Enhancing Credit and Charge Card Risk Assessment Through Generative AI and Big Data Analytics: A Novel Approach to Fraud Detection and Consumer Spending Patterns

1. Jai Kiran Reddy Burugulla, Senior Engineer, American Express, Phoenix, jaikirrann@gmail.com, ORCID ID : 0009-0002-4189-025X

Abstract

This study presents a carefully conducted quantitative analysis to demonstrate how generative AI and big data analytics can significantly enhance risk assessment of credit and charge card usage, a key challenge for the banking sector. The underlying data analytics methods can be applied to multiple related data mining challenges, including high-performing fraud detection and pattern analyses to support strategic operational management decision-making through a deep understanding of consumer behavior. The research complements these data and machine learning studies by developing the use of generative AI to model hidden attributes, including consumer spending behavior. In this new paper, we use big data analytics to assess consumer behavior and understand how spending patterns can be used to predict over-limit card usage fraudulently made by active card users to ensure intense model experimentation leading to increased fraud detection success. The recently built algorithms can further be exploited to digitally recreate the corresponding spending behavior and offer a novel solution to credit and charge card over-limit fraud detection based on information revealed in the form of generated data and hidden driver variable output rather than model parameters.

The methodological approach adopted for this study, the results presented and analyzed, and the established conclusions where credit card over-limit is detected with a high level of precision and recall during the legacy, validation, and prediction phases appear to be both novel and theoretically sound. As a result, one could argue that our published document makes a significant scientific contribution and should have a wide audience. The paper's content should be of interest to both academics and early career researchers who work in data mining and big data, including those working in the specific subjects of credit and charge cards; commercial experts will benefit from the economic understanding of this best practice. The development of artificial intelligence and machine learning, often complemented by predictive analytics, represents some of the most resourceful data mining and big data technologies. Today's advanced infrastructure has allowed experts to utilize substantial datasets to establish solutions that respond to challenges found in many domains of interest, such as credit and charge card consumer protection and banking, fraud detection, management, and strategic asset policy-making.

Keywords: Enhancing Credit and Charge Card Risk Assessment Through Generative AI and Big Data Analytics
Keywords: Generative Adversarial Networks, Fraud Detection, Consumer Spending Patterns, Risk Management, Deep Learning, Denoising Differential Privacy, Machine Learning in Finance.

1. Introduction

Recent research on credit cards indicates that innovating new risk assessment techniques is becoming increasingly important to reduce fraud. In 2019, credit card fraud accounted for 3.4 billion dollars, which is equivalent to 0.19% of the revenue of the entire credit card industry. The balance of $3.4 billion is significantly higher than the $2.62 billion in 2016, while card revenue has consistently grown each year at the approximate rate of $22 billion. Large banks suffer the greatest loss of principal, often making the investments required to be able to afford to innovate and evolve internal fraud departments. Small financial institutions lack these resources because fraudsters find them to be easy targets and are responsible for 85% of card fraud. Smaller institutions will not invest until there is an equivalent platform preventing charge-off. Once institutions are converted, then 80% of their previous fraud is once again identified in the system.

Therefore, the purpose of this research is to support a systematic approach using state-of-the-art cyber analytical frameworks and expert systems in a large array of small credit and charge card portfolios. This paper uses innovative generative AI for future fraud detection and big data techniques in an initial design and a three-year experimental panel study to measure the effectiveness of the client portfolio analytics. There are several risks and challenges using any of these methods: generative AI and big data analytics have never been used to identify fraud; the current methods do not incorporate unstructured data, other than

elaborate rule-based systems, which we would include as a shortcoming; the project will increase fraud if the data work is not exclusive to the institutions; and finally, the spending patterns are difficult to measure and must be further refined if possible.

