International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

AI-Driven Fraud Detection and Prevention Framework for Cloud-Based Banking Systems

[1*]Archana Chaluvadi, [2]Winner Pulakhandam, [3]Visrutatma Rao Vallu and [4]R. Hemnath

[1]Massachusetts Mutual Life Insurance Company, Massachusetts, USA
[2]Personify Inc, Texas, USA
[3]Spectrosys, Woburn, Massachusetts, USA
[4]Kaamadhenu Arts and Science College, Sathyamangalam, India

Received 12 July 2022, Accepted 10 Aug 2022, Available online 12 Aug 2022, **Vol.10 (July/Aug 2022 issue)**

Abstract

Fraud detection in cloud-based banking systems has become increasingly critical as financial transactions continue to move online, leading to sophisticated fraudulent activities. Existing methods face challenges such as limited adaptability to new fraud patterns, imbalanced datasets, and scalability issues, which hinder fraud detection and efficient processing of large transaction volumes. This paper presents an AI-driven fraud detection system designed to overcome these challenges by leveraging deep learning techniques and cloud-based infrastructure. The system begins with the collection of transaction data, user behavior logs, and account details, followed by data preprocessing using Min-Max scaling for numerical data and one-hot encoding for categorical variables. Next, feature extraction using Continuous Wavelet Transform (CWT) is applied to the pre-processed data, capturing temporal and frequency patterns. These features are used to train a Variational Autoencoder (VAE) model to detect anomalies. The trained model is deployed to a cloud-based platform, ensuring scalability and fraud detection. Experimental results show that the system achieves an accuracy of 99.51%, precision of 98.92%, sensitivity of 98.77%, specificity of 99.12%, F-measure of 98.96%, and throughput of 800 transactions per second. This work provides the enhancement of fraud detection systems by integrating advanced AI techniques and cloud infrastructure, offering a robust, scalable, and efficient solution for large-scale banking environments.

Keywords: *Fraud Detection, Banking Systems, Cloud Computing, Deep Learning, Variational Autoencoder and Continuous Wavelet Transform.*

Introduction

The banking industry has undergone a profound transformation driven by rapid technological advancements, with cloud computing and artificial intelligence (AI) emerging as key enablers for enhancing operational efficiency, security, and customer experience [1]. Cloud computing provides banks with a flexible and scalable infrastructure capable of managing vast volumes of transactional data, supporting digital services, and facilitating seamless integration across multiple platforms [2]. Meanwhile, AI technologies, particularly those based on machine learning and deep learning, have been increasingly adopted to automate complex decision-making processes and improve service personalization [3]. These innovations collectively contribute to the modernization of banking operations, enabling institutions to respond more effectively to market demands and evolving regulatory requirements [4].

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr.v.10.4.10

Despite these advancements, financial institutions continue to face significant challenges from increasingly sophisticated fraudulent activities [5]. Fraudsters have evolved their tactics, exploiting loopholes and leveraging advanced techniques to bypass traditional security measures [6]. Legacy fraud detection systems, often reliant on static, rule-based mechanisms or manual oversight, struggle to keep pace with the dynamic nature and sheer volume of modern financial transactions [7]. These conventional approaches are typically limited by their inability to detect novel fraud patterns or adapt quickly to new threats, resulting in increased financial losses and reputational damage [8]. As a consequence, there is a pressing need for more robust, adaptive, and intelligent fraud detection frameworks that can operate effectively at scale [9].

Cloud-based banking systems have emerged as a promising solution to address these challenges by providing a resilient infrastructure capable of handling

real-time data processing and analytics [10]. The scalability of cloud platforms allows for the continuous ingestion and analysis of transactional data streams, facilitating timely detection and response to suspicious activities [11]. AI-driven fraud detection models can leverage this infrastructure to analyze complex transactional patterns, identify anomalies, and flag potentially fraudulent behavior with greater accuracy [12]. These models can be continuously updated and trained on diverse datasets to improve detection performance and reduce false alarms [13]. By integrating cloud computing with AI, banks can deploy more agile and effective security mechanisms that strengthen overall risk management and compliance [14].

