AI Enabled Credit Card Fraud Detection System Using Cloud Computing

Abhishek Shinde*, Rohit Shinde, Satish Chavhan, Alpana Borse

Department of Information Technology PCCOE Pune, India
*shindeabhishek2199@gmail.com

* Corresponding author
doi: https://doi.org/10.21467/proceedings.7.6.52

Abstract

With the exponential growth of digital monetary transactions, the risk of credit card fraud has considerably extended, necessitating the improvement of advanced, real-time fraud detection structures. This studies aimed to design and compare a cloud-based answer powered by using synthetic intelligence (AI) to discover fraudulent transactions with high accuracy and low fake advantageous costs. A hybrid technique combining supervised system getting to know fashions and privacy engineering strategies was adopted to deal with demanding situations which include data imbalance and evolving fraud patterns. The method concerned the deployment of algorithms which include Support Vector Machines (SVM) and Naive Bayes (NB) on a synthetic yet sensible transaction dataset. Hybrid sampling strategies, which include a mixture of Synthetic Minority Oversampling Technique (SMOTE) and random underneath-sampling, were carried out to balance the dataset and improve model robustness. The gadget architecture was designed on a cloud platform to permit scalability and real-time transaction tracking. High-performance models have been deployed as APIs to method streaming statistics and provide instant class of transactions. Additionally, an Explainable AI (XAI) module was incorporated to enhance model transparency and guide regulatory compliance through supplying interpretable predictions. The findings confirmed that AI models should locate fraudulent interest in actual-time with over 99% accuracy, while additionally notably lowering fake positives. The use of cloud infrastructure facilitated dynamic resource scaling and ensured non-stop availability of the detection provider. The proposed framework proved effective in addressing key issues inclusive of integration complexity, information privateness, and real-time responsiveness. This have a look at concluded that the integration of AI, cloud computing, and explainable frameworks presents a scalable and sincere answer for modern-day credit score card fraud detection. Future directions include incorporating federated learning and blockchain technology to in addition decorate safety and transparency.

Keywords: *credit card fraud, artificial intelligence, cloud computing*

1. INTRODUCTION

The rapid increase in digital financial transactions helps both businesses and consumers. Yet the rise occurred in credit card theft, which led to serious financial losses and safety risks. Traditional fraud detection techniques have failed to keep up with the ever-changing tactics used by criminals. This shows how rapidly advanced, scalable, and flexible methods need to be built so as to detect and prevent fraudulent conduct in real time. The goal of this research is to look at how cloud computing and artificial intelligence (AI) may be used to develop efficient systems to identify credit card fraud. Artificial intelligence (AI) tools, such as machine learning algorithms and anomaly detection models, have enormous potential to detect suspicious patterns and anticipate fraudulent activities. By providing the processing authority, scalability, and flexibility needed to manage huge amounts of transaction data in real time, cloud computing improves AI. The goal of this study is to identify the primary AI fraud detection methods, explain how cloud-based platforms enable real-time processing, and assess the difficulties of implementing such solutions. Managing unbalanced databases, preserving data privacy, and addressing system adaptation to novel methods of fraud represent a few among these issues. Given the risks involved and the increasing reliance on electronic payment methods, an investigation is essential.

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

Although substantial progress has been made in fraud detection using AI and cloud computing, most existing systems either lack real-time capabilities or struggle with issues like data imbalance, high false positives, and integration complexity. Additionally, there is limited research focusing on integrating explainable AI (XAI) for transparent decision-making in fraud detection. This study attempts to fill these gaps by proposing a cloud-based AI system with high real-time detection accuracy, reduced false positives, and interpretable outputs to help financial institutions meet compliance and trust requirements.

