Scientific Publications

Universal Journal of Business and Management, 2022, 2, 1224
www.scipublications.org/journal/index.php/ujbm
DOI: 10.31586/ujbm.2022.1224

Review Article

Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks

Lakshminarayana Reddy Kothapalli Sondinti [1]*, Zakera Yasmeen [2]

[1] Assistant Vice President, US Bank, Denver, Colorado, USA
[2] Data Engineering Lead, Microsoft, USA

*Correspondence: Lakshminarayana Reddy Kothapalli Sondinti (lakshminarayana.k.s.se@gmail.com)

Abstract: We investigate and analyze the trends and behaviors in credit card fraud attacks and transactions. First, we perform logical analysis to find hidden patterns and trends, then we leverage game-theoretical models to illustrate the potential strategies of both the attackers and defenders. Next, we demonstrate the strength of industry-scale, privacy-preserving artificial intelligence solutions by presenting the results from our recent exploratory study in this respect. Furthermore, we describe the intrinsic challenges in the context of developing reliable predictive models using more stringent protocols, and hence the need for sector-specific benchmark datasets, and provide potential solutions based on state-of-the-art privacy models. Finally, we conclude the paper by discussing future research lines on the topic, and also the possible real-life implications. The paper underscores the challenges in creating robust AI models for the banking sector. The results also showcase that privacy-preserving AI models can potentially augment sharing capabilities while mitigating liability issues of public-private sector partnerships [1].

Keywords: Credit Card Fraud; Payment Data Analytics; Digital Commerce; Fraud Detection; Federated Learning; Privacy-Preserving Machine Learning

How to cite this paper: Kothapalli Sondinti, L. R., & Yasmeen, Z. (2022). Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks. *Universal Journal of Business and Management, 2*(1), 1224. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1224

Received: July 16, 2022
Revised: September 23, 2022
Accepted: October 28, 2022
Published: November 19, 2022

1. Introduction

As payment systems rapidly evolve, cyber attackers attempt to evade characterization by mirroring these changes, demonstrating adaptive and evasive behaviors such as fraud. This paper aims to utilize techniques geared towards fashioning tools that will assist defenders in a robust, adaptable, and dynamic manner, reflecting their opponents. We investigate the potential ability to identify, learn, and analyze credit card fraud-related behavioral trends from merchant-based fraud patterns. Functional dependencies are employed in relationships between merchant-specific fraud proportion aggregation and credit sales. None of these dependencies correlate historically, and we utilize this assumption for relationship identification and quantification [2]. The credit card fraud problem is a continuous struggle with increasing costs, while the primary goal of applying adequate solutions causes additional strain. Our techniques focus on uncovering potential fraud indicators on a real-world dataset by using functional dependencies and column correlations as learning and analysis tools. The discovered fraud behavioral trends are presented, accompanied by an explanation. As payment systems continue to evolve, cyber attackers adapt by mimicking these changes, employing increasingly sophisticated methods to evade detection, including fraudulent activities. This paper focuses on leveraging advanced techniques to develop tools that help defenders stay one step ahead, adapting to the evolving tactics of fraudsters. By examining merchant-based fraud patterns, we aim to identify and analyze behavioral trends related to credit card fraud. Functional dependencies are used to explore the relationships between merchant-specific fraud proportions and credit sales, with the assumption that these dependencies do not correlate historically, allowing for the identification and quantification of potential fraud indicators. The goal is to uncover hidden fraud behaviors within a real-world dataset, utilizing column correlations and functional dependencies as analytical tools. This approach highlights key fraud trends, providing valuable insights for combating the growing challenge of credit card fraud [3].