Various fraud detection techniques have been explored and implemented, each bringing distinct advantages and limitations [15]. Traditional rule-based systems, often encapsulated in expert systems, rely on predefined fraud scenarios and heuristics, which makes them transparent but less effective against evolving fraud tactics [16]. Machine learning algorithms, such as decision trees, support vector machines (SVM), and random forests, offer improved adaptability by learning from historical data [17]; however, they often face challenges including class imbalance—where legitimate transactions vastly outnumber fraudulent ones—and difficulty generalizing to previously unseen fraud types [18]. More recently, deep learning approaches, including convolutional neural networks (CNNs) and autoencoders, have shown promise in detecting subtle and complex fraud patterns, enhancing detection accuracy [19]. Nevertheless, these methods typically demand extensive labeled datasets and significant computational resources, and they may suffer from high false-positive rates, which can undermine operational efficiency [20]. Despite incremental improvements, existing fraud detection systems continue to fall short in effectively managing the scale and evolving nature of financial fraud, underscoring the need for innovative solutions that balance accuracy, scalability, and resource efficiency [21].

In addition to improving detection accuracy, there is a growing emphasis on developing fraud detection systems that are both scalable and adaptable to the rapid changes in transaction environments [22]. The surge in digital payment platforms, mobile banking, and online financial services has exponentially increased the volume and diversity of transaction data, presenting both opportunities and challenges for fraud management [23]. Systems must therefore be capable of processing vast streams of heterogeneous data in near-instantaneous timeframes to promptly identify suspicious behavior [24]. Furthermore, the heterogeneity of fraud types, ranging from identity theft and account takeover to synthetic fraud and money laundering, requires detection models that can generalize well across multiple fraud scenarios [25]. This necessitates the incorporation of continual learning and real-time model updates to maintain efficacy in dynamic financial landscapes [26].

Another critical factor is the reduction of false-positive rates, which directly impacts operational costs and customer satisfaction [27]. Excessive false alarms can burden fraud investigation teams and inconvenience legitimate customers through unnecessary transaction blocks or additional verification steps [28]. Thus, balancing sensitivity and specificity in fraud detection remains a key design challenge [29]. Advanced AI techniques that include ensemble learning, anomaly detection, and explainable AI (XAI) are being explored to not only improve detection precision but also provide interpretability of model decisions, aiding compliance and trustworthiness [30]. Explainability is especially important in regulated banking environments, where transparent and auditable decision processes are mandated by financial authorities [31].

The proposed framework addresses the drawbacks of existing systems by leveraging cloud-based AI techniques tailored for scalable and efficient fraud detection. By incorporating a robust preprocessing pipeline with advanced feature extraction methods and anomaly detection, the framework improves detection accuracy while minimizing false positives. The novelty of this study lies in its ability to adapt to evolving fraud patterns by utilizing a dynamic model training process. This approach not only enhances the security of cloud-based banking systems but also ensures the scalability of fraud detection mechanisms to handle large volumes of transactional data efficiently. The integration of these components provides a more resilient and responsive fraud prevention system.

The paper is organized as follows: Section 2 presents the literature survey, reviewing related work in fraud detection systems. Section 3 describes the methodology. Section 4 discusses the experimental results, presenting performance metrics and throughput. Finally, Section 5 concludes the paper and outlines future directions for improving the system.

2, Literature Survey

Recent years have witnessed significant progress in cloud-based image and data processing through the application of deep learning techniques, which have substantially enhanced the accuracy and efficiency of various tasks [32]. For instance, multi-scale convolutional feature fusion approaches have been successfully implemented for detecting clouds in remote sensing images, outperforming conventional image processing methods by capturing features at different resolutions [33]. Similarly, the fusion of deep learning features with 3D point cloud data has proven effective in post-disaster damage assessment by leveraging oblique aerial imagery, leading to more precise identification and analysis of affected areas [34]. Additionally, deep learning models such as random forests, long short-term memory networks (LSTMs), and U-Net architectures have been rigorously evaluated for satellite image analysis,

confirming their ability to handle large-scale, complex remote sensing data with improved performance and robustness [35].

In the field of cybersecurity and IoT, distributed deep learning models have been deployed on edge devices to enhance web attack detection, contributing to more stable and convenient management of cloud-based security systems [36]. Hierarchical computing architectures have also been proposed to boost the availability and accuracy of deep learning models used in IoT health monitoring platforms, enabling continuous patient monitoring and timely intervention [37]. Moreover, advances in 3D deep learning techniques, such as Point-Voxel CNNs, have addressed challenges related to memory consumption and computational cost, allowing for efficient processing of high-resolution spatial data [38]. CNN-based models designed specifically for meteorological applications have shown substantial improvements in cloud classification accuracy by utilizing newly created and comprehensive cloud datasets [39].

