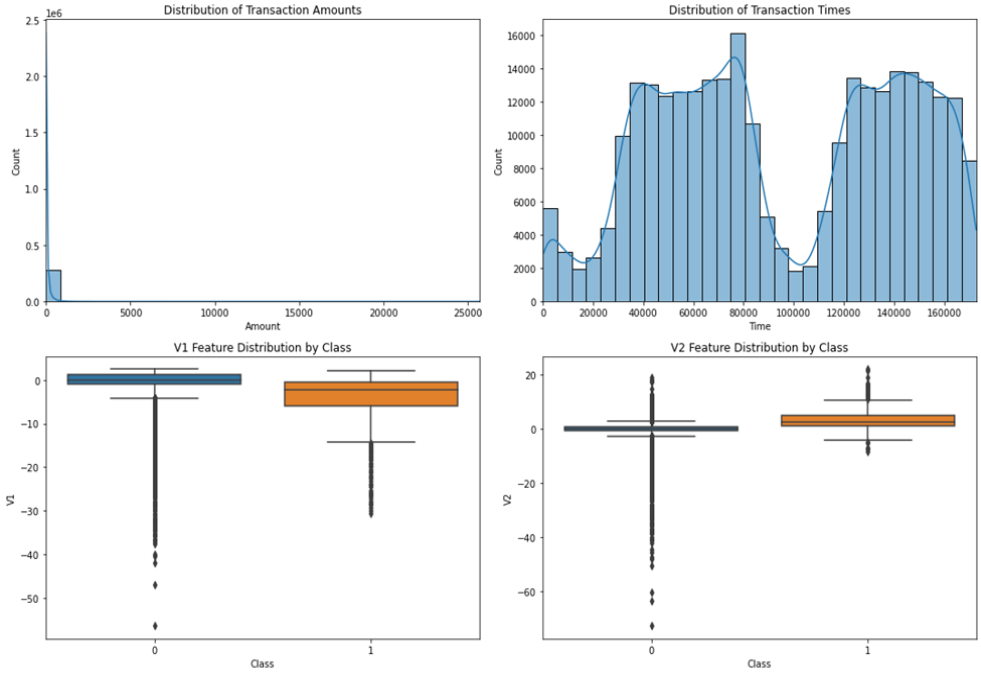

Figure 3: Distributions of transactions

The distribution is right-skewed (Figure 3), indicating that most transactions are of lower amounts, with a few transactions of very high amounts. The distribution of transaction times appears to be fairly uniform, without any obvious patterns or spikes.