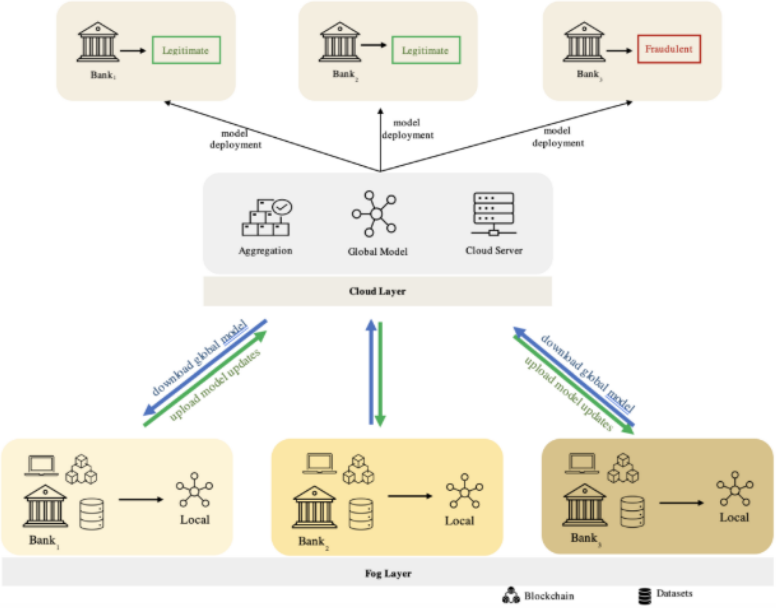

Figure 1. Credit Card Fraud Detection (CCFD) Systems

1.1. Background and Significance

As a continuous and complex social problem, fraud detection is desirable to avoid substantial financial losses and damages after fraud incidents occur. Fraud detection systems are of great concern in various business fields, especially for financial institutions. Credit cards are widely used in e-commerce due to their convenience, so the number of fraud cases in credit card payments has continued to increase over the years. A huge volume of payment transactions is processed every day, so credit card companies need numerous manual workers to prevent fraud. This is why banks are willing to spend substantial amounts of money on machine learning models. The significant collection and storage of human transactional behaviors and patterns have raised several important ethical concerns such as the privacy of personal information in relation to making a profit and the potential for abuse. To tackle these concerns, privacy issues in machine learning models have become the prime factor seriously impacting the adoption of machine learning models [4].

Designing a credit card fraud detection system could optimize expenditures and prevent fraud in advance. Generally, the key characteristics that must be considered for a user's behaviors in a fraud detection system are time and user-specific transaction patterns. With these key characteristics, users' historical purchasing patterns can be identified. Such user-specific patterns are important in distinguishing real users from fraudsters because they reflect the user's purchasing habits to some extent. Furthermore, the purchasing patterns can eliminate the noise of generic models and reduce the number of false positives. However, credit card transactional data often include personal information, which violates the privacy of user-specific patterns and security requirements. Therefore, it is important to implement a privacy-preserving technique to prevent unauthorized access to users' information [5].

Equation 1: Federated Learning Model

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \theta_i^t$$

where:

θ^{t+1} is the global model's parameters after iteration t.

θ_i^t is the model's parameters after training on client $i's$ data.

n_i is the number of data points on client $i's$ local dataset.

n is the total number of data points across all clients.

1.2. Research Objectives

The proposed research primarily focuses on enhancing the existing supervised learning architectures for improving accuracy and response by leveraging federated learning. We have detailed the potential challenges and benefits of the underlying modifications and proposed an illustrative framework. In this regard, this study presents a model that combines the improvement from AGAN, GAN, and Pix2Pix into the inception of a new model that facilitates better image quality with better model performance. This paper also tries to analyze this multi-sequence model and runs experiments which can give more insights into multi-sequence multi-modality GAN. Nonetheless, the inception of the SelectaGAN involves multimodal issues and is a more critical feature of the generation, namely, the multi-sequence problem.

The work in this direction is beginning to be explored and diversified lines of research are likely to have a considerable future impact. We have proposed a novel model namely SelectaGAN, in which we could train it successfully on both generative adversarial networks and perform detestability tasks. The model performs better and at par with state of the art on rewarding benchmarks. It has achieved state of the results and the aim is to partially bridge the gap between unconditional GAN models and a dedicated approach, with a multi-attentive style by means of multi-sequence GAN [6].

2. Literature Review

In literature, generally two rank categories of research have been used to analyze credit card fraud: transactional level and account level. The research relating to transactional level focuses on identifying fraudulent transactions among a high volume of day-to-day transactions. To determine if the transaction is fraudulent or not, several studies have relied on either supervised, unsupervised, or semi-supervised learning methods in conjunction with techniques such as decision trees and fuzzy clustering, probabilistic modeling, logistic regression, and support vector data description. These studies focus on the partial information such as the fraction of, or total dollar amount of, the transaction(s) in coming to a fraudulent conclusion. Most of the transactions are characterized by their low values and the features derived from the transaction. With the transactional data present in the study, we could test the algorithms on their level of detection and thus rate them as good. Outcomes such as control charts and clustering are largely used in detecting fraudulent transactions [7].