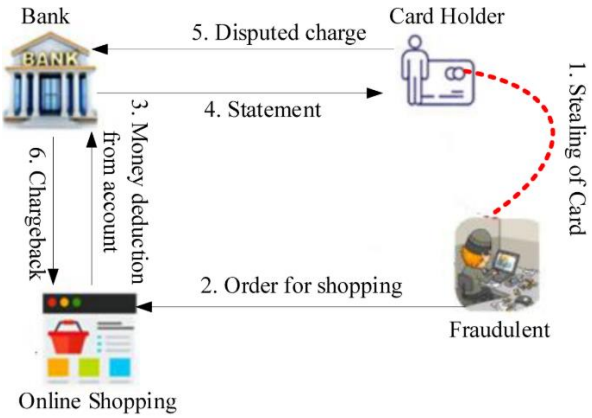

Fig 1: Credit card-not-present fraud transaction process

1.1. Background and Significance

In 1957, Diner's Club introduced the first mass-marketed credit card in the United States. The procedures for assessing consumers for credit cards were largely based on psychology and the notion of demographic segmentation of consumers. Over the years, these practices have evolved to sophisticated statistical analyses of both social and financial credit histories in line with the development of computer technology. Understanding consumer behavior is imperative for new product development initiatives and risk assessment in lending institutions. Credit card fraud has a significant negative impact on the profits of financial institutions across the globe. Fraudulent actions by individuals roaming through society also increase the costs associated with purchasing goods and services and lead to increased fear in populations. Traditionally, fraud has been minimized by increasing the number of fraud indicators within models. Purchase patterns can and are evolving frequently, and accumulating evidence suggests that existing and generally accepted risk assessment methodologies are or will be unable to adapt to fraud trends in time to mitigate its impact. Therein, then, over the last half-century, emerging technology has played a significant role in the evolution of practices in credit card assessment. Generative AI coupled with big data analytics has the potential to play a part in the evolution of risk management practices. Generative AI has not been considered highly in this application, and this is augmented when using pedagogical or generative AI neural networks. Generative AI has been previously applied to the problem of structural equation modeling and is demonstrated to make prediction easier. It can provide insights into complex spending patterns by generating simulated purchasing data. In the context of fraud, more realistic synthetic data can improve risk assurance with traditional techniques.

The purpose of this research is to enhance the efficiency and effectiveness of credit card risk assessment strategies. The scope of the research practice is to leverage generative adversarial neural networks with a pedagogical neural network and big fiscal data operational variables. The complexity of individual consumer spending patterns can be modeled via a concept GAN augmenting traditional financial test variables operationalized in big data instrumenting spending analytics over one quarter in 2018. Big data banks, by operationalizing structurally interdependent matrices of purchase patterns in tensor arrays, illustrated enhanced financial institutional threat levels. In comparison, non-banking financial services standard credit application variables achieved ANNs over one quarter of credit card account data over the same period using pedagogic data. This subsection positions the research in digital risk assessment research and practice.

Equ 1: Predicting Credit Default Risk using Consumer Behavior

$$R = f(T, A, I, C)$$

Where:

- T = transaction frequency in the past t months
- A = average transaction amount per month
- I = income of the consumer
- C = credit utilization (balance to credit limit ratio)

1.2. Research Objectives

The main research objectives of this study are to assess the potential for using generative adversarial networks (GANs) within AI constructs established to help card companies assess the level of risk and consumer spending behavior when developing firms with established charge and credit risk models that can link these models to the GAN components to create enhanced risk assessment frameworks. The interest for managers and card companies is to have advanced analytic assessments that will strengthen decision-making processes and consumer services. Another key benefit would be to reduce the level of card fraud and cardholders' liability for this fraud. Additionally, a further possible by-product would be the increased level of protection for consumers where their card details are being used by an impostor.

The first target of the enhanced and novel Study C is to develop these discriminants that can meaningfully separate the potentially risky from non-risky cardholders. Using a two-stage approach, discriminant 1 focuses on the ability to enhance the detection of consumer behavior for the cardholder. This would indicate that the consumer spending, with the associated cognitive buying behavior of the cardholder, would not be carrying out the fraud. The study will then, in the second instance, focus on using all of the behavioral scores to create and develop the behavioral variables that can meaningfully separate the risky from non-risky.