2. LITERATURE REVIEW

A. Credit Card Fraud Detection Using Optimized Cloud Infrastructure

The rapid increase in online transactions has substantially heightened the hazard of credit card fraud, prompting the need for superior detection structures. The paper examines the enhancement of cloud-based architectures for real-time fraud detection in credit card transactions. By using cloud technologies, machine learning, and artificial intelligence, companies can successfully handle large volumes of transaction datasets, allowing them to identify fraudulent activities and adapt to new fraud patterns. Key features include data ingestion, real-time data processing, and machine-learning model deployment, all of which are vital for effective fraud detection. The study also focuses on data privacy and compliance with regulatory measures. Furthermore, the author emphasizes the necessity of efficient data governance and secure information management to ensure confidentiality and integrity. The results demonstrate that cloud infrastructures provide elasticity and scalability while maintaining performance during high-volume transactions. The inclusion of notification and alerting mechanisms helps organizations detect anomalies quickly and take preventive measures. The overall approach supports the digital financial ecosystem in adapting to evolving fraud mechanisms, proving that optimized cloud frameworks play a pivotal role in proactive credit card fraud detection.[1]

B. AI-Powered Fraud Detection in Identity and Access Management

This study explores the role of artificial intelligence in enhancing fraud detection within Identity and Access Management (IAM) systems for organizations handling vast user datasets. It tackles the challenges of rapid data processing, continuous authentication, and evolving attack patterns. AI techniques such as machine-learning algorithms, anomaly detection, and pattern recognition can efficiently identify suspicious behavior that traditional IAM systems often overlook. The paper also discusses both the benefits and limitations of integrating AI into IAM systems, including issues of data quality, model drift, and scalability. Additionally, the authors present a model that applies one-class classification with Gated Recurrent Units (GRUs) in autoencoders to learn normal user behavior and highlight deviations. The proposed behavioral analytics platform combines statistical anomaly detection with deep learning to achieve higher accuracy in identifying fraudulent access attempts. Results show that this hybrid system reduces false positives significantly while improving detection precision. The inclusion of explainable components provides administrators with interpretability, enhancing confidence in AI-driven IAM systems.[2]

C. Cloud and AI based Approach For Real Time Digital Banking Fraud Prevention

This study presents a detailed approach to real-time fraud prevention in digital banking using advanced technologies like machine learning and cloud computing. The increasing complexity of online transactions demands immediate detection and prevention of fraudulent activities to protect financial institutions and customers. Data collection and preprocessing are followed by feature-extraction methods such as dimensionality reduction to identify suspicious behavior. Machine-learning models like Support Vector Machines (SVM) and Naive Bayes (NB) are employed to classify transactions as fraudulent or genuine. The paper highlights how cloud

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

computing enables scalable and timely fraud detection, improving the safety and reliability of digital banking systems.[3]

D. AI Based Fraud Detection In Banking

This review analyzes over a hundred peer-reviewed publications on AI-driven banking fraud detection following the PRISMA methodology. It evaluates supervised, unsupervised, and hybrid techniques for identifying anomalies, transaction deviations, and identity theft. Supervised algorithms like Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), and XGBoost deliver high accuracy on known frauds, while unsupervised methods such as K-Means clustering, autoencoders, and isolation forests help identify emerging fraud patterns.