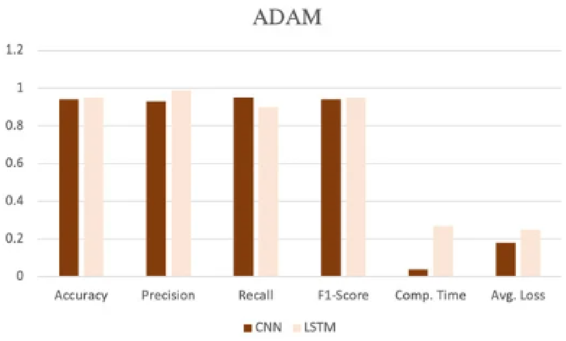

Figure 2. Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD)

2.1. *Credit Card Fraud Detection Techniques*

Credit card fraud detection techniques can be broadly classified into two groups: rule-based and clustering/classification techniques. Most techniques combine multiple algorithms, including neural networks, clustering, or support vector machines, at least in the first phase of processing. A popular technique is to preprocess the attributes to reduce the dimensionality of neural network training. This technique may lead to a reduction in the neural network training and computation times. In practice, most models are not complicated; they consist of relatively simple rule-based or classification-based techniques. Classifiers such as support vector machines are usually the most beneficial when they are used to combine evidence regarding the presence of fraud from different neural networks or from a wide variety of different neural network-based classifiers since neural networks may have different induction biases. On the other hand, neural networks with different architectures have similar inductive biases. However, simple voting or averaging of neural network predictions is a more efficient way of combining evidence, but it is effective only when both bias and prior training samples are similar [8].

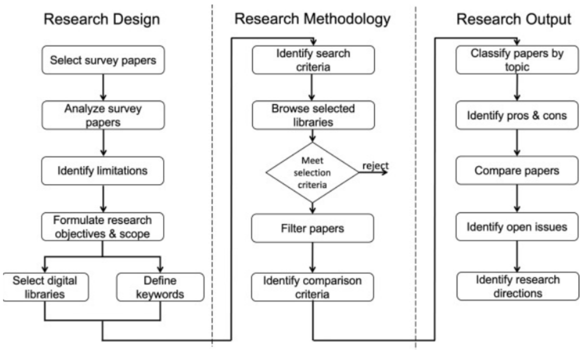

Figure 3. Credit card fraud detection in the era of disruptive technologies

2.2. *Federated Learning in Fraud Detection*

The analysis of customers' transactional patterns in credit card fraud is particularly sensitive. Federated learning provides an effective solution to maintaining privacy by training models on user-preprocessed data and sharing the model without data leakage. While it has not been applied to the customer transactional pattern in fraud detection, a dual problem for merchant ID analysis has been studied. The data are from the actual financial industry, and in some cases cannot be supported for sharing data due to the lack of specific merchant features. Therefore, we train a teacher model on financial data, and then use this data to improve transactional services by training fraud detection models. The first step is to create a teacher model. Then we use the teacher to check the classification of transactions. If the customer name of a transaction is not known to the platform, then the platform will process the transaction based on the transaction information. Fill in the standard merchant name of the purchase transaction of the customer using similarity or machine learning algorithms, which is used to build the training set. The training set is made up of purchases that have expired, which are classified as a purchase label. From the financial services we subscribe to, fill the platform database with these updated label purchase data and obtain training on the finance model. After the financial subscription layer is completed, the retrained model will be available [9].

3. Methodology

Figure 1 illustrates the novel privacy-preserving end-to-end framework, which allows for training and evaluation of an ART model on in-house credit card fraud detection datasets using a customized data connector without data sharing. First, the predefined standardized queries and payment card attributes are executed using the PAI layer as requests by multiple different data controllers while applied to a given dataset. Anonymous IID data splits are published to these researchers subsequently. Any retrieval of raw sensitive dataset payment information from external parties is thus avoided. Second, the researchers support ART model training as per privacy-preserving and corporate data governance principles within their secure enclave by incorporating standardized PAI-restricted transaction-level queries in the preconfigured and trusted codebase. The data connectors to facilitate this PAI layer interaction are implemented inside the secure enclave. Third, once trained, only the trained ML model binary files are repatriated to the data owners for evaluation using PAI queries on the raw sensitive dataset. Indeed, the ownership of the data is maintained throughout the full process end to end, including model validation. This information barrier effectively mitigates the model-stealing vulnerabilities, adversarial attacks, and unregulated AI model usage, ultimately ensuring compliance and support for regulatory obligations with trusted partners for model development [10].

3.1. Data Collection and Preprocessing

In this project, a business unit comprising data science, operations research, and optimization model development groups partnered with a team to analyze two years of credit card transaction data from 14 countries. The goal of this analysis was threefold: Improve potential fraud detection while reducing the number of false positives. Explore ways of conducting fraud analytics in a federated machine learning environment, adhering to the necessary privacy and data controls regulations for individual markets. Develop both standardized and shrouded measures for transaction risk. In order to ensure the security and privacy of cardholders' personal information and reduce friction in fraud prevention, it was important to leverage ML models that are both custom-built for highly imbalanced fraud problems and powered by privacy-preserving AI methods: encryption of compressed and locally updated models between a server and multiple participants, model ensembling, and homomorphic encryption for feature engineering and calculations with the noisy real-numbered models. With private coordination across geographic boundaries enabled, models developed using federated ML in a privacy-preserving mode can help improve fraud detection while respecting data control concerns in individual markets and facilitate advanced analytics [11].