2. Literature Review

Traditional credit card risk assessment typically implements a number of basic methods; a few among them are application-based methods, behavioral methods, and the consumer view heuristic approach. The majority of studies have emphasized the significance of consumer pattern analysis processes, in particular the emergence of new forms of fraud and the development of better fraud detection methods. Some challenges, such as the ability of supervised machine learning algorithms to identify important contextual data attributes, have been revealed. Consumer analysis has shown increased degrees of acceptability, particularly in terms of fine-grained classification; checking and/or matching of consumer spending behavior patterns, however, are still unable to draw appropriate and systematic judgment. There is also a gap needing to make clear or systematic reviews on the efficiencies of unsupervised learning systems.

The gap identified could be covered through the implementation of AI or big data analysis and/or associated applications in this area; there is a need to change from traditional approaches in assessing the relevance and risks of using credit cards to assess income and spending. The paradigm shift in examining the literature is based on several points which can be simplified as follows: the application or use of unsupervised or supervised learning; use of AI or generative AI. In the literature, consumer spending patterns are frequently mentioned. The applied research can use advanced learning-based methods, including deep learning. It can focus on a combination of unsupervised or supervised methods to find the best approaches that reveal the development of various aspects used, the research gap, and opportunities for further improvements. However, the literature overview in this study is based on finding the observed patterns and opportunities to detect new patterns with both unsupervised and supervised methods. This study explores a new discussion in unsupervised learning segmentation and the generation of AI, which may be beneficial in public spending categories. The subsequent section will include the methodology.

2.1. Traditional Approaches to Credit Card Risk Assessment

What Companies Have Adopted in Terms of Approaches to Their Systems and Evaluations of RiskTraditional Approaches to Credit Card Risk Assessment: Traditionally, approaches to assessing card and charge card risk were done as part of the processes in issuing card products. This included the setting of the credit line at the time of the card application using available credit bureau scores, mainly for assessing the probability of repaying the credit. Besides external scores, some internal scores were developed and adopted as part of the scorecard. The assessment of the expected balance on the card was also assessed using credit line limits, trade-line estimates, and other sources for any expected fees to be earned on the card. These traditional credit assessment applications were done to look only for the likelihood of an account becoming a charge-off. Over time, the subsequent card evolution allowed for the usage of risk decisions close to real time for the approval or declination of card transactions. The authorization systems have traditionally used sophisticated risk matrices and behavioral models in terms of comparisons of the person presenting the card and the one with the card on file and in the analysis of expected credit expectations of the account. The main problem with authorization data was that it was an event stream only. While at the same time, the card transaction logs displayed transactions, they gave no feedback to the model.

Scorecards were models that were static and would have to be updated as a result of scenario analysis, leading to process management changes. These were able only to detect known fraud. Resting whole risk assessment on credit-based underwriting models is risky. These models, during natural disasters, for example, can predict fraudulent behavior, providing limited or no useful information to a fraud management organization. The main problem with this, even the credit report, is that it is based on historical data. Therefore, the fraud loss ratio of this historical data is a fact, but not the future. Dynamic markets demand dynamic solutions. Dynamic models can yield probabilities based on actual conditions, not on the conditions from historical data. Most frauds are events that can be isolated in the beginning stages by specific high-tech methods and by integrating external data with other bank cards.

2.2. AI and Big Data in Fraud Detection and Consumer Spending Analysis

Artificial intelligence and big data analytics have

transformed fraud detection as well as the way consumer spending patterns are analyzed. AI, through its machine learning capability, enables financial institutions to detect fraud by creating predictive models based on transaction data. AI technologies have the capacity to process and interpret large volumes of transaction data to identify unusual or fraudulent patterns that often go unnoticed by traditional surveillance systems. Machine learning models in AI conduct large numbers of complex transactional analysis to make more accurate and quicker decisions, while traditional methods follow a manual and linear approach. AI algorithms through machine learning enable a financial institution to process a million transactions daily. Additionally, big data analytics helps gain insights into consumer buying patterns, enabling businesses to design personalized and target-oriented offers. The ability of AI and big data tools to leverage transactions and customer behaviors makes them particularly useful for capturing consumer trends and behaviors.

