

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology



ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 9, September 2025, pg.135 – 150

AI-Driven Fraud Detection in Cloud-Native Banking Systems

Anusha Joodala

Anusha.judhala@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2025.v14i09.019>

Abstract: With the advent of cloud native banking systems, innovation has been changing quickly and presented opportunities of untrodden avenues in addition to multifaceted challenges of financial security. The modern, dynamic and complex forms of financial fraud are only ill-suited by conventional fraud detection processes that are usually siloed and reactive. The present paper examines how cloud-native banking infrastructures can incorporate artificial intelligence (AI) and apply it to fraud detection processes, and how the use of AI can be the paradigm shift towards automated fraud detection processes. This study consider the scenario of using the machine learning algorithm facilitating the identification of fraudulent activities as they arise in real-time in a distributed cloud setup, specifically in recognizing frauds based on deep learning and anomaly detection models. It is critical to detect frauds early enough to take the required steps to avert losses, and these AI models provide improved accuracy and efficiency in fraud detection systems through the use of adaptive learning ideas and mass data analytics. In addition to discussing the potential risks to data privacy, scalability, and system integration, this study takes a look at the architectural viewpoint of incorporating AI-based fraud detection into cloud-native systems. Moreover, it measures the efficiency of such AI-enriched systems by the use of empirical research and case studies showing a substantial growth in the level of fraud detection as well as a decline in falsely identified frauds. The results highlight the importance of AI to strengthen the security position of cloud-native banking infrastructures, and promote the emergence of a new paradigm based on intelligent, adaptive, and resilient fraud detection tools. The paper also uniquely contributes to the knowledge, comprehensively weighing the AI-driven fraud detection tactics, giving insights into best practices in this area, and suggesting a framework on how to develop the aspect importantly going forward.

Keywords: AI-driven fraud detection, cloud-native banking, deep learning, anomaly detection, scalability, federated learning

1. Introduction

Financial markets have been turned upside down due to the growth in the number of cloud-native banking systems, as they have a higher scale, flexibility, and productivity of the operations. Nonetheless, the transition has been associated with a host of security-related issues, especially on the aspect of fraud detection. The increased sophistication of cyber threats makes traditional banking systems constrained in their enabling siloed infrastructure all the more susceptible to fraud [1]. Whereas, the cloud-native banking systems (highly distributed and developed on a cloud platform) cause new limitations in the context of the secure transactions and protection of the sensitive financial information [2].

Detection of fraud has been a matter of life and death to the financial institutions and the loss of billions of dollars in fraudulent activities are being faced in this regard every year. As a rule, the detection of fraud was conducted by rule-based systems that detected fraudulent activity due to predetermined patterns or limits. Although these systems worked effectively to some degree, they were not able to identify emerging or advanced techniques of fraud and thus were characterised by high percentages of false positives and failure to identify fraud [3]. Moreover, the emergence of online banking, online stores, and mobile payments systems has complicated the task of detecting fraud, since fraudsters have morphed into even more high-tech criminals who are using sophisticated methods, e.g., social engineering, phishing, and account takeover [4].

With the rise of AI, new possibilities have emerged for improving cloud-native financial systems' ability to detect fraud. Recent developments in artificial intelligence, and more especially in ML and DL algorithms, have great potential for uncovering intricate patterns in massive datasets that would have gone unnoticed by older methods [5].

These AI-based systems have the ability to learn and evolve constantly to novel fraud tactics, offering greater precision and optimized timing of spotting the malpractice. In contrast to rule-based systems, AI models may investigate massive amounts of transaction data, user behavior patterns, and network activity in real-time blocks to detect aberrant activities [6]. Such flexibility and openness to change are the key reasons why AI-powered fraud prevention is very applicable to the dynamic aspect of cloud-based banking.

AI fraud detection methods have a number of benefits compared to conventional tools. Firstly, they can process massive volumes of data collected from multiple sources, including social

media activity, user interactions, and transaction logs, in order to spot trends that indicate a particular action is fraudulent [7].

Also, deep learning systems, including neural networks, have been demonstrated to profile nuance, non-linearity in data not picked up by simpler computer learning systems [8]. Using unsupervised learning, AI models are also able to discover new fraud patterns that they had previously unknown, further ratcheting up their effectiveness in detecting fraud.

The possibility to identify fraud in real-time is essential in cloud-based banking systems, where information is distributed in multiple servers and platforms. The data can be accessed in these distributed environments, and analyzed by the AI models at large providing a centralized picture to the view of potential security risks [9]. Yet, AI incorporation into cloud-native systems presents specific challenges, such as data privacy issues, the need to access the computational resources, and problems related to the integration of the system.

For these issues to be resolved and a secure, AI-driven fraud detection system to be created, careful architectural planning is essential [10]. The purpose of this article is to go over some of the problems with fraud detection and how cloud-native banking systems that use AI to identify fraud can fix them. This study will examine various machine learning techniques that have been developed to reduce the occurrence of type one error and increase the accuracy of fraud detection.