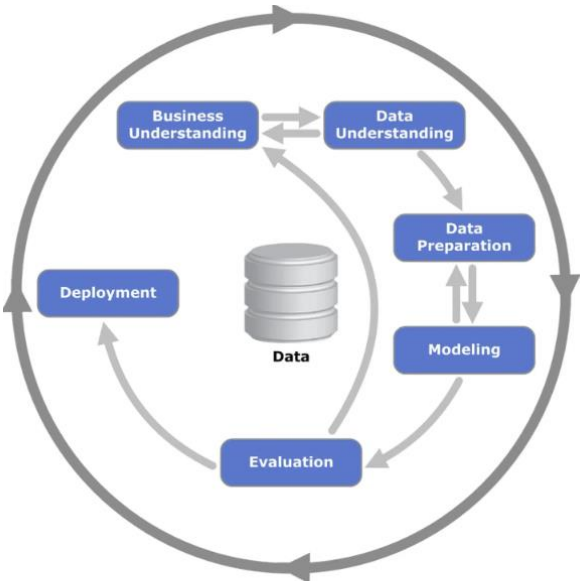

Figure 4. Data Collection for Machine Learning

3.2. Federated Learning Framework Implementation

The setup of the federated learning ecosystem can be divided into three parts. First, there is a cluster of n devices serving as the reserves for the customers' models used. These devices can be their smartphones, tablets, laptops, or desktop computers. These devices contain the customers' data, including client identification together with the purchase data. We partition this part of the data into equal allocations, where each device has a portion of clients in the system, including their requirements. Their purchase patterns are learned by different machine learning models, and it is possible that these models have different privacy-preserving computing mechanisms [12].

Second, the customers obtain a service to issue instructions on personalized products. We define a service that provides these instructions on products that cater to the demands of the customers in a personalized way. The service accesses a composite machine learning architecture leveraging the retraining of a custom model, weighted model averaging, and feature rule-based scores on the device. It follows that the service learns from different device data without requiring the data beyond the personalized products to be aggregated. Instead, the service allows the customers to utilize only the locally learned models in combination with the different learning models on the devices. In the second part of the federated learning ecosystem, customers access a service that provides personalized product recommendations tailored to their specific needs. This service operates by leveraging a composite machine learning architecture that integrates several techniques, such as retraining custom models, weighted model averaging, and feature rule-based scoring. The service operates on the device level, ensuring that the learning process remains localized without requiring the aggregation of sensitive data. Instead of pooling customer data across devices, the service enables the individual devices to learn from their own data, allowing for a personalized model to be developed for each user. This approach ensures privacy by keeping the customers' data on their own devices, while still benefiting from the collaborative learning across the ecosystem of devices, where models are continuously improved and refined in a decentralized manner [13].

Equation 2: Anomaly Detection Using Autoencoders

$$z = f_{enc}(x)$$

$$\hat{x} = f_{dec}(z)$$

where:

x is the input transaction data.

z is the encoded representation.

$\hat{x}$ is the reconstructed input.

4. Results and Analysis

In this section, we present our results and detailed analysis. Throughout our discussion, we limit our analysis to results obtained from the ensemble of tree-based models, primarily because ensemble models tend to perform well on a variety of problems. Our analysis includes examining how various input parameters differentially affect each reported result, shedding light on the regressors used by the models to uncover fraud, evaluating detection times, studying the robustness of the model to adversarial behaviors by would-be fraudulent cardholders, and carefully examining the role of our subsampling strategy that allows us to reverse the class imbalance problem in the dataset [14].

We analyze how our model performance relates to the use of the following hyperparameters: usual plastic transactional details, postal code and country code identities, binary timeslots, continuously scaled transaction amounts, and transaction labeling by both duplicate detection and balance thresholding. We examine during what times the machine performs best. To do so, we compare our model's detection performance by differentiating label-wise, which is instantaneously known based on the recorded hour, as well as instantaneously unknown to the model, calculated later across all instances. Furthermore, we measure the confusion rate split by those with high risk aversion for committing the crime data fails to realize, at the disadvantage of loss of following a distribution closer to benign cardholders, and those wanting to exploit the system at the expense of incurring more false negatives [15].