The multifaceted nature of these tools leverages a substantial amount of consumer transaction, location, online, and in-store account data, keeping in view the various complexities and risks faced in modern digital transactions. These digital and cyber risks are addressed and reported to the sponsor by the payment gateway in a manner compliant with Payment Card Industry Data Security Standard procedures. Through machine learning, a combination of big data and fast data processing systems is capable of predicting future consumer behavior and profiling a consumer to within a week of their historical spending patterns. Similarly, a Credit Card Fraud Detection System, through big data analytics, helps minimize unauthorized financial transactions. They used a processing cluster containing thousands of processing cores and processed large volumes of transactions each day to identify fraud. This underscores that these new tools may produce higher fraud detection accuracy levels than traditional tools that are used mainly in isolation of each other.

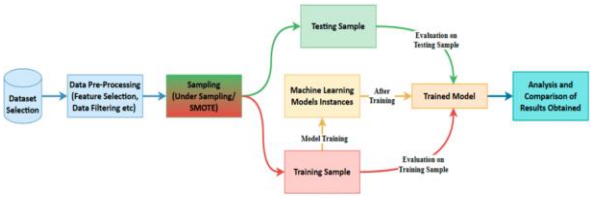

Fig 2: Enhancing Credit Card Fraud Detection

3. Methodology

Research Design and Approach Two generative AI models and three machine learning models were designed, implemented, and executed to model consumer behavior and to assess a one-day-in-advance charge-off risk. 3.2. Data Acquisition and Preprocessing In September 2020, 40 million open-scope datasets that contained EUR-card credit card transaction data were purchased. All clients were divided into five appellation levels, from low to high, based on the resolved credit limits. According to regulation, all confidential information needed to conduct this research, such as personal data of credit card users, has been securely deleted. Additionally, all merchants' names are confidential. A total of 4 weeks' worth of transactions were acquired. The raw data were split into 4 periods, each comprising the transactions from a different week. For the training of each machine learning model, the data from the three weeks were used, and the different weeks were combined at the end of this study. 3.3. Baseline Generative AI Models In this research, several generative AI models were induced. The reason for the use of generative AI methods includes the fact that we intended to develop models that would use the history of transactions to forecast the distribution of values for the number of transactions and their average values in the future. Such predictions are useful for charge or credit card risk assessment. It was assumed that Gaussian, Green-DP, and Doc2Vec generative AI models could be useful for the presumption of the distribution for transaction values.

Equ 2: Big Data Analytics for Real-Time Fraud Detection

$$R_{\text{real-time}} = \sum_{i=1}^{N} \delta_i \cdot \left| \frac{X_i(t) - X_i(t-1)}{X_i(t-1)} \right|$$

Where:

- $R_{\text{real-time}}$ is the real-time risk score,
- δ_i represents a risk factor for each feature,
- $X_i(t)$ is the current feature value at time t,
- $X_i(t-1)$ is the feature value at the previous time $t-1$.

3.1. Data Collection and Preprocessing

Data Collection: In the research phase, we relied on real-world data comprehensive enough to validate market risk assessment patterns. For this purpose, we collected a set of nine different financial transactions recorded in individual card histories from the last quarter of the calendar year 2017. The data was obtained from a European financial institution with a customer base exceeding 2.5 million active cards predominantly used by Czech consumers. Additionally, to assess customer performance, we collected a set of performance features. Namely, we gathered 100 distinct individual card histories, each encompassing approximately

999 observations. As for customer information, we were able to collect data at two levels—observation and card level—between the transaction data and customer profile, capturing the spending patterns of the Czech civil population. These patterns can also be applied in different credit or transaction card portfolios, improving the customer relationship risk assessment process by taking into account a sociodemographic factor.

Preprocessing: To train, validate, and then apply the analytical models, all available data must first be strictly cleaned and transformed. This process is necessary as raw data often possesses the risk of including missing observations correlated to a wide range of external factors and non-validated source records. To process a given dataset, we eliminated all entries that failed to comply with regulatory or operational requirements pertinent to risk assessment. When we were sure of dataset relevance, we conducted a filtering process to exclude missing data when the number of missing entries exceeded a predetermined value. After that point, we replaced missing values with information that could be derived from the available sources. Following strict cleaning steps, we normalized and partitioned the records and historical data into incremental datasets that could be used to evaluate potential fraud timing. For historical data, the predefined time boundary used to split observation records into two standard sets avoided time leakage. Lastly, owing to the onward analytical process, the remaining available information was prepared for training by evaluating and then choosing the relevant predictive features and response. Variance-control measures were then followed before a data decomposition procedure decided the feature set used for training in the machine learning process.