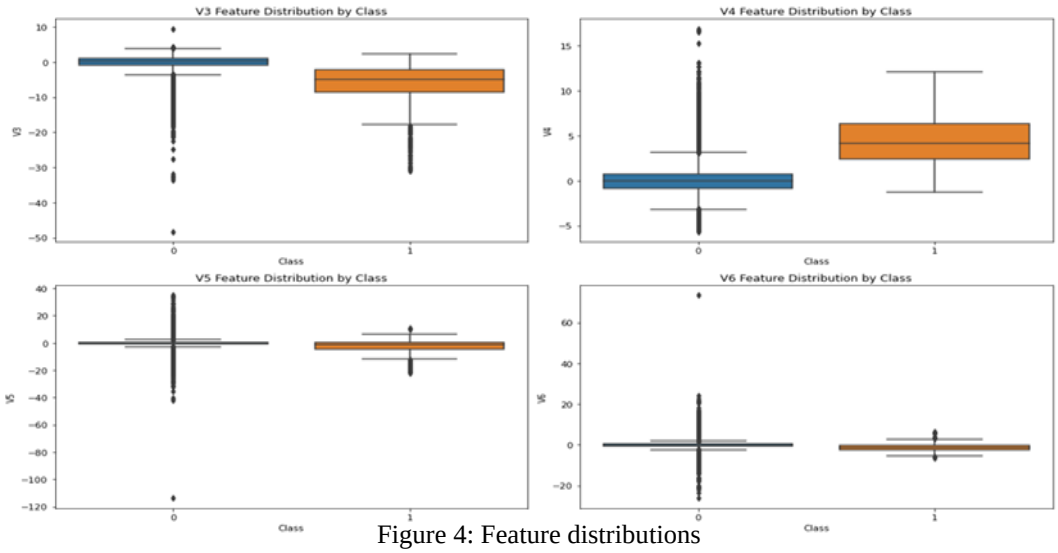

Figure 4: Feature distributions

The boxplots for V1, V2, V3, V4, V5, and V6 show differences in their distributions between fraudulent (Class 1) and non-fraudulent (Class 0) transactions. For some features like V1, V2, and V3, fraudulent transactions tend to have values more skewed to one side. These visualizations can help in understanding the characteristics of the data, especially in distinguishing between fraudulent and legitimate transactions. They also guide the feature selection process for predictive modeling. Feature distributions are shown in (Figure 3) and (Figure 4).

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

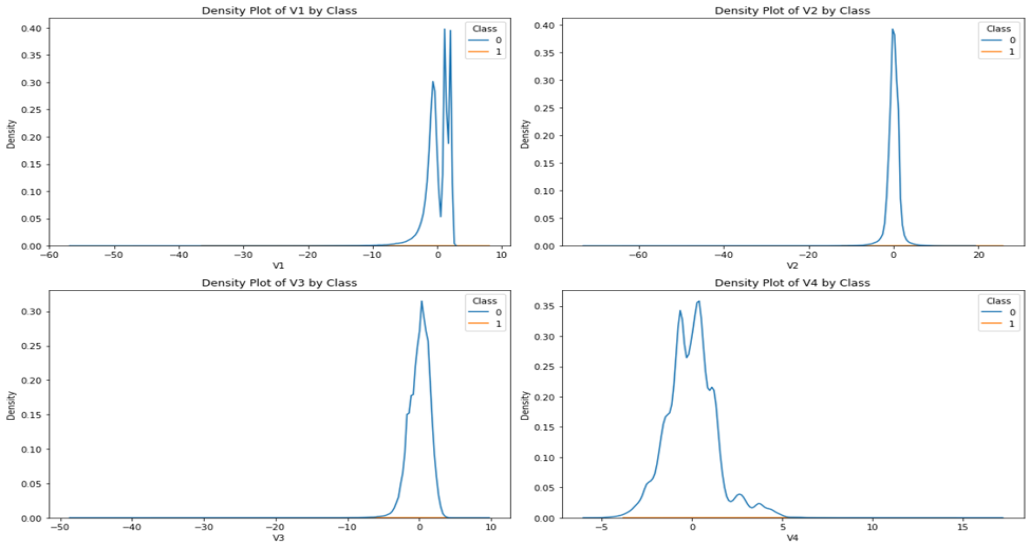

Figure 5: Density plots

The Kernel Density Estimation (KDE) plots (Figure 5) for V1, V2, V3, and V4 show the density distribution for fraudulent and non-fraudulent transactions. Each feature exhibits distinct patterns for different classes, which can be useful for classification.