Figure 5. Credit Card Fraud Dataset Analysis

4.1. Behavioral Trends in Credit Card Fraud Patterns

A major part of the fraud detection model relies on dissecting existing fraud characteristics based on historical fraud patterns. For us to uncover the right mechanism based on well-developed deep learning and other machine learning paradigms, it is important that a problem statement is corrected and defined through a combination of problem framing and visualization analysis. This can only be accomplished with insights and feedback from both data scientists and business product stakeholders. Through a number of brainstorming sessions and industrial visits, we were able to define fraud patterns in three stages: at a portfolio level, transaction processing level, and analysis of characteristics within fraudulent patterns [16].

4.1.1. Portfolio Level

Fraud Within Organic and Inorganic Growth Across multiple service and product portfolios, we discovered that while there were organic transactional patterns and demands from credit card customers, there were also several spurt-and-stop growths led by syndicates or travelers who were perpetrating fraudulent behavior.

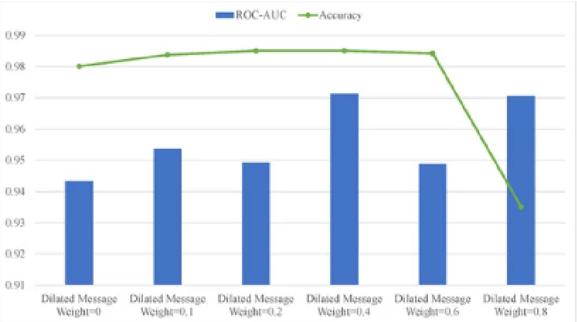

Figure 6. Advanced Credit Card Fraud Detection Using Federated Learning, Graph Attention Networks, and Dilated Convolutions

5. Discussion and Implications

Developing efficient privacy-preserving remote payment fraud analytics methods yields various business, privacy, and governance implications. In conjunction with legislation and appropriate governance frameworks, it fosters the democratization of AI tools alongside the development of fraud detection systems across multiple jurisdictions and state-owned banks [17]. On the enterprise level, it drives value for financial institutions by reducing data regulation time and effort, reinforcing fraud detection processes, and allowing the study of real public data on global and sector behavioral trends that aid the decision-making processes. Additionally, it supports payment processors and merchants by enhancing the detection and prevention of fraud in single transactions. As for the consumer, the dissemination of financial crime analytics at a mass scale has the potential to refine the safety of e-payments, especially as part of the proposed consortium.

We discuss the obstacles of getting access to behavioral public data, but we also highlight the technical challenges and restrictions on leveraging the proposed framework in global payments [18]. In particular, even if we hypothesize a public consortium where member banks share payment data, the analytics could not leverage this data for beneficial purposes. Centralizing payment information hinders the propagation of Fireflies to all member banks and exposes the consortium data to potential breaches that compromise members' business operations [19].

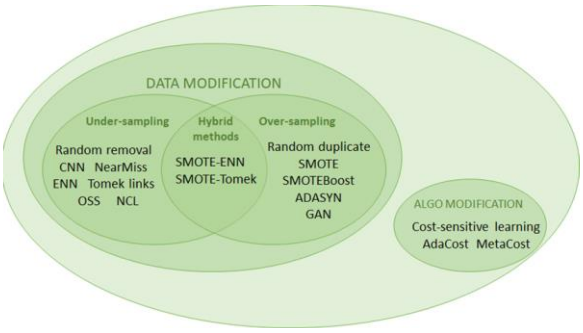

Figure 7. Discussion and Implications

5.1. Privacy Concerns and Solutions in AI Frameworks

Researchers have long been sensitive to data privacy issues. The latest artificial intelligence technologies typically use huge models and large-scale datasets. As such, a modern privacy-preserving solution is generally needed, such as secure multiparty computation, homomorphic encryption, and federated learning [20]. Secure multiparty computation is a secure computation method in which a number of participants can jointly compute a function over their inputs while keeping these inputs privately confidential. It can avoid both data privacy issues and accidental information leakage. Federated learning, based on the concept of averaging models, is a typical horizontally distributed protocol where participants train individual models on their local data. Here, the data's distributed features cannot be shared, and thus it can protect the privacy of sensitive data [21]. Homomorphic encryption, including additively homomorphic encryption and fully homomorphic encryption, is the property of the cryptosystem that allows adding two ciphertexts together to produce a new ciphertext that acts as the sum of the plaintexts of the previous ciphertexts. Although the homomorphic scheme bears computational costs, it can effectively protect data privacy, especially in privacy-preserving machine learning. With its theoretical advantages, federated learning and homomorphic encryption have become the main prototyping methods for standard privacy-preserving analysis. However, our real-world banking data is represented as RS, where 'R' represents Rescaled or Restricted and 'S' represents selectively sharing. Selectively sharing is another method in the privacy-preserving analytics section. An organization shares a given function of their input data with an analysis party, who then applies it to a function only. In this proposal, we use the share method to conduct privacy-preserving analytics [22].