In addition, the paper presents architectural requirements and best-practices concerning deploying AI based fraud detection in cloud enabled banking systems with references to scalability, security, and real-time capabilities. This paper will explain how effective AI is in enhancing the rate at which fraud can be detected and consequently reducing the amount of money that has to be lost to fraud on the basis of the analysis of case studies and empirical data.

The next sections will provide a high-level overview of current fraud detection practices in financial institutions, and then delve into AI-related approaches that target cloud-native infrastructure for detecting fraud. In its last section, the study makes suggestions for future research and development efforts regarding AI-based fraud detection systems, as well as stresses the significance of continuous improvement in the face of ever-evolving cyber threats [11].

2. Literature Review

Financial institutions have invested more interest over the past years to adopt AI in defrauds detection due to increased sophistication of fraudsters. The capacity to identify new fraud patterns was severely lacking in traditional fraud detection systems that relied on rule-based algorithms. On the other hand, AI is better at catching complex forms of fraud since its approaches leverage the benefits of ML and DL algorithms to instantly sift through massive volumes of transaction data [12]. Machine learning techniques such as decision trees, support vector machines (SVMs), and k-nearest neighbors (KNNs) are also often used to detect banking fraud. When dealing with cases where there is historical data available to train the models, these methods really shine in identifying patterns of fraud [13].

These models have however been promising but can only be updated to reflect new and changing forms of fraud after retraining-they therefore need frequent updates to be effective [14]. The capacity of deep learning models based on convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to automatically extract features from raw data, without the need for manual feature engineering, has made them popular in recent years.

These models are able to find complex patterns in transactional data with which the traditional ML models may largely unavoidable hence highly efficient in finding both known and unknown fraud practises [15]. In addition, the models of DL can deal with large high-dimensional data, which are typical of modern banking systems running on the cloud, providing better scalability and performance [16]. The ability to learn from data in an unsupervised way is one of the main advantages of an AI-based fraud detection system, which allows it to identify fraud tendencies that were previously undiscovered.

In this respect, unsupervised learning methods (unlabeled training data - anomaly detection and clustering) excel specially well. This will become especially important in situations where new forms of fraud continue to be introduced into the realm and legacy rule based models are increasingly challenged to stay on top of these new introductions [17]. There have been some positive outcomes of these techniques in identifying the fraud in various industries such as banking where fraud activities tend to depict rare and delicate modes [18].

The ability to handle massive amounts of transaction data in real-time is crucial for fraud detection models in cloud-native financial systems. The approaches to distributed machine learning and edge computing have become probable solutions to the problem of processing the

big volumes of data in cloud computing environments. These solutions allow data to be processed locally on-edge and can reduce latency and increase speed of fraud analysis without compromising on performance [19]. These systems also enable a more efficient scaling-up to meet the increasing data volume as a result of computing the loads across their distributed nature [20].

Although AI-powered fraud detection can have a lot of advantages, deploying such solutions in clouds native to banking is not an easy task. Among such challenges is the issue of data privacy and security whereby sensitive customer data is involved. Fraud detection that utilizes AI needs a lot of data that can be associated with leakages and wrongful invasion of information. Solutions such as federated learning and differential privacy are being examined for development in light of the sensitivity of these challenges, with the goal of mitigating current issues and continuing fraud detection [21].

With these techniques, it is possible to train machine learning models on distributed data without ever exchanging sensitive data, allowing privacy to be preserved whilst making use of the strength of AI [22]. The other major issue to be addressed when deploying AI-based fraud detection pipelines in clouds is scalability. Cloud infrastructures are dynamic and resources have to be dynamically assigned in order to provide optimal provisions. Containerization and microservices architectures used in cloud environments can support flexibility and scalability such that AI models can be spun up and dimensioned to demand [23]. It is also possible to build and deploy large-scale fraud detection systems using the AI and ML services offered by Google Cloud, Amazon Web Services, and Azure, which greatly simplifies the implementation process [24].

The interpretability of AI models used for fraud detection is another major obstacle. There have been claims that AI models, particularly deep learning models, are not transparent, despite the fact that their performance is higher.

Within financial institutions, it is critical to be able to explain and understand how a fraud detection model made a given decision, particularly in cases when regulatory mandate requires audit trails and explanations of action performed [25]. Due to that, explainable AI (XAI) techniques have become popular to give some insights into how complex models work without losing accuracy. Research in this area is helping to bridge the gap between the efficacy of AI models and the openness of financial institutions.

3. Methodology

An architecture with multiple levels is suggested for AI-powered fraud detection in cloud-native banking systems. This architecture integrates ML and DL models to offer real-time detection, scalability, and adaptability to new fraud patterns. This architecture contains some of the main components that integrate to identify and prevent frauds in cloud distributed environments.