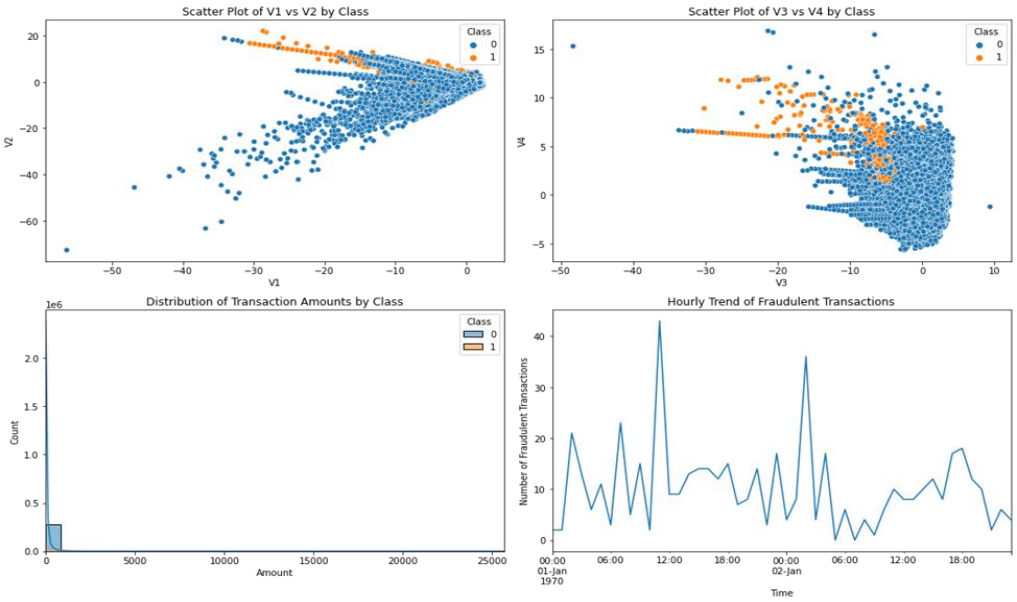

Figure 6: Scatter plots

The scatter plots (Figure 6) display the relationship between pairs of features. While there's some overlap, certain areas seem to be more densely populated by either fraudulent or non-fraudulent transactions, indicating potential patterns. The histogram provides a comparison between fraudulent and non-fraudulent transactions based on the transaction amount. It shows that fraudulent transactions often occur in different amount ranges compared to non-fraudulent ones.

The time series plot shows the hourly trend of fraudulent transactions. This can help identify certain periods with higher frequencies of fraud. These visualizations deepen our understanding of the dataset and can guide further analysis, such as feature selection for machine learning models or identifying key periods for fraud monitoring. Feature distributions are shown in (Figure 6).

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

Divide the data into training and testing sets after that. I will use stratified sampling in light of the class imbalance to make sure that the ratio of legitimate to fraudulent transactions in both groups is comparable.
After splitting the data, select two machine learning algorithms for this task. Considering the nature of the dataset, logistic regression and random forest classifiers are good candidates. Logistic regression is effective for binary classification problems, and random forest can handle non-linear relationships and is less prone to overfitting. Proceed with data splitting and then train and evaluate both models.

A. Evaluation Metrics

In cases of unbalanced classification, precision, accuracy, F1-score, recall, and ROC-AUC score are all crucial. TP, FP, FN, and TN are defined specifically in the domain of intrusion detection as follows: TP is the process of classifying a real danger as a threat. FP is the process of classifying a common, acceptable behaviour as illegal. FN refers to the procedure of assigning a normal equivalent to an actual type of crime. TN is the official term used to designate a typical normal category as such.
Accuracy

- Logistic Regression: 99.73%
- Random Forest: 99.89%
- Both models have extremely high accuracy. This means that a vast majority of predictions (fraudulent or not) are correct.

However, in imbalanced datasets (common in fraud detection), high accuracy can be misleading as it might reflect the ability of the model to predict the majority class well (often the non-fraudulent class) rather than its effectiveness in identifying the minority class (fraudulent transactions).
Precision

- Logistic Regression: 4.09%
- Random Forest: 9.78%
- Precision is the ratio of true positive predictions to the total positive predictions. Both models have low precision, especially the Logistic Regression model. This indicates that a high number of transactions predicted as fraudulent are normal (false positives). A low precision can be problematic in a fraud detection context as it leads to many false alarms, which could be inconvenient and cause unnecessary verification processes.

Recall

- Logistic Regression: 68.89%
- Random Forest: 68.89%
- Recall, or sensitivity, measures the proportion of actual positives correctly identified. Both models have the same recall rate, which is moderately high. This means they are reasonably good at detecting fraudulent transactions (true positives), but there's still a notable proportion of fraudulent transactions they fail to detect (false negatives).