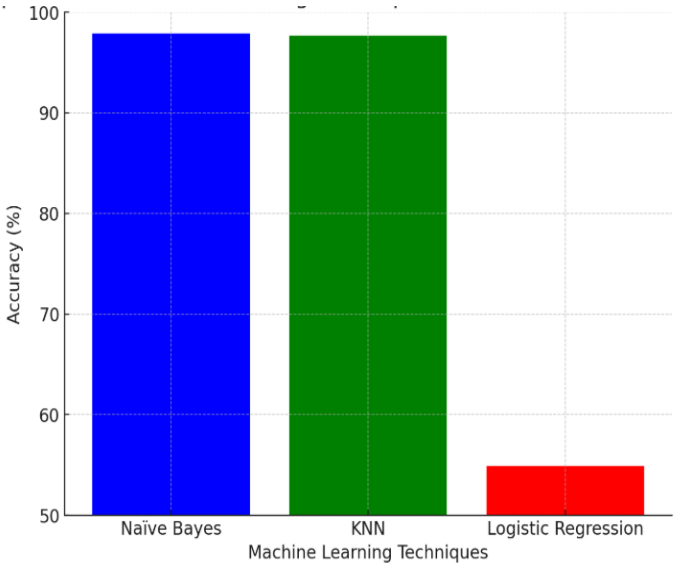

Fig. 1 : Machine Learning techniques accuracy

Figure 1 in the paper illustrates comparative accuracy across these machine-learning models, confirming that ensemble and deep architectures outperform standalone approaches. The authors note persistent challenges with imbalanced data, evolving fraud schemes, and privacy preservation. They advocate for adaptive AI models capable of self-learning from new data streams while maintaining interpretability. The combination of traditional supervised models with autoencoders demonstrated improved detection accuracy and reduced false positives in complex financial environments.[4]

E. ML Techniques For Credit Card Fraud Detection

This study evaluates the performance of Naive Bayes, K-Nearest Neighbors (KNN), and Logistic Regression for detecting credit card fraud on highly imbalanced datasets. Using 2,84,807 real transactions from European cardholders, the authors apply hybrid sampling techniques combining SMOTE and random undersampling to balance class distribution. The analysis shows that Naive Bayes achieves 97.9 % accuracy, followed closely by KNN at 97.7 %, whereas Logistic Regression lags at 54.8 %.

As shown in Figure 2, the conceptual framework emphasizes hybrid sampling and autoencoder-based anomaly detection. Autoencoders effectively capture general transaction behavior, allowing the model to flag unusual deviations that could indicate fraud. The authors conclude that combining classical algorithms with neural autoencoders significantly boosts system adaptability. They recommend further research into meta-classifiers and adaptive ensembles to handle evolving fraud trends.[5]

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

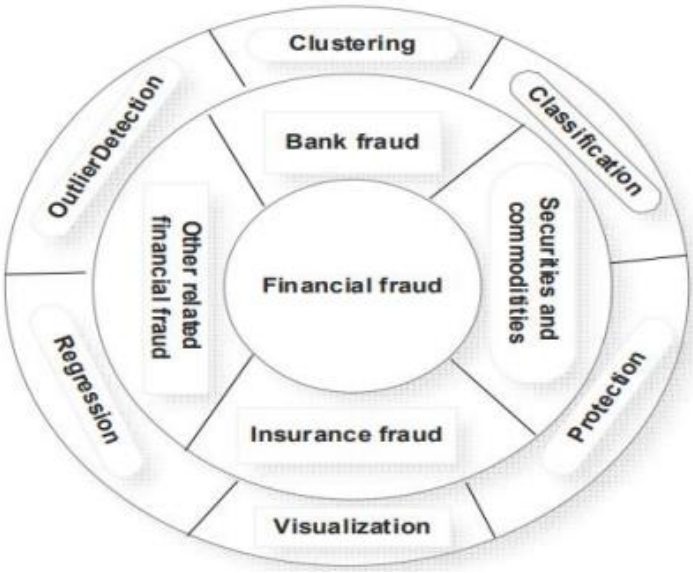

Fig. 2 : Conceptual Framework for Classification of Frauds.

F. Real-Time Data Processing and Model Deployment in Cloud-Based Fraud Detection Systems

With the exponential growth in transaction volume, there is an urgent requirement for scalable fraud detection frameworks. This work presents a cloud-based pipeline supporting data ingestion, preprocessing, model training, and live deployment. Preprocessed data are analyzed using algorithms such as Random Forest, SVM, and Neural Networks. The trained models are deployed as APIs for low-latency classification, enabling seamless integration with existing financial systems. Continuous monitoring and logging ensure anomaly detection with real-time alerts. Cloud platforms like AWS, Azure, and Google Cloud offer automatic resource scaling and fault tolerance. Table I in the paper compares the accuracy, precision, recall, and F1-scores of multiple models, highlighting that neural networks achieved the best overall performance with 99.4 % accuracy, followed closely by XGBoost at 99.3 %. The study concludes that distributed cloud architectures guarantee high availability, reliability, and adaptability for modern fraud detection pipelines. [6]