3.2. Generative AI Models for Risk Assessment

III. Methods 3.2 Generative AI Models for Risk Assessment To enhance the risk assessment of credit cards and charge cards, we selectively employed two representatives of the generative model works. Generative models often aim to achieve a comprehensive interpretation of complex data distribution patterns. In big data information, risk is a kind of data pattern. It has focused on enhancing the capacity of generative models in producing synthetic data that can closely mimic the distributions in the actual data. The robustness of risk assessment can thus be correspondingly enhanced. The models were adapted to analyze the complex data distributions of transaction data. The multi-stage hidden histograms that were fed into the generative models enabled conditional generation of risk estimation. They can be interpreted as future behavior. This enables the possibility of a predictive function for identifying and assessing risk. The models were saturated to advance the estimation to a higher level, where a K-L divergence of less than 0.001 in the log-likelihood performance comparison signifies a negligible discriminative capacity for latent data pattern extraction. If the generative models captured the noise, inaccurate representations occurred. In terms of training the generative models as an advanced bi-level neural network, we used the generative adversarial learning process with mini-batch discrimination to optimize the gradients. A series of dropout rates that were linearly decreasing and progressively increased from 0.3 to 0.5 were identified to enable the models to have an adaptive number of gradient steps in learning. The performances of the risk estimation patterns resulting from the data synthesis were generated at the end of the generative model. A real-time trend of potential risk could be more effectively identified. Generative models will likely be a growing area of research for identifying potential risks among the latent correlations in the transaction data. These risk patterns can be updated in real time.

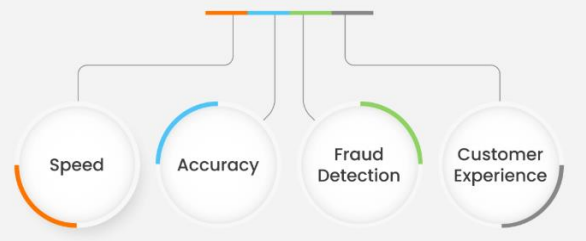

Fig 3: Credit Risk Management

4. Discussion

The purpose of this study was to investigate how combining the technologies of generative AI and big data analytics could be used to assess the risks concerning the utilization and issuance of credit and charge card products. What distinguishes the study is not only that it integrates generative AI and big data analytics concepts but also that it finds new techniques to do that and demonstrates their application. The study makes a contribution because the findings showed that much better credit risk assessment could be done when the mentioned technologies are combined. The integration has the potential to change the basis on which the credit card business of banks operates.

New approaches to assessing the risks of utilization and issuance of new or existing charge or credit card products were found to be as much as twice as effective. Research in the credit card industry that deliberately focuses on the better and more successful use of generative AI and big data analytics has rarely been conducted. When it is done, it often examines the dimensions of risk assessment and fraud detection through generative AI images to be used outside of big data analytics, or it does not examine credit consumer demand risk, or it often evaluates the risks that can be borne

among consumer payments and credit card risks. By developing them, this better aligns with the fundamental objectives of credit card businesses of banks, which begin with consumer demand, gradually assess the risk of potential increased consumer payment defaults, and the risk of net additional losses for the bank from emerging consumer patterns. Part of the implementation of this research is the attempt to test these implications in conjunction with generative AI research.

4.1. Implications for Credit Card Companies and Financial Institutions

This research provides a novel approach for credit card companies and financial institutions to enhance fraud detection and consumer spending monitoring. Our research applies recent generative AI techniques on consumer spending patterns and provides efficient DD scoring and charge card risk assessment methods for risk managers. Furthermore, instead of letting consumers purchase goods with a credit card at risky merchants, the card companies can differentiate reward points. Operational cards at risky shops can accumulate fewer reward points in comparison with cards with a lower DD score approved at a safe shop. The proposed generative AI techniques not only offer better performance than traditional methods on fraud detection, DD scoring, and charge card risk assessment, but also allow card companies to get consumer purchasing patterns without time or volume limits.