F1 Score

- Logistic Regression: 7.73%
- Random Forest: 17.13%
- The F1 Score is the harmonic mean of precision and recall, providing a balance between them. The low F1 scores for both models, especially for Logistic Regression, suggest that they are not effectively balancing precision and recall. This is primarily because the models are not very accurate.

ROC AUC

- Logistic Regression: 84.31%
- Random Forest: 84.39%
- The ROC AUC value indicates a classifier's capacity to discriminate between two classes. It can also be seen that both models have good measure of separability as seen from the ROC AUC scores. They are relatively good in separating between fraudulent and non-fraudulent transactions.

5. Results and Discussion

The training and the testing data set have been split with almost the same proportions of normal and fraudulent transactions as in the original data set. The training set consists of approximately 89.6% normal transactions and 10.4% fraudulent transactions, while the testing set has about 99.9% normal and 0.1% fraudulent transactions.
•Model Training: Utilising the training data, train a logistic regression model and a random forest classifier.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

•Model Evaluation: Metrics such as accuracy, recall, F1-score, precision, and ROC-AUC score, which are essential for unbalanced classification issues, should be used to assess both models on the testing set.
•Model Comparison: Compare the performance of both models based on the evaluation metrics.
Start with training and evaluating the logistic regression model and then proceed with the random forest classifier.
To categorise the likelihood of distinct groups based on certain dependent variables, use logistic regression. Table (1) presents an overview and comparison of the various models' performance measures:

Table 1: Multi-class classification

Metric	Logistic Regression	Random Forest
Accuracy	99.73%	99.89%
Precision	4.09%	9.78%
Recall	68.89%	68.89%
F1 Score	7.73%	17.13%
ROC AUC	84.31%	84.39%

Interpretation
•The high accuracy of both models is likely due to the imbalanced nature of the dataset, where correctly predicting the majority class (typically non-fraudulent transactions) can lead to high accuracy.
•The low precision, especially in Logistic Regression, suggests a high rate of false positives, which can be a significant issue in practical applications.
•Moderate recall indicates a decent capability in detecting actual fraudulent cases, but there is room for improvement.
• The need for a better balance between accuracy and recall is shown by the poor F1 ratings, especially for Logistic Regression.
•The relatively high ROC AUC scores suggest that the models are, to some extent, capable of distinguishing between the two classes.
Given these insights, it may be necessary to further tune the models, possibly by adjusting the decision threshold, trying different feature engineering techniques, or using more sophisticated models. Additionally, addressing the data imbalance with techniques like SMOTE or adjusting class weights might improve model performance, especially in terms of precision and F1 score.

Analysis
Based on the latest results showing the performance metrics of Logistic Regression and Random Forest models in a fraud detection context, we can draw several conclusions about the impact of big data and artificial intelligence (AI) in banking and finance. High Accuracy with Imbalanced Data: The performance of both models is high in terms of accuracy and this is usually the case in imbalanced datasets as is the case in fraud detection. This goes to show that it is unwise to rely only on accuracy in the evaluation of models in such settings. The challenge in Balancing Precision and Recall: The low precision, especially in the case of Logistic Regression, means that a large number of normal transactions are marked as fraudulent. This suggests a challenge inherent in fraud detection: Minimizing the number of false positives while at the same time ensuring that the organization has the capability to detect actual fraud.
Moderate Success in Detecting Fraud: The recall rates are quite reasonable for both models, meaning that they are fairly good at identifying fraudulent transactions. However, there is still much that can be done as a substantial portion of the fraudulent activities are still going unnoticed. Need for Improved Model Balance: The low F1 scores particularly for Logistic Regression means that there is room for improving the trade-off between precision and recall. This is especially relevant in fraud detection where it is equally important to not raise false alarms and at the same time be able to capture all the fraud cases.
Effective Class Differentiation: The ROC AUC scores are quite high, which means that both models are rather accurate in terms of classifying fraudulent and non-fraudulent transactions. Practical Implications in Banking and Finance: The findings reveal the implementation issues of AI models in fraud detection in the finance industry. Despite the ability of these models to detect fraud to a certain extent, the problem of high false positive rates means that they are not operationally efficient or