G. Explainable AI (XAI) In Fraud Detection: Enhancing Transparency And Trust

As fraud detection models become more sophisticated, their decision-making processes often appear opaque to analysts. This study integrates Explainable AI (XAI) methods—such as SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations)—into AI-based fraud detection systems. These frameworks clarify why a transaction is flagged as fraudulent by quantifying feature importance and generating local explanations for individual predictions.The results demonstrate that integrating XAI significantly improves transparency and regulatory compliance with frameworks such as GDPR and CCPA. Analysts can interpret model outputs with greater confidence, reducing false-positive rates and enabling actionable insights. The authors also emphasize the potential of XAI in auditing and governance, helping institutions build more trustworthy AI systems. By merging interpretability with accuracy, XAI strengthens user confidence and regulatory acceptance of AI-driven fraud detection tools.[7]

3. CHALLENGES

Despite the promising abilities of AI and cloud-primarily based structures for credit score card fraud detection, numerous substantial challenges remain of their realistic implementation. One

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

of the foremost worries is statistics privacy, as regulations along with the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) impose strict restrictions on the collection, processing, and storage of sensitive economic information. Ensuring complete compliance with these policies even as constructing actual-time fraud detection systems poses a complicated mission for builders and agencies alike. Another essential problem is the imbalance and excellence of records. Fraudulent transactions generally constitute a totally small portion of the general dataset, which results in class imbalance. This imbalance can bring about biased fashions that fail to accurately hit upon fraud. Additionally, poor records, together with lacking or inconsistent values, can further restrict model overall performance and reliability. The complexity of integration also affords an impediment. Incorporating AI-pushed answers into existing monetary IT infrastructures regularly calls for considerable architectural adjustments, together with useful resource-extensive efforts related to device compatibility, API deployment, and facts flow synchronization. This integration is especially tough in legacy systems that were not designed with present day AI skills in mind. Lastly, excessive technical expenses are a primary challenge, mainly when deploying advanced AI fashions including deep learning networks. These fashions demand widespread computational sources, along with effective processors, big memory capacities, and excessive-throughput information pipelines.

4. CONCEPTUAL SYSTEM ARCHITECTURE

This section presents a conceptual architecture for an AI-enabled credit card fraud detection system deployed on a cloud-based environment, consolidated from the methodologies reviewed in the literature. The system is designed to enable real-time transaction monitoring, data processing, and fraud detection leveraging the scalability and flexibility of cloud platforms.

4.1 Overview

The architecture integrates multiple functional components including data ingestion, preprocessing, feature engineering, AI-based model deployment, and real-time decision-making. Cloud services offer elastic compute resources, storage scalability, and on-demand model retraining to adapt to new fraud patterns.

4.2 Components of the Architecture

4.2.1 Data Ingestion Layer:

Transaction data is continuously collected from financial systems, payment gateways, and digital wallets via secured APIs and uploaded to a cloud-based storage system.

4.2.2 Data Preprocessing & Feature Engineering:

Incoming data is cleansed, normalized, and converted into suitable formats. Feature selection and engineering are performed to extract relevant transaction attributes like amount, location, transaction type, and customer profile.

4.2.3 Hybrid Sampling Techniques:

Given the class imbalance typically present in fraud detection datasets, hybrid techniques such as SMOTE (Synthetic Minority Oversampling Technique) combined with random under-sampling are applied to balance the dataset.

4.2.4 AI/ML Model Deployment:

Processed data is passed to multiple machine learning models (e.g., Random Forest, SVM, XGBoost, Neural Networks) deployed via cloud-based APIs. The models classify each transaction as fraudulent or legitimate based on learned patterns.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

4.2.5 Real-Time Detection and Alerts:

Predicted outcomes are monitored in real-time. If a transaction is flagged as suspicious, immediate alerts are generated for the financial institution's risk management team for further investigation.