Real-time applications of deep learning have been extended to fraud detection, where autoencoder-based deep neural networks classify credit card transactions to detect fraudulent activities promptly and accurately [40]. Similarly, assistive technologies for visually impaired individuals have benefited from the integration of 3D computer vision and deep learning for obstacle detection, offering enhanced mobility and safety [41]. Privacy-preserving personalized text input methods have been introduced by training deep learning models directly on mobile devices, ensuring that sensitive user data remains on-device without compromising usability [42]. Intelligent medication recognition systems have also been developed by combining mobile device capabilities with cloud-based deep learning platforms, facilitating better medication management for chronic patients and improving healthcare outcomes [43].

Hybrid approaches combining rule-based systems with machine learning and deep learning techniques have gained traction as a way to enhance detection accuracy while maintaining interpretability [44]. Rule-based filters serve as the first line of defense by quickly flagging obvious fraud attempts, while subsequent AI models perform more nuanced analyses on suspicious transactions [45]. This layered strategy improves both the precision and recall of fraud detection systems [46]. Additionally, ensemble learning methods that integrate multiple machine learning classifiers have shown promise in mitigating issues such as data imbalance and overfitting [47]. These ensembles leverage the diversity of individual models to produce more robust and reliable fraud predictions, a critical factor in minimizing false positives in banking applications [48]. The emergence of explainable AI (XAI) has been particularly relevant in the financial domain, where regulatory compliance and auditability are paramount [49]. Researchers have developed techniques that provide transparency into the decision-making processes of complex AI models, enabling fraud analysts and compliance officers to understand and trust model outputs [50]. Methods such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) have been integrated into fraud detection pipelines to highlight key features influencing predictions [51]. This interpretability not only aids in regulatory adherence but also facilitates faster investigation and resolution of flagged transactions, enhancing operational efficiency in banking institutions [52].

Privacy preservation remains a significant concern when developing AI-driven fraud detection systems, especially given the sensitive nature of financial data [53]. Recent frameworks have incorporated privacy-preserving techniques such as federated learning, which enables collaborative model training across multiple institutions without sharing raw data [54]. Differential privacy mechanisms have also been employed to mask sensitive information in training datasets, balancing data utility with confidentiality [55]. These advancements allow banks to benefit from collective intelligence and improved fraud detection capabilities while ensuring compliance with data protection regulations such as GDPR and CCPA [56]. The integration of privacy-aware AI methods with scalable cloud architectures represents a promising direction for secure and effective fraud management [57]. Further advancements in 3D data processing involve the use of sparse voxel octree structures combined with 3D CNNs to segment and classify dental models, effectively addressing the misclassification issues that arise due to the high similarity between tooth types [58]. The application of deep learning within embedded systems has been explored to support real-time data analysis while minimizing power consumption, which is essential for IoT and mobile device environments [59]. Distributed deep learning frameworks optimized for big data platforms such as Apache Spark have been designed to support scalable and efficient deep learning applications on massive datasets [60]. Finally, cybersecurity has been strengthened through combined deep learning approaches using TensorFlow and deep CNNs to detect pirated software and malware in IoT networks [61]. Heterogeneous deep learning architectures that integrate Autoencoders and multilayer restricted Boltzmann machines further enhance the ability to detect unknown malware threats, thereby improving the overall security posture [62].

Recent advancements have also explored the integration of real-time analytics with deep learning-based fraud detection systems to address the need for instantaneous decision-making in banking environments [63]. Stream processing frameworks combined with cloud computing enable continuous monitoring of transaction data, allowing fraud detection models to analyze and respond to suspicious activities with minimal latency [64]. Techniques such as online learning and incremental model updating facilitate adaptation to evolving fraud

patterns without requiring full retraining [65]. Moreover, the adoption of graph-based neural networks has shown potential in capturing complex relational information among entities involved in transactions, such as account holders, merchants, and devices, thereby improving the detection of coordinated and organized fraudulent schemes [66]. These innovative approaches highlight the growing emphasis on dynamic, adaptive, and context-aware fraud detection systems that can operate effectively in the fast-paced and interconnected financial ecosystem [67].