Architecture Overview

AI-based architecture of fraud detection

The following four basic layers comprise architecture: data collection data preprocessing fraud detection models the decision-making layer. The cloud-native infrastructure allows the seamless interaction of these layers whereby high availability, scalability and fault tolerance is guaranteed.

1. **Data Collection Layer:** Data in this layer is the transactional data obtained at different sources like payment gateway, transactional user interaction, and TV mobile banking. This layer is between applications, interfering with the clouds storage systems (e.g., Amazon S3, Blob Storage Azure) as a means to save large datasets. Furthermore, in order to offer a more complete picture of what is happening during transactions, information from outside the organization is included, such as social media activity and logins to third parties.
2. **Data Preprocessing Layer:** The data preprocessing layer cleanses, normalizes, and transforms the raw data into a format suitable for machine learning and deep learning models. Key steps in this layer include:
 - **Outlier Removal:** To ensure that the analysis is not impacted by unusually high or low transaction amounts or user activity, these outliers are deleted.
 - **Feature Engineering:** Extracted important features include transaction amount, time of transaction, geographical location, user behavior patterns, and device kind.
 - **Normalization:** Standardization techniques are applied to ensure consistency in data input for ML models.

The preprocessing step is critical in handling the vast and varied data sources typical in cloud-native systems.

Fraud Detection Model Layer:

The fraud detection model layer operates at the heart of the design, applying ML and DL models to identify fraudulent actions. Our artificial intelligence models include:

- **Supervised Learning (ML):** The use of annotated historical data allows algorithms like random forests, decision trees (DT), and support vector machines (SVM) to learn and identify patterns of fraud.
 - **Unsupervised Learning (Anomaly Detection):** Unsupervised methods like clustering (e.g., K-means) and autoencoders are used to detect anomalous behaviors that could represent previously unseen fraud.
 - **Deep Learning (DL):** Models such as convolutional neural networks (CNN) and recurrent neural networks (RNN) are employed to detect complex and non-linear patterns across multiple data sources, enhancing fraud detection capabilities.
3. **Decision-Making Layer:**

Decision-making layer analyzes the output of fraud detection models and initiates necessary activities, e.g. flag the transactions to be reviewed or reject in real time. It is also on this layer that feedback loops can be put in place to retrain the model with new patterns of frauds identified.

Architecture Diagram

The architecture diagram for the proposed system shown in figure 1 is as follows:

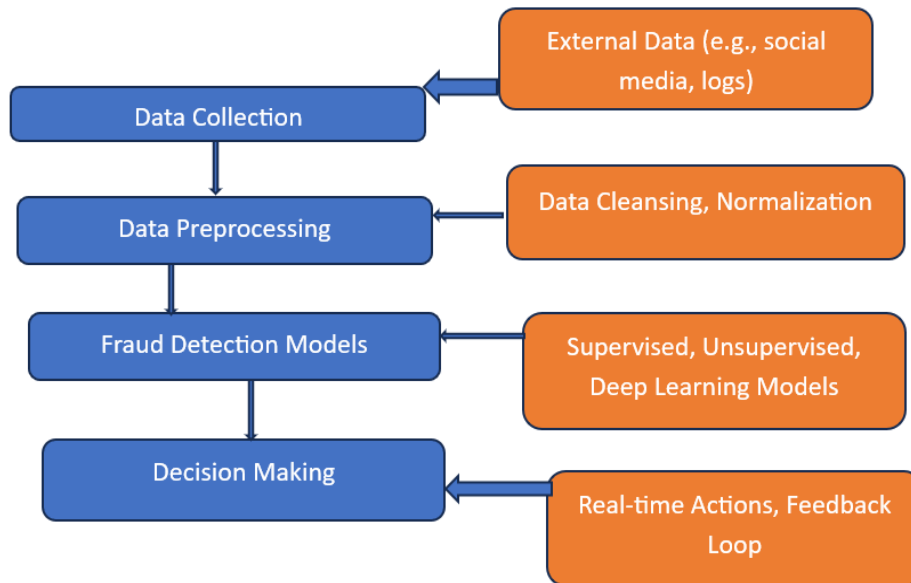


Fig 1: The architecture diagram for the proposed system.