Equation 3: Behavioral Trend Analysis for Fraud Detection

$$P\left(\text{Fraud} \mid x\right) = \frac{1}{1 + e^{-x^T \beta}}$$

where:

x is the feature vector representing transaction data (e.g., amount type).

β is the vector of model parameters (weights).

$P\left(\text{Fraud} \mid x\right)$ is the probability that the transaction is fraudulent.

6. Conclusion

The results of this study demonstrate the profound insights that can be derived from leveraging a distributed, privacy-preserving model [23]. The federated learning approach allows access to decentralized information and patterns, representing activities in various locations, at different times, using diverse devices, and reflecting disparate behaviors. The exploration of the immediate neighborhood models uncovered substantial dispersion across time and location while revealing stable patterns representing daily, weekly, and annual periodic components [24]. These insights are used to define an unconventional approach using federated learning to train student models that can be contemporaneously located in real time and gradually decay in importance, mimicking negative human behavior. Furthermore, the model assigns substantial value to events that occur at lower frequencies. This dynamic, real-time locality-based monitoring and risk identification through incidence learning exploits both spatial and temporal effects [25].

This paper applied our proposed dynamic federated learning approach to identify behavioral trends and patterns related to both credit card fraud as well as authentic transacting events. The model decomposes its estimated effect into time, space, and periodic factors [26]. The end result is multiple constituent models per stripe layer, each trained to track the neighborhood group patterns or periodic shopping activity, tampered on annular affect behavior, subjected to decay in importance over time and ranging, with minimum sale component clustering for outlier and potential fraud detection. The interpretation of the exploration and analysis of the results provides immediate actionable insights into general suspected fraud behavior including annualized holiday, post-holiday event patterns as well as 'unpredictable behaviors' [27].

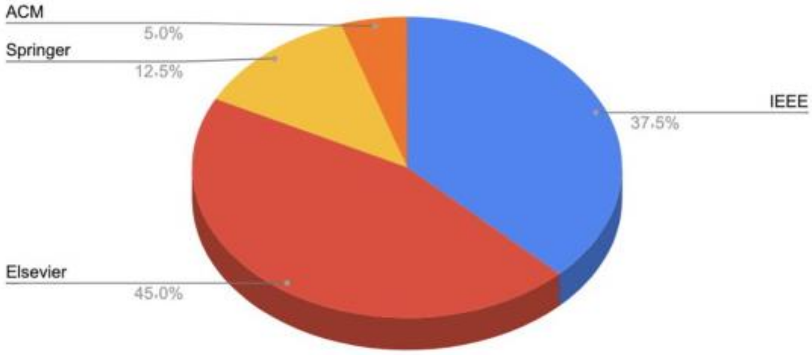

Figure 8. Credit card fraud detection

6.1. Summary of Findings

We conducted an exploratory analysis on a novel dataset that contains both 42 synthetic and 42 non-synthetic credit card fraud scenarios in which we simulate three different behavioral variations: no behavioral variation, three transaction features showed blatant behavioral variation, three transaction features showed subtle behavioral variation, and whether just a single transaction feature showed subtle behavioral variation. [28] The goal of this work is to find initial insights into introducing artificial synthetic behavior patterns in the data to favor credit card fraud detection models [29]. We used the 42 synthetic credit card fraud scenarios to train four different credit card fraud detection classification models in a federated learning setup, in which we also compare the efficiency of both a state-of-the-art privacy-preserving deep learning framework and a standard deep learning framework [30].

In this exploratory analysis, we find that several synthetic behavioral patterns lead to higher AUC-ROC credit card fraud detection model scores, suggesting an intermediate level of usability in adding synthetic behavior patterns to the real-world scenarios when looking to leverage AI models to efficiently detect credit card fraud [31]. Here, we summarize the main takeaways from the observed behavioral changes and conclude with possible enhancements we are looking to apply to improve underperforming behavioral variations [32].

6.2. Future Trends

We have proposed using the federated learning pipeline for modeling behavioral trends in credit card fraud detection, offering the unique capability of modeling an incredibly large and highly detailed feature space over numerous classes while protecting user data [33]. Within the scope of our work, we identified that a signal’s behavioral outcome is attributed to a combination of product usage and the potential relationship between the user and the product to which a variable number of features contribute [34]. Despite not obtaining the desired control of credit card fraud channel responses, we showcased an ability to rapidly prototype and create one-to-many credit card fraud modeling tasks by leveraging a private and disparate dataset in which user actions are monitored across a variety of relationship channels. By doing so, we were able to observe that, as per the sum of values, users who showed longer relationships appeared to have an exploitable different feature distribution between both the behaviorally good and bad populations [35].