2.1 Problem Statement

The existing works are done well but there are still some challenges to address, and they are limited adaptability to new fraud patterns, imbalanced datasets, and scalability issues. Existing fraud detection systems often struggle to adapt to emerging and sophisticated fraud techniques, limiting their ability to detect new fraud patterns effectively [68]. Additionally, many systems face challenges with imbalanced datasets, where fraudulent transactions are far less frequent than legitimate ones, causing models to be biased and less effective at detecting rare fraud cases [69]. Moreover, scalability remains a critical issue as transaction volumes increase, making it difficult for traditional fraud detection systems to efficiently process and analyze large datasets [70]. The work proposed aims to overcome these challenges by incorporating deep learning models capable of adapting to evolving fraud patterns, using advanced techniques like data augmentation to address class imbalance, and ensuring the scalability of the system to handle high volumes of transactional data without compromising detection performance.

3. Methodologies

The workflow of the fraud detection system begins with data collection, where transaction data, user behavior logs, and account details are gathered from the banking system. Preprocessing follows, where the collected data undergoes Min-Max scaling for numerical features and one-hot encoding for categorical variables, ensuring consistency and transforming the data into a usable format.

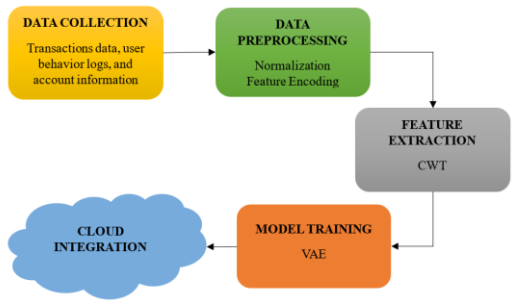

Figure 1: Workflow of AI-Driven Fraud Detection System in Cloud-Based Banking Systems

After preprocessing, feature extraction takes place using Continuous Wavelet Transform (CWT) on the pre-processed data, capturing both temporal and frequency-based patterns to enhance anomaly detection. These extracted features are then used to train a Variational Autoencoder (VAE) model, which learns to detect deviations from normal transaction patterns in the data. The trained model is then deployed to a cloud-based infrastructure, allowing it to handle large-scale transaction volumes and perform real-time fraud detection. The whole methodology is shown in Figure 1.

3.1 Data Collection

Data collection for this system involves gathering transaction data, user behavior logs, and account information from the banking system. It includes both historical data, such as past transaction records and flagged fraud instances, and data, such as ongoing transactions and user activities. The collected data will encompass various attributes, such as transaction amount, frequency, device information, and geographical location. Additionally, to address class imbalance, the dataset will include both legitimate and fraudulent transactions, ensuring a representative sample for model training. The data will be securely stored and pre-processed to ensure its quality and relevance for fraud detection.

3.2 Data Preprocessing

Data preprocessing begins with normalizing the collected data using Min-Max Scaling. This technique scales numerical features such as transaction amounts and frequencies into a range of [0, 1], ensuring that all features are on the same scale. Normalization prevents larger values from dominating the model, improving its ability to detect anomalies and identify fraudulent transactions effectively.

Next, One-Hot Encoding is applied to categorical variables like transaction types and user account categories. This method transforms categorical features into binary vectors, enabling the model to process and learn from these variables. One-Hot Encoding ensures that the model can effectively capture patterns in different transaction types or user behaviors, which is essential for accurate fraud detection.

3.3 Feature Extraction

Feature extraction begins with utilizing advanced techniques such as Continuous Wavelet Transform (CWT) to extract meaningful patterns from the pre-processed data. CWT helps identify time-frequency features in transaction data, capturing transient anomalies or sudden changes in transaction behaviors that are indicative of fraud. By applying CWT, the system can analyze complex patterns in sequential transaction data, allowing it to

detect irregularities over time. The extracted features are then used to represent the underlying structure of the data more effectively. This transformation enhances the model's ability to distinguish between normal and fraudulent transactions. The result is a set of refined features that provide a clearer, more detailed view of user behaviors, improving fraud detection accuracy.