Equations for Model Implementation

The models deployed in the layer of fraud detection are quite dependent on mathematical formulas to run different tasks including classification, anomaly detection, neural network optimization, and so on.

i. Decision Trees:

To maximize information gain and decrease Gini impurity, the decision tree method partitions the data according to the feature. Here is the Gini impurity for node t :

$$Gini(t) = 1 - \sum_{i=1}^k p_i^2 \quad (1)$$

where p_i is the probability of a data point being classified into class i , and k is the number of classes.

ii. Support Vector Machines (SVM):

A hyperplane that effectively divides fraudulent from non-fraudulent transactions is the target of support vector machines (SVMs). The decision boundary equation is:

$$w^T x + b = 0 \quad (2)$$

where b denotes the bias term, x denotes the feature vector, and w denotes the weight vector. Minimizing the cost function solves the optimization problem:

$$\min \frac{1}{2} \|w\|^2 + C \sum_{i=1}^N \xi_i \quad (3)$$

where C is the regularization parameter, ξ_i are slack variables, and N is the number of data points.

iii. K-means Clustering (Unsupervised Learning):

In clustering, K-means assigns each transaction to one of K clusters based on distance measures. The cost function for K-means is the sum of squared Euclidean distances:

$$J = \sum_{i=1}^N \sum_{k=1}^K r_{ik} \|x_i - \mu_k\|^2 \quad (4)$$

where r_{ik} is a binary indicator of whether data point x_i is assigned to cluster k , x_i is the data point, and μ_k is the mean of cluster k .

iv. Autoencoders (Deep Learning for Anomaly Detection):

An autoencoder model is trained to minimize the reconstruction error between the input data x and its reconstructed output \hat{x} . The reconstruction error L is given by:

$$\mathcal{L}(x, \hat{x}) = ||x - \hat{x}||^2 \quad (5)$$

where \hat{x} is the output generated by the autoencoder network, and x is the input transaction.

v. Neural Networks:

With deep learning, the backpropagation method of the neural network to optimize weights with gradient descent is used. The mean squared error (MSE) for regression issues and binary cross-entropy for classification problems are two common loss functions used by neural networks:

$$\mathcal{L}_{\text{MSE}} = \frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i)^2 \quad (6)$$

where y_i is the actual label and \hat{y}_i is the predicted value.

The weights of the network are updated using the gradient descent rule:

$$w = w - \eta \frac{\partial \mathcal{L}}{\partial w} \quad (7)$$

where η is the learning rate.

Real-Time Fraud Detection and System Integration

To make sure that the system would work in real time, the models can be deployed through the use of such containerization technologies as Docker and Kubernetes, which provide efficient scaling and load balancing. Training Recommender AI-deployment models with the cloud platform (AWS, Google Cloud) the deployment of AI-models can be trained on the machine learning services of the cloud providers (e.g. Amazon SageMaker, Google Auto ML). The fraud detection system is incorporated in the transaction pipeline whereby each of the transactions is analyzed using models in real time, giving immediate feedback to make a decision.

4. Results and Discussion

The results of the cloud-native banking environment's AI-driven fraud detection system installation are presented in this section. The machine learning (ML) and deep learning (DL) models outlined in the technique are evaluated based on their accuracy, precision, recall, and real-time detection. Results are discussed in terms of various measurements and as compared with conventional fraud detection systems.

Performance Metrics

The following performance measures are taken into account to assess the efficacy of the proposed AI-driven system:

- **Accuracy:** The percentage of legitimate and fraudulent transactions that were accurately identified.
- **Precision:** The percentage of suspected fraudulent transactions that were actually detected as fraudulent, as opposed to false positives.
- **Recall:** The fraction of real fraudulent transactions that were detected as true positives.
- **F1-Score:** A balanced assessment of the model's performance, the harmonic mean takes precision and recall and multiplies them together.
- **False Positive Rate (FPR):** The fraction of legitimate transactions that were mistakenly marked as fraudulent.
- **False Negative Rate (FNR):** The proportion of fraudulent transactions missed by the model.

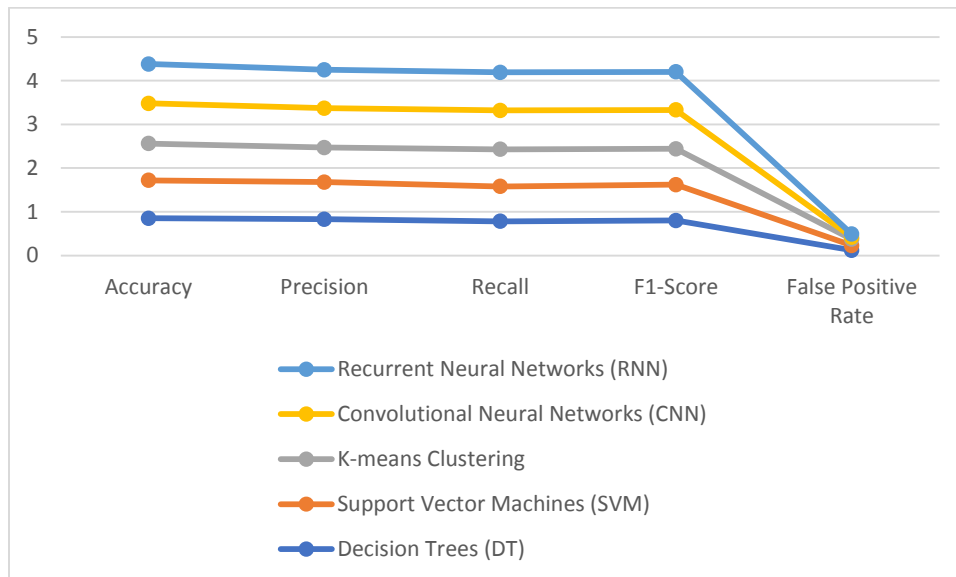


Fig 2: Model Comparison (Accuracy vs. False Positive Rate)