In addition, we noticed that increasing user-related damage amounts would seem to have a marginal effect in improving the classification model's ability to correctly describe the behaviorally bad population, beyond a certain threshold in all class instantiations, without any behaviorally good changes [36]. While updating the federated model using only weighted global gradients from other model instances did not offer an observable benefit, if better control of channel response data could be obtained, we do believe that if a larger data pool and the private data's greater quality could be leveraged, substantial improvements in various class longer-term models' confidence could be expected. A future focus would be on extracting more detailed product channel response data [37].

References

[1] Syed, S. (2022). Breaking Barriers: Leveraging Natural Language Processing In Self-Service Bi For Non-Technical Users. Available at SSRN 5032632.

[2] Nampally, R. C. R. (2022). Neural Networks for Enhancing Rail Safety and Security: Real-Time Monitoring and Incident Prediction. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 49–63). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1155

[3] Danda, R. R. (2022). Innovations in Agricultural Machinery: Assessing the Impact of Advanced Technologies on Farm Efficiency. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 64–83). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1156

[4] Rajesh Kumar Malviya, Shakir Syed, RamaChandra Rao Nampally , Valiki Dileep. (2022). Genetic Algorithm-Driven Optimization Of Neural Network Architectures For Task-Specific AI Applications. Migration Letters, 19(6), 1091–1102. Retrieved from https://migrationletters.com/index.php/ml/article/view/11417

[5] Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. International Journal of Engineering and Computer Science, 11(08), 25618–25631. https://doi.org/10.18535/ijecs/v11i08.4698

[6] Syed, S. (2022). Integrating Predictive Analytics Into Manufacturing Finance: A Case Study On Cost Control And Zero-Carbon Goals In Automotive Production. Migration Letters, 19(6), 1078-1090.

[7] Nampally, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258

[8] Danda, R. R. (2022). Application of Neural Networks in Optimizing Health Outcomes in Medicare Advantage and Supplement Plans. Journal of Artificial Intelligence and Big Data, 2(1), 97–111. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1178

[9] Chintale, P., Korada, L., Ranjan, P., & Malviya, R. K. (2019). Adopting Infrastructure as Code (IaC) for Efficient Financial Cloud Management. ISSN: 2096-3246, 51(04).

[10] Kumar Rajaram, S.. AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance. In Educational Administration: Theory and Practice (pp. 285–296). Green Publication. https://doi.org/10.53555/kuey.v28i4.7529

[11] Syed, S. (2022). Leveraging Predictive Analytics for Zero-Carbon Emission Vehicles: Manufacturing Practices and Challenges. Journal of Scientific and Engineering Research, 9(10), 97-110.

[12] RamaChandra Rao Nampally. (2022). Deep Learning-Based Predictive Models For Rail Signaling And Control Systems: Improving Operational Efficiency And Safety. Migration Letters, 19(6), 1065–1077. Retrieved from https://migrationletters.com/index.php/ml/article/view/11335

[13] Danda, R. R. (2022). Deep Learning Approaches For Cost-Benefit Analysis Of Vision And Dental Coverage In Comprehensive Health Plans. Migration Letters, 19(6), 1103-1118.

[14] Sarisa, M., Boddapati, V. N., Kumar Patra, G., Kuraku, C., & Konkimalla, S. (2022). Deep Learning Approaches To Image Classification: Exploring The Future Of Visual Data Analysis. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.7863

[15] Syed, S. (2022). Towards Autonomous Analytics: The Evolution of Self-Service BI Platforms with Machine Learning Integration. Journal of Artificial Intelligence and Big Data, 2(1), 84-96.

[16] Nampally, R. C. R. (2021). Leveraging AI in Urban Traffic Management: Addressing Congestion and Traffic Flow with Intelligent Systems. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 86–99). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1151

[17] Ramanakar Reddy Danda. (2022). Telehealth In Medicare Plans: Leveraging AI For Improved Accessibility And Senior Care Quality.

[18] Venkata Nagesh Boddapati, Manikanth Sarisa, Mohit Surender Reddy, Janardhana Rao Sunkara, Shravan Kumar Rajaram, Sanjay Ramdas Bauskar, Kiran Polimetla. Data migration in the cloud database: A review of vendor solutions and challenges . Int J Comput Artif Intell 2022;3(2):96-101. DOI: 10.33545/27076571.2022.v3.i2a.110

[19] Syed, S. (2021). Financial Implications of Predictive Analytics in Vehicle Manufacturing: Insights for Budget Optimization and Resource Allocation. Journal Of Artificial Intelligence And Big Data, 1(1), 111-125.