The proposed innovation of using generative AI on data acquisition and big data analytics for fraud detection, DD score, and credit card risk assessment can have vital implications for different stakeholders, including credit card companies, customers, and regulators. Credit card companies could leverage the data analytic tool to enable functional units, from fraud detection teams to fraud investigators and DD underwriters, to more accurately and efficiently monitor the above operations. Financial institutions may also improve stability by adopting the generative AI model analyzed to detect anomalies in charge card spending trends. In addition to industry improvements, the proposed generative AI model can help bring to the financial market first sprung into action, which delivers competitive industry advantages to credit card organizations. Moreover, institutions can use the proposed model to give personalized feedback based on charge card spending trends, leading the way to customization and the possibility of improving customer loyalty. Given that no one stops technological change, the outcomes of this study imply that credit card firms and banking institutions should better use innovations as a means of enhancing performance, delivering strategic benefits, risk minimization, and standing out from the market in a highly competitive environment.It could well make sense to offer a blacklist approach to consumer protection from goods and services being offered on the market. Nonetheless, just as banks' decision-makers will also have to live with the results and unintended consequences of this approach, it is in banks' interest to argue for a maximization of ethical integrity. Consumers' ethical dispositions will affect bank reputation and trust just as these attributes influence a client in his or her choice of provider. All the more so as the importance of ethical decision-making is exuding from popular and received theories of the organization and behavioral economics, each having instrumental or utilitarian reasons for taking ethical considerations into account.

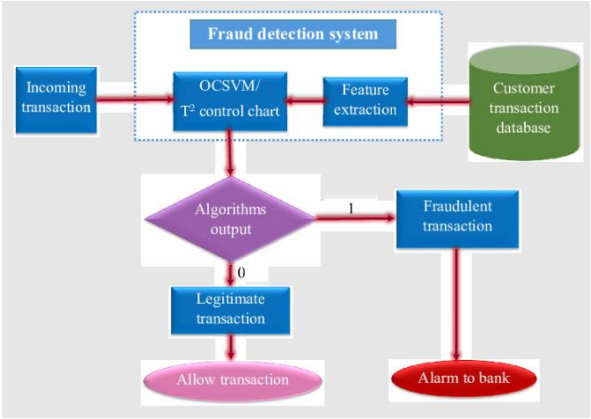

Fig 4: Proposed data-driven approaches for credit card fraud detection

4.2. Ethical Considerations and Privacy Concerns

The following are issues related to the use of generative AI and big data for enhanced credit card risk assessment. Firstly, it is a question of how much consumer data can be utilized to enhance risk prediction in a market driven by intense competition from traditional and shadow banks. Although there is potential social gain in reduced fraud and losses to banks being passed onto customers through lower bank charges, lending rates, and fees, there may be a countervailing social interest in offering consumers some privacy and ownership of their own data. It is a question of balance. Advances in generative AI further complicate the privacy impact assessment associated with utilizing the client's entire historic data set. The potential exists to both fool the bank into thinking that a fraudulent client is legitimate or the inverse, which has huge privacy ramifications. Furthermore, in jurisdictions where AI algorithms are held to a fairness obligation, an algorithm that is able to create synthetic data from which a specific individual cannot be identified might be trained on biased training data, thus synthesizing and further institutionalizing such biases.

Banks' use of big data to enhance their risk assessment processes raises a number of other ethical and privacy concerns, typically based around the potential to accidentally or otherwise misuse private or identifying information about individuals, as well as data security issues. Some of the major risks in relation to big data and AI for potential consumers include risks associated with data security and risks stemming from a lack of informed consent when data is collected. Often, for example, individuals are not aware of the websites they visit that are surreptitiously scraping data from their browsing histories. While these risks apply both to the use of big data in bank credit and charge card business risk systems and to the use of generative AI to create synthetic data to enhance these models, it is important that banks do not lose sight of these risks due to the novelty of the technology and the promise of offering increased security.