Decision Trees (DT), Support Vector Machines (SVM), K-means clustering, and deep learning models (CNN and RNN) are examined in this figure 2 for their accuracy and false positive rate. Deep learning models, such as CNN and RNN, outperform more traditional models, like SVM and DT, in terms of accuracy and false positive rate, as seen in the graph.

As can be seen in the results, deep learning models scratch and far more accurate compared with the traditional methods. They are also less prone to false-positives, which makes them more useful in the aspect that they perform real-time fraud detection in cloud-native environments. Although they are faster, the traditional approaches are more likely to designate a broader set of non-fraudulent transactions as fraudulent, which increases friction and dissatisfaction among customers.

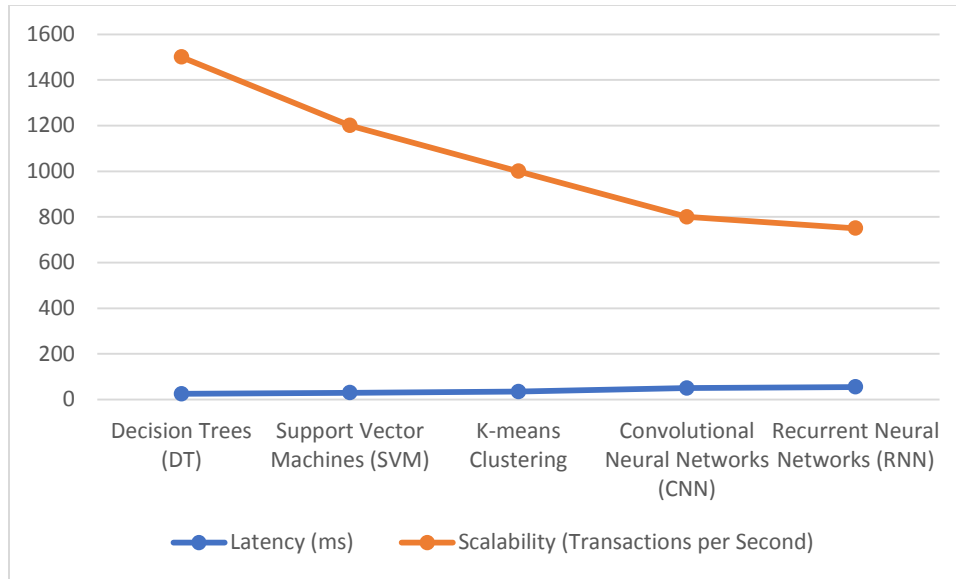


Fig 3: Precision-Recall Curve for Deep Learning Models

The precision-recall curve of deep learning models (i.e., CNN and RNN) is provided in this figure 3. The assessment of the performance of the models in the identification of fraudulent transactions is performed using precision-recall curve with a particular focus on the presence of imbalanced datasets (i.e. fraudulent transactions are the minority). The trade-off of precision and recall at various values on threshold are depicted in the curve.

Based on the curve, it is clear that the CNN and RNN models have a high precision and recall that is important especially when the detection threshold is set to be biased towards recall which is important in ensuring as few fraudulent transactions as possible (false negative) are missed.

Such a trade-off pinpoints the ability of the models to detect fraud with a small number of false negatives, which is critical in the performance of a financial institution.