4.2.6 Explainable AI (XAI) Module:

To improve interpretability and compliance, explainability frameworks like SHAP or LIME provide insights into why a transaction was classified as fraudulent, assisting analysts in decision-making and audits.

4.2.7 Feedback Loop and Model Retraining:

System performance is continuously monitored. Feedback from confirmed fraud investigations is used to update and retrain models periodically to adapt to evolving fraud patterns.

4.3. Conceptual Workflow Diagram

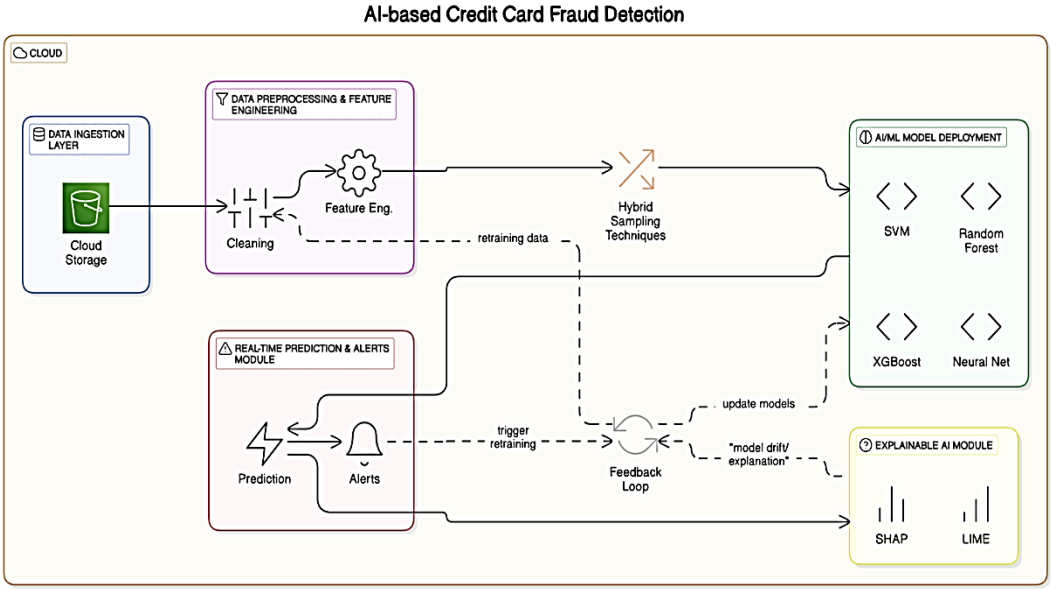

Fig. 3 : Typical Workflow of AI-Based Credit Card Fraud Detection in Cloud Environment

This architecture provides a consolidated view of how AI and cloud technologies can be synergistically combined to develop efficient, scalable, and transparent credit card fraud detection systems, as highlighted across multiple studies in the literature.

5. FUTURE DIRECTION

To further enhance the effectiveness and trustworthiness of AI-primarily based credit score card fraud detection systems, several promising directions can be pursued. One such advancement is the mixing of blockchain era, that may appreciably improve the security and transparency of transaction records. By leveraging blockchain's immutable ledger, it turns into lots extra difficult for malicious actors to govern or tamper with financial records, thereby strengthening fraud prevention mechanisms.Another important location is the adoption of federated learning, which lets in system studying fashions to be trained across decentralized gadgets without the need to switch touchy records to a valuable server. This approach now not simplest enhances statistics privacy but also enables collaborative version improvement using diverse data assets from more than one establishments.The implementation of AI-more desirable Multi-Factor Authentication (MFA) additionally

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

holds capability. By incorporating dynamic risk assessment and behavioral analysis, AI can intelligently adjust authentication necessities based on user pastime styles, making security structures more adaptive and strong towards fraud.