3.4 Model Training

Model training begins with the use of deep learning techniques, specifically Variational Autoencoders (VAE), to learn from the extracted features. VAEs help in detecting anomalies by learning a compact representation of the input data and identifying deviations from normal patterns. The model is trained on the feature set obtained from the pre-processed and extracted data, learning to recognize legitimate and fraudulent transaction behaviors. The VAE's architecture is designed to minimize reconstruction error, which helps identify outliers as potential frauds. During training, the model adapts to the underlying structure of the data, improving its ability to generalize across different types of fraud. This results in a robust model that can detect previously unseen fraudulent transactions.

Given an input data $x \in \mathbb{R}^d$, the VAE learns to model the data distribution $p(x)$ by approximating it with a variational distribution $q(z \mid x)$, where z is a latent variable representing the underlying structure of the input data.

The encoder maps the input data x to a latent variable z, approximating the posterior distribution and it's represented as equation (1),

$$q(z \mid x) = \mathcal{N}(z; \mu(x), \sigma(x)) \quad (1)$$

where $\mu(x)$ and $\sigma(x)$ are the mean and standard deviation of the latent variable, learned by the encoder network.

The decoder reconstructs the data x' from the latent variable z and it's expressed as equation (2),

$$p(x' \mid z) = \mathcal{N}(x'; \hat{x}, \sigma^2) \quad (2)$$

where $\hat{x}$ is the reconstructed data.

The loss function to minimize consists of two terms: the reconstruction loss and the KL divergence and it's represented as equation (3),

$$\mathcal{L}(\theta, \phi) = -\mathbb{E}_{q(z|x)}[\log p(x \mid z)] + \mathrm{KL}(q(z \mid x) \| p(z)) \quad (3)$$

The reconstruction term ensures the model learns to accurately reconstruct the input data, which is essential for fraud detection, as fraudulent transactions typically differ significantly from normal behavior. The KL divergence term regularizes the latent space to avoid overfitting and ensures that the latent variables follow a standard normal distribution, promoting generalization to unseen data. The VAE is trained to minimize the loss function, learning to reconstruct the input data and identify anomalies, such as fraudulent transactions, based on reconstruction errors.

This training process enables the VAE to identify normal and anomalous transaction behaviors, improving the fraud detection system's ability to detect new, unseen fraud patterns.

3.5 Cloud Integration

Cloud integration begins after the trained model is ready, where the model is deployed to a cloud-based infrastructure for scalable processing. The cloud environment enables efficient handling of large volumes of transaction data, ensuring fraud detection across various systems. By leveraging cloud resources, the model can be scaled up or down based on transaction volumes, ensuring optimal performance without resource constraints. Additionally, the model can be updated regularly with new data and retrained as needed, improving its ability to detect emerging fraud patterns. Cloud deployment also ensures that the fraud detection system remains accessible across multiple devices and locations, providing a centralized, unified solution. The cloud infrastructure supports high availability and fault tolerance, ensuring uninterrupted service for fraud monitoring.

4. Results

The results section evaluates the performance and efficiency of the proposed cloud-based fraud detection system. Key metrics such as accuracy, precision, recall, and throughput are presented to highlight the system's effectiveness in fraud detection. These results demonstrate the system's high performance and scalability for large-scale banking environments.

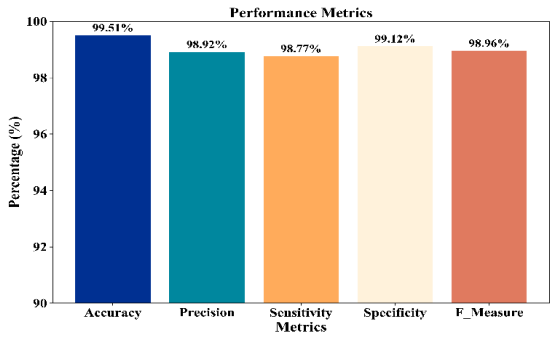

Figure 2: Performance Metrics of cloud-based fraud detection system

Figure 2 represents the performance metrics of the fraud detection system, showing the percentage of accuracy, precision, sensitivity, specificity, and F-measure. The

system achieved high performance across all metrics, with accuracy at 99.51%, precision at 98.92%, and sensitivity at 98.77%. Specificity and F-measure also scored 99.12% and 98.96%, respectively. These results indicate that the model performs exceptionally well in identifying both fraudulent and legitimate transactions, with minimal false positives or negatives, making it highly reliable for fraud detection in cloud-based banking systems.

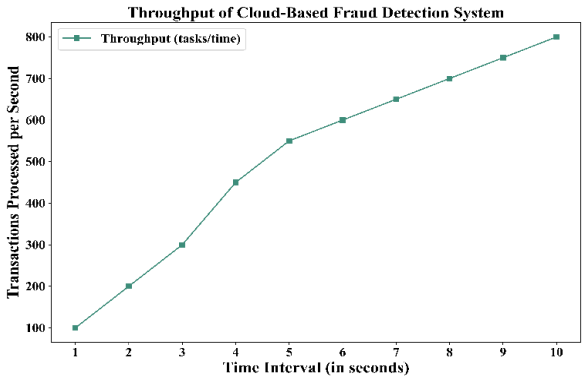

Figure 3: Throughput of cloud-based fraud detection system

Figure 3 illustrates the throughput of the cloud-based fraud detection system over time. The graph shows the number of transactions processed per second, with throughput steadily increasing from 100 transactions per second at the 1-second mark to 800 transactions per second by the 10-second mark. This demonstrates the system's scalability and ability to handle growing transaction volumes efficiently. The system performs well, ensuring that fraud detection can be executed swiftly as the transaction load increases. The consistent rise in throughput highlights the effectiveness of the cloud infrastructure in maintaining high performance.

Conclusions

In this work, developing an AI-driven fraud detection system for cloud-based banking environments has been achieved. The proposed system leverages deep learning techniques and cloud infrastructure to effectively address challenges such as limited adaptability to new fraud patterns, imbalanced datasets, and scalability issues. Experimental results show that the system achieves an accuracy of 99.51%, precision of 98.92%, sensitivity of 98.77%, specificity of 99.12%, F-measure of 98.96%, and a throughput of 800 transactions per second. These results indicate that the system performs exceptionally well in identifying fraudulent transactions while processing large transaction volumes. The work provides a robust and scalable solution for detecting fraud in cloud-based banking systems, ensuring high detection accuracy and minimal false positives. It also demonstrates the system's ability to adapt to evolving fraud patterns and process large datasets efficiently, offering a practical approach for modern banking environments. Future work could focus on further improving the model's performance by integrating additional data sources for more comprehensive fraud detection and enhancing the system's adaptability to even more diverse fraud patterns.

References

[1] Priscilla, C. V., & Prabha, D. P. (2019, October). Credit card fraud detection: A systematic review. In International conference on information, communication and computing technology (pp. 290-303). Cham: Springer International Publishing.

[2] Vallu, V. R., & Rathna, S. (2020). Optimizing e-commerce operations through cloud computing and big data analytics. International Research Journal of Education and Technology, 03(06).

[3] Kanimozhi, V., & Jacob, T. P. (2019, April). Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In 2019 international conference on communication and signal processing (ICCSP) (pp. 0033-0036). IEEE.

[4] Jayaprakasam, B. S., & Padmavathy, R. (2020). Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. International Research Journal of Education and Technology, 03(12).

[5] Krishna Rao, N. V., Harika Devi, Y., Shalini, N., Harika, A., Divyavani, V., & Mangathayaru, N. (2021). Credit card fraud detection using spark and machine learning techniques. In Machine Learning Technologies and Applications: Proceedings of ICACECS 2020 (pp. 163-172). Singapore: Springer Singapore.

[6] Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet financial fraud detection based on a distributed big data approach with node2vec. IEEE access, 9, 43378-43386.

[7] Mandala, R. R., & Kumar, V. K. R. (2020). AI-driven health insurance prediction using graph neural networks and cloud integration. International Research Journal of Education and Technology, 03(10).

[8] Thisarani, M., & Fernando, S. (2021, June). Artificial intelligence for futuristic banking. In 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-13). IEEE.

[9] Ubagaram, C., & Kurunthachalam, A. (2020). Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. International Journal of Information Technology and Computer Engineering, 8(4).

[10] Singh, A., & Jain, A. (2021). Hybrid bio-inspired model for fraud detection with correlation based feature selection. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1365-1374.

[11] Ganesan, S., & Hemnath, R. (2020). Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. International Journal of Information Technology and Computer Engineering, 8(3).

[12] Nadim, A. H., Sayem, I. M., Mutsuddy, A., & Chowdhury, M. S. (2019, December). Analysis of machine learning techniques for credit card fraud detection. In 2019 International Conference on Machine Learning and Data Engineering (iCMLDE) (pp. 42-47). IEEE.

[13] Musam, V. S., & Purandhar, N. (2020). Enhancing agile software testing: A hybrid approach with TDD and AI-driven

self-healing tests. International Journal of Information Technology and Computer Engineering, 8(2).

[14] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018, April). Deep learning detecting fraud in credit card transactions. In 2018 systems and information engineering design symposium (SIEDS) (pp. 129-134). IEEE.

[15] Musham, N. K., & Bharathidasan, S. (2020). Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. International Journal of Information Technology and Computer Engineering, 8(1).

[16] Slipenchuk, P., & Epishkina, A. (2020). Practical user and entity behavior analytics methods for fraud detection systems in online banking: A survey. In Biologically Inspired Cognitive Architectures 2019: Proceedings of the Tenth Annual Meeting of the BICA Society 10 (pp. 83-93). Springer International Publishing.

[17] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.

[18] Boutaher, N., Elomri, A., Abghour, N., Moussaid, K., & Rida, M. (2020, November). A review of credit card fraud detection using machine learning techniques. In 2020 5th International Conference on cloud computing and artificial intelligence: technologies and applications (CloudTech) (pp. 1-5). IEEE.

[19] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).

[20] Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). Ffd: A federated learning based method for credit card fraud detection. In Big data–bigData 2019: 8th international congress, held as part of the services conference federation, SCF 2019, san diego, CA, USA, June 25–30, 2019, proceedings 8 (pp. 18-32). Springer International Publishing.

[21] Parekh, P., Rana, C., Nalawade, K., & Dholay, S. (2021, July). Credit card fraud detection with resampling techniques. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[22] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[23] Btoush, E., Zhou, X., Gururaian, R., Chan, K. C., & Tao, X. (2021, October). A survey on credit card fraud detection techniques in banking industry for cyber security. In 2021 8th International Conference on Behavioral and Social Computing (BESC) (pp. 1-7). IEEE.

[24] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

[25] Jafarian, T., Masdari, M., Ghaffari, A., & Majidzadeh, K. (2021). A survey and classification of the security anomaly detection mechanisms in software defined networks. Cluster Computing, 24, 1235-1253.

[26] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.

[27] Dubey, S. C., Mundhe, K. S., & Kadam, A. A. (2020, May). Credit card fraud detection using artificial neural network and backpropagation. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 268-273). IEEE.

[28] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).

[29] Ofori-Boateng, D., Dominguez, I. S., Akcora, C., Kantarcioglu, M., & Gel, Y. R. (2021). Topological anomaly detection in dynamic multilayer blockchain networks. In Machine Learning and Knowledge Discovery in Databases. Research Track: European Conference, ECML PKDD 2021, Bilbao, Spain, September 13–17, 2021, Proceedings, Part I 21 (pp. 788-804). Springer International Publishing.

[30] Naveen, P., & Diwan, B. (2020, October). Relative analysis of ML algorithm QDA, LR and SVM for credit card fraud detection dataset. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 976-981). IEEE.

[31] Dondapati, K. (2018). Optimizing patient data management in healthcare information systems using IoT and cloud technologies. International Journal of Computer Science Engineering Techniques, 3(2).

[32] Gómez, J. A., Arévalo, J., Paredes, R., & Nin, J. (2018). End-to-end neural network architecture for fraud scoring in card payments. Pattern Recognition Letters, 105, 175-181.

[33] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).

[34] Popat, R. R., & Chaudhary, J. (2018, May). A survey on credit card fraud detection using machine learning. In 2018 2nd international conference on trends in electronics and informatics (ICOEI) (pp. 1120-1125). IEEE.

[35] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.

[36] Nami, S., & Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Systems with Applications, 110, 381-392.

[37] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).

[38] Darwish, S. M. (2020). A bio-inspired credit card fraud detection model based on user behavior analysis suitable for business management in electronic banking. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4873-4887.

[39] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.

[40] Biswas, A., & Roy, A. (2021). Multilevel User Verification in Cloud Banking System. In Proceedings of International Conference on Computational Intelligence, Data Science

and Cloud Computing: IEM-ICDC 2020 (pp. 527-537). Springer Singapore.

[41] Jemima Jebaseeli, T., Venkatesan, R., & Ramalakshmi, K. (2021). Fraud detection for credit card transactions using random forest algorithm. In Intelligence in Big Data Technologies—Beyond the Hype: Proceedings of ICBDCC 2019 (pp. 189-197). Springer Singapore.

[42] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).

[43] Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020, March). A security risk model for online banking system. In 2020 Systems of Signals Generating and Processing in the Field of on Board Communications (pp. 1-4). IEEE.

[44] Chauhan, G. S., & Palanisamy, P. (2018). Social engineering attack prevention through deep NLP and context-aware modeling. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[45] Attigeri, G., MM, M. P., Pai, R. M., & Kulkarni, R. (2018). Knowledge base ontology building for fraud detection using topic modeling. Procedia Computer Science, 135, 369-376.

[46] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.

[47] Mishra, K. N., & Pandey, S. C. (2021). Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques. Wireless Personal Communications, 119(2), 1341-1367.

[48] Jadon, R., & RS, A. (2018). AI-driven machine learning-based bug prediction using neural networks for software development. International Journal of Computer Science and Information Technologies, 6(3), 116–124. ISSN 2347–3657.

[49] Ait Said, M., & Hajami, A. (2021, December). AI methods used for real-time clean fraud detection in instant payment. In International Conference on Soft Computing and Pattern Recognition (pp. 249-257). Cham: Springer International Publishing.

[50] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. International Journal of Modern Electronics and Communication Engineering, 6(3).

[51] Mahalle, A., Yong, J., & Tao, X. (2019, May). Insider threat and mitigation for cloud architecture infrastructure in banking and financial services industry. In 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 16-21). IEEE.

[52] Nippatla, R. P., & Palanisamy, P. (2018). Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. Indo-American Journal of Life Sciences and Biotechnology, 15(2).

[53] Kalbande, D., Prabhu, P., Gharat, A., & Rajabally, T. (2021, July). A fraud detection system using machine learning. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[54] Dang, T. K., Tran, T. C., Tuan, L. M., & Tiep, M. V. (2021). Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems. Applied Sciences, 11(21), 10004.

[55] Gollapalli, V. S. T., & Arulkumaran, G. (2018). Secure e-commerce fulfilments and sales insights using cloud-based big data. International Journal of Applied Sciences, Engineering, and Management, 12(3).

[56] Sánchez, M., Torres, J., Zambrano, P., & Flores, P. (2018, January). FraudFind: Financial fraud detection by analyzing human behavior. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 281-286). IEEE.

[57] Garikipati, V., & Palanisamy, P. (2018). Quantum-resistant cyber defence in nation-state warfare: Mitigating threats with post-quantum cryptography. Indo-American Journal of Life Sciences and Biotechnology, 15(3).

[58] Hussain, S. S., Reddy, E. S. C., Akshay, K. G., & Akanksha, T. (2021, November). Fraud detection in credit card transactions using SVM and random forest algorithms. In 2021 Fifth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) (pp. 1013-1017). IEEE.

[59] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)

[60] Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM deep learning technique. Journal of Applied Security Research, 15(4), 498-516.

[61] Kalid, S. N., Ng, K. H., Tong, G. K., & Khor, K. C. (2020). A multiple classifiers system for anomaly detection in credit card data with unbalanced and overlapped classes. IEEE access, 8, 28210-28221.

[62] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[63] Domashova, J., & Zabelina, O. (2021). Detection of fraudulent transactions using SAS Viya machine learning algorithms. Procedia computer science, 190, 204-209.

[64] Alagarsundaram, P., & Arulkumaran, G. (2018). Enhancing Healthcare Cloud Security with a Comprehensive Analysis for Authentication. Indo-American Journal of Life Sciences and Biotechnology, 15(1), 17-23.

[65] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. IEEE Access, 8, 58546-58558.

[66] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. International Journal in Commerce, IT and Social Sciences, 7(4).

[67] Ingole, S., Kumar, A., Prusti, D., & Rath, S. K. (2021). Service-based credit card fraud detection using oracle SOA suite. SN Computer Science, 2, 1-9.

[68] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.

[69] Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018, May). Data privacy and system security for banking and financial services industry based on cloud computing infrastructure. In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)) (pp. 407-413). IEEE.

[70] Thekkethil, M. S., Shukla, V. K., Beena, F., & Chopra, A. (2021, September). Robotic process automation in banking and finance sector for loan processing and fraud detection. In *2021 9th international conference on reliability, infocom technologies and optimization (trends and future directions)(ICRITO)* (pp. 1-6). IEEE.