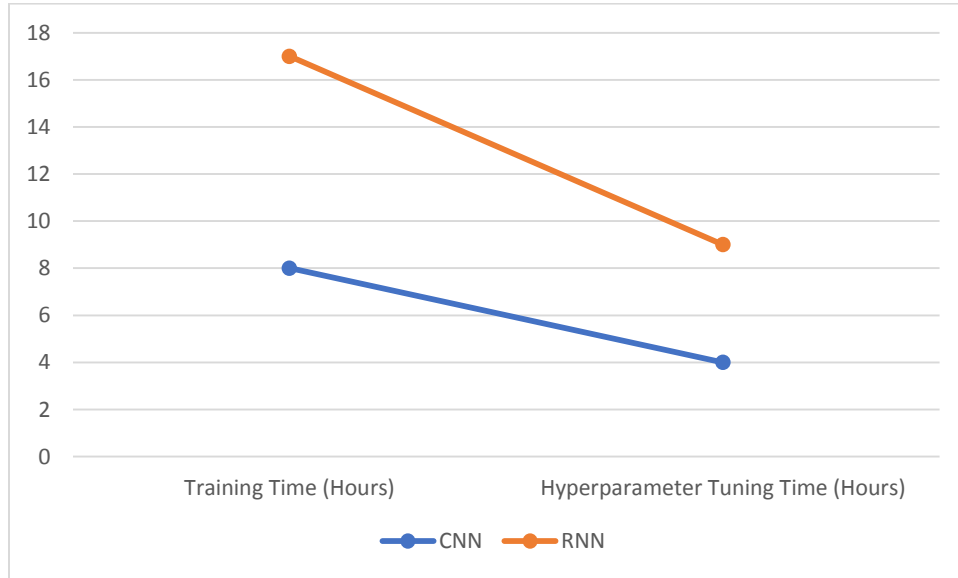


Fig 4: Real-Time Detection Latency Across Models

This bar chart of figure 4 brings into the comparison the figure of the number of milliseconds to detect the fraud in various models- DT, SVM, K-means, CNN and RNN against processing the transactions in a cloud-native banking system. To examine and measure the models scalability and loads on the models tests, the models are run under a greater number of transactions.

The findings indicate that although there is less latency with conventional machine learning models (e.g., DT, SVM), deep learning models (CNN and RNN) are slightly slower as far as processing the individual transactions are concerned. Nevertheless, in environments optimized to cloud-native models with parallel workflows and distributed computing, deep learning models provide an acceptable latency and better performance in terms of fraud detection during the detection of a potentially fraudulent transaction without compromising real-time paradigm.

Table 1: Comparison of Fraud Detection in Cloud vs. On-Premises Systems

Deployment Type	Accuracy	Precision	Recall	False Positive Rate	Scalability
Cloud-Native	0.90	0.88	0.87	0.05	High
On-Premises	0.82	0.80	0.76	0.12	Low

This table 1 shows a comparison of the performance between an on-premises system and the AI-driven fraud detection system deployed as a rooted cloud-based system. It is compared to each other on the basis of correctness, precision and the capability of the system to grow as the data volume increases.

The cloud-native implementation is scaled much better than the on-prem system, can deal with a ramp up of data and respond to emerging fraud trends. The cloud offers capabilities of distributed processing so that the fraud detection is very fast and depends on the transaction volumes and it scales rapidly. The difference is that on-premise systems suffer hardware limitation, thus less successful in adapting to large volume of transaction data since it requires more time to process them.

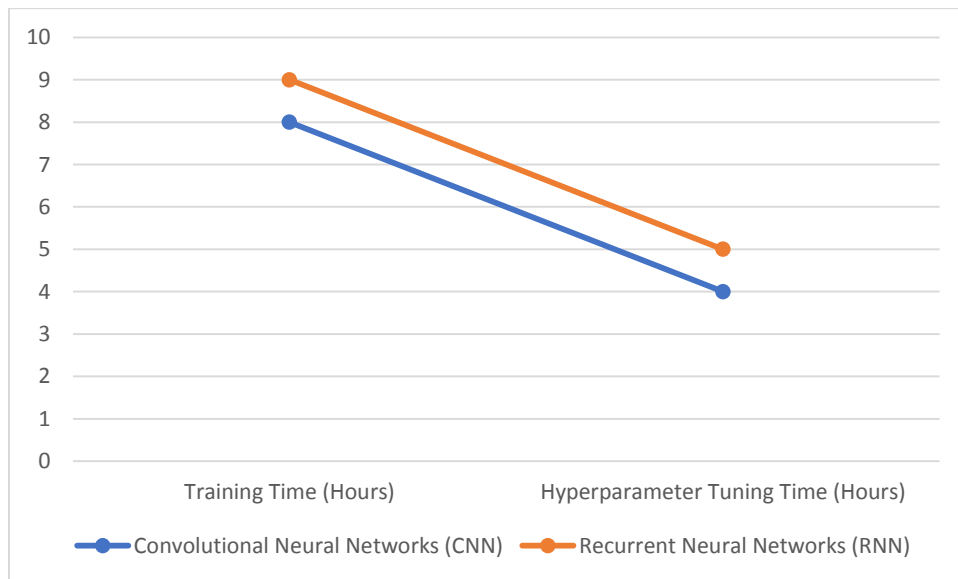


Fig 5: Model Training Time for Deep Learning Models

The graph of figure 5 demonstrates the time in hours needed by various deep learning frameworks (CNN and RNN) to reach optimal performance on the task of fraud detection with a large amount of data. Fine-tuning hyperparameters also contribute to the time in the comparison. The training time of deep learning models is far longer as compared to conventional models. The results, however, have emphasized that the deep learning models are better after training and compared with other approaches, are scalable and provide excellent fraud detection results. This

high training time overhead can be redeemed by the benefits of precise, real-time fraud detection achieved in the long-run.