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

customer friendly. Potential for Model Improvement and Tuning: It can also be seen that there is a need for further improvements of the models. This may require adjusting the hyperparameters, using a more complex model, integrating several models, or applying techniques for handling imbalanced data, for instance, oversampling the minority class or applying anomaly detection. Data Quality and Feature Engineering: The accuracy of the models also shows the possibly of requiring improved feature extraction or using more relevant data. When it comes to financial transactions, aspects such as the customers' behavior, the contexts of the transactions, and previous data may be crucial.
Regulatory and Compliance Considerations: The banking industry has strict rules and regulations on banking and financial practices. High false-positive rate models may not be feasible because of the operational costs and the impact on the customer's experience. Thus, improving models to achieve these standards is important.
AI as a tool, not a solution: These findings support the notion that AI and machine learning are helpful tools in fraud identification but not as a guaranteed method. It has to be integrated into a system of checks and balances as far as financial activities are concerned.
In conclusion, it can be stated that AI and machine learning are very helpful in fraud detection in banking and finance, however, the problems and difficulties described in the results section show that the choice of the model, its constant improvement, and the balance of true and false results are critical.

B. Discussion

In conclusion, big data and artificial intelligence have become the game-changer in the banking and finance industry due to the creation of venues for innovation, efficiency, and customer focus. Financial institutions may control risk and provide clients with individualised services by using data analytics, machine learning, and predictive modelling. However, the same technologies also present several issues concerning data security, compliance with the law, and recruitment of staff. In future, financial institutions should aim to strike a balance between innovation and risk management to harness the power of big data and AI for growth in the digital economy.

C. Research Limitations

Clearly defining the research's scope in relation to big data and artificial intelligence's impact on the banking and financial industry is crucial to rectifying any misconceptions. Despite our efforts and attempts to gather and analyze data from sources, there are some factors that may influence the depth and generalization of the results.

- Focus: We concentrate on the applications of AI and big data in banking and finance. While topics such as cybersecurity or regulatory aspects are important, they are not directly related to the subject of this research.
- Data accessibility: Nevertheless, there is a huge volume of literature on the topic, companies' data and information may be scarce. This could limit our analysis by the data that is available and the quality of that data.
- Time-related aspects: What this implies is that the environment of data and AI in banking is dynamic due to the dynamics in technology and regulation. However, with the aim of presenting the trends some of the findings may become obsolete with time.
- Biases: As with any research, our study could be subjected to certain types of bias including selection bias in obtaining information or analytical bias in analyzing the data. To reduce bias, we have also incorporated appropriate methods and peer review.
- External influences; Factors beyond the study, such as situations, global events, and technological changes could impact the outcomes of this study. Although efforts have been put into separating the effects of data and AI, external influences cannot be completely disregarded.

6. Conclusions and Future Work

Big data, artificial intelligence and cybersecurity are used in banking and finance as a trend due to the shift in conditions in the industry. Cutting-edge technologies like, machine learning, deep learning, and natural language processing are thought to help financial institutions better understand their customers' behavior, predict market trends, and enhance profitable and efficient procedures. Nevertheless, cybersecurity and privacy concerns become a problem as data and artificial intelligence become more popular among companies. Some of the security measures that can be implemented by the banks include encryption, authentication, and monitoring to protect the networks and prevent the data accessibility. AI also helps banks identify risks early enough to formulate good risk management strategies and make sound investment decisions. The use of automation, predictive analytics, and real-time insights also improves the operations by cutting on costs while increasing the efficiency. The future research directions are to design AI models that are transparent and to develop methods

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

for AI compliance and AI ethicality. Scientists need to establish best practices for building the models that will evaluate the risks. They also need to put in place measures that will deal with issues of bias in AI and protection of data. Quantum computing is the next generation of computing technology that can change data processing, encryption methodologies and optimization techniques in banking and finance industries. More research can be done to show how quantum computing can be applied in risk assessment, fraud detection, portfolio optimization, security reinforcement, and decision-making acceleration.