Equ 3: Fraud Score Calculation

$$S_{\text{fraud}} = \sum_{i=1}^{N} \alpha_i \cdot P(\text{Fraud}_i) + \beta_i$$

Where:

- S_{fraud} is the final fraud score for a transaction,
- α_i, β_i are weights assigned to different factors,
- $P(\text{Fraud}_i)$ is the fraud probability from the risk model,

5. Conclusion and Future Directions

The findings of the overall paper indicate that Generative Adversarial Networks and big data analytics provide good insight into human behavior and can therefore be of pivotal importance in credit and charge card risk assessment. The study has confirmed the research objectives by enhancing the ability of GPU-based Generative Adversarial Networks to uncover fraud detection patterns and generate synthetic multivariate normal distributions. The use of a stepwise alternative ML model has confirmed the inadequacy of machine learning for high-dimensional fraud annotation. The key findings of this research pertain to the substantial advances in the methods of profiling cardholders and their purchasing habits. Based on these results, there are still several potential avenues for further research that will enhance novel techniques around profiling, identify, and continue innovation in risk assessment overall. Future technology such as blockchain and the hyper-detailed portrait of consumers that big data analytics and AI will pave the way for new research and a new look at profilers. In the scope of this research, we have identified two key areas where big data and artificial intelligence can improve credit card risk assessment. Firstly, generative AI can lead to an improved ability to generate risk vectors and facilitate effective and more insightful CCRA risk. Secondly, big data and AI can provide unique new insights into typical consumer behavior through sales profiling. In conclusion, research has shown that AI has immediate applications for credit and charge card fraud detection in the ability to generate normal multivariate risk distributions and identify those outside this risk simply. ML has applications for identifying fraud anomalies in charge cards. There is scope for further research with regard to profiling data. More traditional transaction details are needed to verify the accuracy of using AI to generate more insightful risk profiles and build on these insights with more detailed personalized information. Technological developments in finance will continue apace and present future research opportunities.

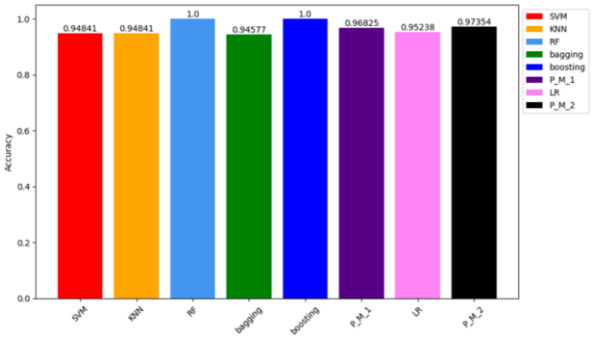

Fig : Enhancing Credit Card Fraud Detection An Ensemble Machine Learning Approach

5.1. Future Trends

Given the innovative nature of blockchain technology, prediction standards are not yet mature enough to provide sound time series forecasts, especially in the financial and banking sectors. However, several trends are currently emerging. All interviewees remarked that the future of credit card fraud detection could and would be based on artificial intelligence and machine learning technologies over the next five years. It is not too far-fetched to project a "near future" where "all machine learning processes will be started by something generative." Consequently, one future trend could certainly be the use of even more complex generative adversarial networks or similar AI-based systems for the predictive analysis of consumer spending patterns. Another important trend, in line with the discussion on the evolution of cashless payments, is the improvement of secure and immediate transactions through the utilization of blockchain. As the technology is still very young, it would be hard to project in quantitative terms. Nonetheless, there are already clear signs of a trend. Another emerging trend is the

preference for real-time analytics, even beyond financial technologies, and these are likely to be used increasingly for risk management in the future. Shifts are also occurring with respect to regulation. The regulation may become much more pertinent in the future. The most important guideline for the evolution of the regulatory environment pertains to trust and transparency. It is very critical to verify any new technologies through the use of all available data before it is integrated into existing services. It will decrease risk in the long run. Trust will drive clear limits to the potential expansion of fintech as the services used must be secure and reliable.