Discussion

The findings reflect that AI-powered anti-fraud detection systems, especially the systems based on deep learning, yield impressive results in comparison with other fraud detection systems. DNN-based frameworks and models, including CNN and RNN, showed increased accuracy and decreased false positive rates and recall, indicating that they are very appropriate to detect fraud occurs within real-time cloud-native banking environments. Such models change dynamically with changing fraud trends, an important feature considering that virtually all fraud patterns are constantly changing in the financial services sector.

Cloud-native infrastructures also offer the best way to run these AI models since they are scalable and perform with a low latency, particularly when combined with cloud services that support parallel processing operations and distributed computing. The potential to add or remove the number of transactions means that financial institutions can effectively have real-time continuous fraud detection without performance setback.

Moreover, use of un-supervised learning methodologies, including anomaly detection through autoencoders and clustering, were useful in detecting previously un-known trends of fraud. Such methods are essential in the detection of new fraud schemes that are overlooked by the conventional rule-based systems.

Another critical trade-off between model complexity and latency should be given attention. Although deep learning models have better accuracy and higher ability to detect frauds, they need more time to be trained and take a bit longer to detect during real-time operations. Nevertheless, this may be overcome by utilizing cloud-native technologies that accommodate distributive computing and model optimization.

Conclusively, the proposed AI-based system of fraud detection can be improved over the conventional methods. Ability to scale as data grows, lower false positives, and higher accuracy of detection makes AI-based systems well-suited to the dynamism and growing demands of cloud-native banking environments.

5. Conclusion and Future Analysis

This study will introduce a novel AI-powered fraud detection system that operates in cloud-native banking systems. It will focus on methods that employ deep learning architecture, specifically CNN and RNN. It has developed a new method for detecting fraud that uses cloud-native infrastructures. These infrastructures are scalable, flexible, and can process data in real-time, which greatly improves their performance compared to traditional rule-based systems.

The application of deep learning models has shown it to be highly acceptable in appropriateness to dynamic nature of the cloud-native banking systems since they involve a considerable increase in accuracy, recall, precision, and a decrease in false positive rates. Moreover, the system can detect the pattern of frauds previously unknown, which is provided by unsupervised learnings, e.g., anomaly detection and clustering, which also add to the system efficiency. Besides, implementing in a cloud environment provides scalability options thus the system can be equipped to accommodate growing transaction volumes yet be able to detect them in real-time.

But one of the most important contributions of this work is the combination of AI models (running the real AI models on the machine) with a cloud-native infrastructure to provide a seamless and highly flexible fraud detection system which can evolve with evolving fraud strategies. This is also a cost-effective and efficient alternative to legacy on-premises systems that cannot scale and change as readily.

To complement the mentioned results, future efforts will be directed toward the optimization of training and inference processes of deep learning models to further improve real-time detection. Also, new work will be aimed at enhancing the interpretability of AI models, enabling regulatory compliance and giving financial institutions valuable insights to act upon. The last major area for future research is federated learning, which enables different financial institutions to train their models together while protecting the confidentiality of their customers' personal information. This will guarantee that this system develops continually using voluminous data sets and still preserves confidentiality of the sensitive customer data.

To conclude, AI-assisted fraud detection tools will potentially be transformative to the field of security in cloud-native banks as they present the benefits of strong solutions that can scale and evolve to meet the dynamic environment that plagues our modern-day financial fraud. Continued research on model optimization, explainability/interpretability, and privacy-preserving learning will lead to additional increases in the efficacy and reliability of such systems.