Additionally, the usage of predictive analytics can play a vital position in early fraud detection. By reading historic transaction statistics, AI models can perceive ability fraudulent behavior earlier than it happens, permitting financial institutions to take proactive measures and limit losses.Lastly, improving the user experience stays a key awareness. By leveraging advanced anomaly detection techniques, AI systems can lessen false positives, minimizing pointless transaction blocks and making sure a smoother revel in for legitimate users. At the same time, these systems can keep excessive requirements of fraud detection accuracy, making sure a stability between safety and convenience.

6. Comparative Analysis of Machine Learning Models for Fraud Detection

The following table describes the various performance metrics applied on machine learning algorithms and deep learning algorithms. It is clearly observed that the Neural Network shows the highest accuracy of all. Hence it can be used for this system while integrating real time processing of data. Second highest accuracy was achieved by XGboost, making it clear indication to consider XGboost while implementing such systems. Although, both have some pros and cons embedded while using them to develop an efficient system.

Table I. Comparative Analysis of Machine Learning Models for Fraud Detection

Model	Accuracy	Precision	Recall (TPR)	F1-Score
SVM	98.5	96.2	97.8	97.0
Random Forest	99.1	98.3	98.9	98.6
Neural Network	99.4	98.8	99.1	99.0
Logistic Regression	94.5	92.1	93.4	92.7
XGBoost	99.3	98.7	99.0	98.9

7. Conclusion

A competent credit card fraud detection system driven by Cloud Computing makes significant progress in the prevention of fraud, providing real-time monitoring, high accuracy and scalability. By integrating machine learning models such as SVM, Random Forest, XGBOOST and Neural Network with cloud infrastructure, the system ensures effective processing of data from large -scale transactions. Cloud's ability to scale dynamic resources allows for uninterrupted handling of spikes in the amount of transaction, making the system very effective in identifying real -time scam activities. The use of hybrid sampling techniques and switched models significantly reduces false positivity and improves general identity accuracy. With the performance of more than 99% accuracy in practical results, the system provides a strong solution for detecting fraud in the financial sector. In addition, cloud architecture ensures flexibility, cost certificate and easy distribution, making it suitable for large financial institutions and e-commerce platforms. Future promotion in the system will further strengthen its safety, accuracy and transparency. Integration of blockchain technology will increase data integrity by creating irreversible transactions, stopping data manipulation and enabling transparent revision. In addition, the use of contemporary AI (XAI) will improve

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

the interpretation of the system by providing clear justification for the fraud classification, promoting the confidence and helping the conformity of the regulator.

REFERENCES

[1] J. Sekar, "Optimizing Cloud Infrastructure for Real-Time Fraud Detection in Credit Card Transactions," Journal Name, vol. 6, pp. 381–388, 2023.
[2] V. Tamraparani, "Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on Large-Scale Customer Data," Journal of Computational Analysis and Applications, vol. 31, no. 4, 2023.
[3] J. Sekar, "Real-Time Fraud Prevention in Digital Banking: A Cloud and AI Perspective," Journal of Emerging Technologies and Innovative Research, vol. 10, pp. P562–P570, 2023.
[4] N. A. Faisal, J. Nahar, N. Sultana, and A. A. Mintoo, "Fraud Detection in Banking: Leveraging AI to Identify and Prevent Fraudulent Activities in Real-Time," Journal of Machine Learning, Data Engineering, and Data Science, vol. 1, no. 1, pp. 181–197, 2024.
[5] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis," in Proc. 2017 Int. Conf. on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, Oct. 2017, pp. 1–9.
[6] Y. Liu, S. Li, D. Wu, and Y. Jin, "Real-Time Credit Card Fraud Detection Using Machine Learning and Cloud Computing," IEEE Access, vol. 8, pp. 211682–211692, 2020.
[7] F. Carcillo, Y. A. Le Borgne, O. Caelen, G. Bontempi, and D. Jolly, "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," Information Sciences, vol. 557, pp. 317–331, 2021.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922