[20] Syed, S., & Nampally, R. C. R. (2021). Empowering Users: The Role Of AI In Enhancing Self-Service BI For Data-Driven Decision Making. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v27i4.8105

[21] Danda, R. R. (2021). Sustainability in Construction: Exploring the Development of Eco-Friendly Equipment. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 100–110). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1153

[22] Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Kiran Polimetla. An analysis of chest x-ray image classification and identification during COVID-19 based on deep learning models. Int J Comput Artif Intell 2022;3(2):86-95. DOI: 10.33545/27076571.2022.v3.i2a.109

[23] Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Gollangi, H. K. (2022). PREDICTING DISEASE OUTBREAKS USING AI AND BIG DATA: A NEW FRONTIER IN HEALTHCARE ANALYTICS. In the European Chemical Bulletin. Green Publication. https://doi.org/10.53555/ecb.v11:i12.17745

[24] Wang, X., & Thompson, B.. *AI-Driven Insights: The Role of Cloud Analytics in Shaping Data Narratives for Business Strategy*. International Journal of Artificial Intelligence and Data Analytics, 41(3), 184-203. https://doi.org/10.1007/ijai.41.03

[25] Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions Educational Administration: Theory and Practice, 27(4), 1228 –1236 Doi: 10.53555/kuey.v27i4.7592

[26] Roberts, J., & Garcia, P. (2022). *Exploring AI Storytelling: Bridging the Gap Between Cloud Analytics and Actionable Insights*. Journal of Digital Transformation, 8(1), 46-58. https://doi.org/10.1016/j.jdt.2022.01.008

[27] Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Data-Driven Management: The Impact of Visualization Tools on Business Performance, International Journal of Management (IJM), 12(3), 2021, pp. 1290-1298. https://iaeme.com/Home/issue/IJM?Volume=12&Issue=3

[28] Lin, H., & Jackson, E.. *AI-Driven Narrative Visualization: A New Era of Cloud-Based Data Storytelling*. Journal of Advanced Analytics, 39(5), 415-431. https://doi.org/10.1109/jaa.39.05

[29] Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Venkata Nagesh Boddapati, Manikanth Sarisa, An Analysis and Prediction of Health Insurance Costs Using Machine Learning-Based Regressor Techniques, International Journal of Computer Engineering and Technology (IJCET) 12(3), 2021, pp. 102-113. https://iaeme.com/Home/issue/IJCET?Volume=12&Issue=3

[30] Chen, Z., & Patel, V. (2021). *Storytelling with Data: Integrating AI into Cloud Analytics for Business Intelligence*. International Journal of Data Science, 23(3), 98-115. https://doi.org/10.1093/ijds.2021.23.03

[31] Venkata Nagesh Boddapati, Eswar Prasad Galla, Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Gagan Kumar Patra, Chandrababu Kuraku, Chandrakanth Rao Madhavaram, 2021. "Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times", ESP Journal of Engineering & Technology Advancements, 1(2): 134-146.

[32] Miller, R., & Huang, W.. *AI-Powered Narratives: Leveraging Cloud Analytics for Smarter Decision Making and Business Solutions*. Jour

[33] Ravi Kumar Vankayalapati, Chandrashekar Pandugula , Venkata Krishna Azith Teja Ganti , Ghatoth Mishra. (2022). AI-Powered Self-Healing Cloud Infrastructures: A Paradigm For Autonomous Fault Recovery. Migration Letters, 19(6), 1173–1187. Retrieved from https://migrationletters.com/index.php/ml/article/view/11498

[34] Tulasi Naga Subhash Polineni, Kiran Kumar Maguluri, Zakera Yasmeen, Andrew Edward. (2022). AI-Driven Insights Into End-Of-Life Decision-Making: Ethical, Legal, And Clinical Perspectives On Leveraging Machine Learning To Improve Patient Autonomy And Palliative Care Outcomes. Migration Letters, 19(6), 1159–1172. Retrieved from https://migrationletters.com/index.php/ml/article/view/11497

[35] Venkata Obula Reddy Puli, & Kiran Kumar Maguluri. (2022). Deep Learning Applications In Materials Management For Pharmaceutical Supply Chains. Migration Letters, 19(6), 1144–1158. Retrieved from https://migrationletters.com/index.php/ml/article/view/11459

[36] Maguluri, K. K., Pandugula, C., Kalisetty, S., & Mallesham, G. (2022). Advancing Pain Medicine with AI and Neural Networks: Predictive Analytics and Personalized Treatment Plans for Chronic and Acute Pain Managements. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 112–126). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1201

[37] Lekkala, S. (2021). Ensuring Data Compliance: The role of AI and ML in securing Enterprise Networks. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v27i4.8102