Acknowledgment

Additionally, the authors would like to thank Majmaah University's Deanship of Scientific Research for their cooperation with this effort.
Funding: "This research received no external funding"
Conflicts of Interest: "The authors have declared no conflicts of interest."

References

[1] Villar, A. S., & Khan, N. (2021). Robotic process automation in the banking industry: a case study on Deutsche Bank. Journal of Banking and Financial Technology, 5(1), 71-86.
[2] Al-Sai, Z. A., Husin, M. H., Syed-Mohamad, S. M., Abdin, R. M. D. S., Damer, N., Abualigah, L., & Gandomi, A. H. (2022). Explore big data analytics applications and opportunities: A review. Big Data and Cognitive Computing, 6(4), 157.
[3] Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. International Review of Financial Analysis, 81, 102103.
[4] Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? Review of Accounting Studies, 27(3), 938-985.
[5] Hasan, M. M., Popp, J., & Oláh, J. (2020). Current landscape and influence of big data on finance. Journal of Big Data, 7(1), 1-17.
[6] Aleksandrova, A., Ninova, V., & Zhelev, Z. (2023). A Survey on AI Implementation in Finance,(Cyber) Insurance and Financial Controlling. Risks, 11(5), 91.
[7] Bisht, D., Singh, R., Gehlot, A., Akram, S. V., Singh, A., Montero, E. C., ... & Twala, B. (2022). Imperative role of integrating digitalization in the firms finance: A technological perspective. Electronics, 11(19), 3252.
[8] Wu, C., Liu, T., & Yang, X. (2023). Assessing the Impact of Digital Finance on the Total Factor Productivity of Commercial Banks: An Empirical Analysis of China. Mathematics, 11(3), 665.
[9] Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. Sensors, 21(5), 1594.
[10] Al-Baity, H. H. (2023). The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework. Sustainability, 15(18), 13725.
[11] SHETTY, S. K., SPULBAR, C., BIRAU, R., & FILIP, R. D. (2022). Impact of Artificial Intelligence in the Banking Sector with Reference to Private Banks in India. Annals of the University of Craiova, Physics, 32.
[12] Sanchez-Roger, M., Oliver-Alfonso, M. D., & Sanchís-Pedregosa, C. (2019). Fuzzy logic and its uses in finance: a systematic review exploring its potential to deal with banking crises. Mathematics, 7(11), 1091.
[13] Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. IEEE Access, 7, 93010-93022.
[14] Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), 5875.
[15] Mhlanga, D. FinTech and Artificial Intelligence for Sustainable Development. Kothari C. R. Research Methodology: Methods and Techniques. Second Revised Edition. New age publishers. New Delhi, 2004.
[16] Kothari C. R. Research Methodology: Methods and Techniques. Second Revised Edition. New age publishers. New Delhi, 2004.
[17] Bono J. E., McNamara G. From the editors: Publishing in AMJ - Part 2: Research design. Academy of Management Journal, 2011, vol. 54, iss. 4, pp. 657660. DOI 10.5465/amj .2011.64869103
[18] Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. Human resource development review, 19(1), 94-106.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024

[19] De Lange, P. E., Melsom, B., Vennerød, C. B., & Westgaard, S. (2022). Explainable AI for credit assessment in banks. *Journal of Risk and Financial Management*, *15*(12), 556.
[20] Pelari, O. M., & Hoxhaj, M. (2021, September). An Empirical Investigation of the Influence of the Pandemic on Albanian Internet Banking Service Usage. In The International Conference On Global Economic Revolutions (pp. 139-148). Cham: Springer International Publishing.
[21] Binkhonain, M., & Zhao, L. (2019). A review of machine learning algorithms for identification and classification of non-functional requirements. *Expert Systems with Applications: X*, *1*, 100001.

Doi : https://doi.org/10.54216/JCIM.140101
Received: January 26, 2024 Revised: Marach 15, 2024 Accepted: May 18, 2024