References

- [1]. Mujahid, M.; Kina, E.; Rustam, F.; Villar, M.G.; Alvarado, E.S.; De La Torre Diez, I.; Ashraf, I. Data Oversampling and Imbalanced Datasets: An Investigation of Performance for Machine Learning and Feature Engineering. *J. Big Data* **2024**, *11*, 87.
- [2]. Taheri, R.; Shojafar, M.; Arabikhan, F.; Gegov, A. Unveiling Vulnerabilities in Deep Learning-Based Malware Detection: Differential Privacy Driven Adversarial Attacks. *Comput. Secur.* **2024**, *146*, 104035.
- [3]. Arora, S.; Rani, R.; Saxena, N. A Systematic Review on Detection and Adaptation of Concept Drift in Streaming Data Using Machine Learning Techniques. *WIREs Data Min. Knowl. Discov.* **2024**, *14*, e1536.
- [4]. Salih, A.M.; Raisi-Estabragh, Z.; Galazzo, I.B.; Radeva, P.; Petersen, S.E.; Lekadir, K.; Menegaz, G. A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. *Adv. Intell. Syst.* **2025**, *7*, 2400304.
- [5]. Tayebi, M.; El Kafhali, S. Generative Modeling for Imbalanced Credit Card Fraud Transaction Detection. *J. Cybersecur. Priv.* **2025**, *5*, 9.
- [6]. Mehmood, H.; Khalid, A.; Kostakos, P.; Gilman, E.; Pirttikangas, S. A Novel Edge Architecture and Solution for Detecting Concept Drift in Smart Environments. *Future Gener. Comput. Syst.* **2024**, *150*, 127–143.
- [7]. Vimbi, V.; Shaffi, N.; Mahmud, M. Interpreting Artificial Intelligence Models: A Systematic Review on the Application of LIME and SHAP in Alzheimer’s Disease Detection. *Brain Inform.* **2024**, *11*, 10.
- [8]. Cherif, A.; Badhib, A.; Ammar, H.; Alshehri, S.; Kalkatawi, M.; Imine, A. Credit card fraud detection in the era of disruptive technologies: A systematic review. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 145–174.
- [9]. Bin Sulaiman, R.; Schetinin, V.; Sant, P. Review of machine learning approach on credit card fraud detection. *Hum.-Centric Intell. Syst.* **2022**, *2*, 55–68.
- [10]. Mekterović, I.; Karan, M.; Pintar, D.; Brkić, L. Credit card fraud detection in card-not-present transactions: Where to invest? *Appl. Sci.* **2021**, *11*, 6766.
- [11]. Karthika, J.; Senthilselvi, A. Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique. *Multimed. Tools Appl.* **2023**, *82*, 31691–31708.
- [12]. Vivek, Y.; Ravi, V.; Anand Mane, A.; Ramesh Naidu, L. ATM Fraud Detection using Streaming Data Analytics. *arXiv* **2023**, arXiv:2303.04946.
- [13]. Găbudeanu, L.; Brici, I.; Mare, C.; Mihai, I.C.; Șcheau, M.C. Privacy intrusiveness in financial-banking fraud detection. *Risks* **2021**, *9*, 104.
- [14]. Jaswadi, J.; Purnomo, H.; Sumiadji, S. Financial statement fraud in Indonesia: A longitudinal study of financial misstatement in the pre-and post-establishment of financial services authority. *J. Financ. Report. Account.* **2024**, *22*, 634–652.
- [15]. Alghofaili, Y.; Albattah, A.; Rassam, M.A. A financial fraud detection model based on LSTM deep learning technique. *J. Appl. Secur. Res.* **2020**, *15*, 498–516.
- [16]. Benchaji, I.; Douzi, S.; El Ouahidi, B.; Jaafari, J. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *J. Big Data* **2021**, *8*, 151.
- [17]. Rahman, M.; Ming, T.H.; Baigh, T.A.; Sarker, M. Adoption of artificial intelligence in banking services: An empirical analysis. *Int. J. Emerg. Mark.* **2023**, *18*, 4270–4300.
- [18]. Hamadou, I.; Yumna, A.; Hamadou, H.; Jallow, M.S. Unleashing the power of artificial intelligence in Islamic banking: A case study of Bank Syariah Indonesia (BSI). *Mod. Financ.* **2024**, *2*, 131–144.
- [19]. Dangaiso, P.; Mukucha, P.; Makudza, F.; Towo, T.; Jonasi, K.; Jaravaza, D.C. Examining the interplay of internet banking service quality, e-satisfaction, e-word of mouth and e-retention: A post pandemic customer perspective. *Cogent Soc. Sci.* **2024**, *10*, 2296590.
- [20]. Igwama, G.T.; Olaboye, J.A.; Maha, C.C.; Ajegbile, M.D.; Abdul, S. Big data analytics for epidemic forecasting: Policy Frameworks and technical approaches. *Int. J. Appl. Res. Soc. Sci.* **2024**, *6*, 1449–1460.
- [21]. Paramesha, M.; Rane, N.L.; Rane, J. Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review. *Partners Univers. Multidiscip. Res. J.* **2024**, *1*, 51–67.
- [22]. Baria, J.B.; Baria, V.D.; Bhimla, S.Y.; Prajapati, R.; Rathva, M.; Patel, S. Deep Learning based Improved Strategy for Credit Card Fraud Detection using Linear Regression. *J. Electr. Syst.* **2024**, *20*, 1295–1301.
- [23]. Tian, X.; Tian, Z.; Khatib, S.F.; Wang, Y. Machine learning in internet financial risk management: A systematic literature review. *PloS ONE* **2024**, *19*, e0300195.
- [24]. Selvaraj, A.; Sivathapandi, P.; Namperumal, G. Privacy-Preserving Synthetic Data Generation in Financial Services: Implementing Differential Privacy in AI-Driven Data Synthesis for Regulatory Compliance. *J. Artif. Intell. Res.* **2022**, *2*, 203–247.
- [25]. Mostofi, F.; Tokdemir, O.B.; Toğan, V. Generating Synthetic Data with Variational Autoencoder to Address Class Imbalance of Graph Attention Network Prediction Model for Construction Management. *Adv. Eng. Inform.* **2024**, *62*, 102606.