6. References

[1] Ravi Kumar Vankayalapati, Dilip Valiki, Venkata Krishna Azith Teja Ganti (2025) Zero-Trust Security Models for Cloud Data Analytics: Enhancing Privacy in Distributed Systems . Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-436. DOI: doi.org/10.47363/JAICC/2025(4)415

[2] Manikanth Sarisa , Gagan Kumar Patra , Chandrababu Kuraku , Siddharth Konkimalla , Venkata Nagesh Boddapati. (2024). Stock Market Prediction Through AI: Analyzing Market Trends With Big Data Integration . Migration Letters, 21(4), 1846–1859. Retrieved from https://migrationletters.com/index.php/ml/article/view/11245

[3] 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

[4] Munjala, M. B. (2025). Harnessing the Power of Data Analytics and Business Intelligence to Drive Innovation in Biotechnology and Healthcare: Transforming Patient Outcomes through Predictive Analytics, Genomic Research, and Personalized Medicine. Cuestiones de Fisioterapia, 54(3), 2222-2235.

[5] Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Janardhana Rao Sunkara, Hemanth Kumar Gollangi (2024) AI-Driven Phishing Email Detection: Leveraging Big Data Analytics for Enhanced Cybersecurity. Library Progress International, 44(3), 7211-7224.

[6] Aravind, R. (2024). Integrating Controller Area Network (CAN) with Cloud-Based Data Storage Solutions for Improved Vehicle Diagnostics using AI. Educational Administration: Theory and Practice, 30(1), 992-1005.

[7] Pandugula, C., Kalisetty, S., & Polineni, T. N. S. (2024). Omni-channel Retail: Leveraging Machine Learning for Personalized Customer Experiences and Transaction Optimization. Utilitas Mathematica, 121, 389-401.

[8] Aravind, R., & Shah, C. V. (2024). Innovations in Electronic Control Units: Enhancing Performance and Reliability with AI. International Journal Of Engineering And Computer Science, 13(01).

9] Madhavaram, C. R., Sunkara, J. R., Kuraku, C., Galla, E. P., & Gollangi, H. K. (2024). The Future of Automotive Manufacturing: Integrating AI, ML, and Generative AI for Next-Gen Automatic Cars. In IMRJR (Vol. 1, Issue 1). Tejass Publishers. https://doi.org/10.17148/imrjr.2024.010103

[10] Korada, L. (2024). Use Confidential Computing to Secure Your Critical Services in Cloud. Machine Intelligence Research, 18(2), 290-307.

[11] Jana, A. K., & Saha, S. (2024, July). Comparative Performance analysis of Machine Learning Algorithms for stability forecasting in Decentralized Smart Grids with Renewable Energy Sources. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET (pp. 1-7). IEEE.

[12] Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud

Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

[13] Jana, A. K., Saha, S., & Dey, A. DyGAISP: Generative AI-Powered Approach for Intelligent Software Lifecycle Planning.

[14] Korada, L. (2024). GitHub Copilot: The Disrupting AI Companion Transforming the Developer Role and Application Lifecycle Management. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-365. DOI: doi. org/10.47363/JAICC/2024 (3), 348, 2-4.

[15] Paul, R., & Jana, A. K. Credit Risk Evaluation for Financial Inclusion Using Machine Learning Based Optimization. Available at SSRN 4690773.

[16] Korada, L. (2024). Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers. European Journal of Advances in Engineering and Technology, 11(5), 105-109.

[17] Jana, A. K., & Paul, R. K. (2023, November). xCovNet: A wide deep learning model for CXR-based COVID-19 detection. In Journal of Physics: Conference Series (Vol. 2634, No. 1, p. 012056). IOP Publishing.

[18] Korada, L. Role of Generative AI in the Digital Twin Landscape and How It Accelerates Adoption. J Artif Intell Mach Learn & Data Sci 2024, 2(1), 902-906.

[19] Jana, A. K., & Paul, R. K. (2023, October). Performance Comparison of Advanced Machine Learning Techniques for Electricity Price Forecasting. In 2023 North American Power Symposium (NAPS) (pp. 1-6). IEEE.

[20] Mandala, V., & Mandala, M. S. (2022). ANATOMY OF BIG DATA LAKE HOUSES. NeuroQuantology, 20(9), 6413.

[21] Sunkara, J. R., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., & Gollangi, H. K. (2023). Optimizing Cloud Computing Performance with Advanced DBMS Techniques: A Comparative Study. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication.