INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)
VOL.06 ISSUE 02 (2026)

*Research Article*

# Hybrid Optimization Framework for Cloud-Based Financial Fraud Detection and Intelligent Alert Generation Using Deep Belief Learning

**Azizbek Karimov** [1]

[1]Department of Artificial Intelligence and Computer Science Uzbekistan Institute of Intelligent Technologies, Uzbekistan

Received: 25 May 2026
Revised: 20 June 2026
Accepted: 14 July 2026
Published: 14 August 2026

**Doi**:10.55640/ijdsml-06-02-04

Page No: 93-102



## Abstract

The increasing digitization of financial services has expanded the volume, velocity, and heterogeneity of transaction data while simultaneously increasing opportunities for sophisticated fraudulent activity. Conventional fraud detection approaches frequently encounter difficulties associated with nonlinear transaction patterns, evolving fraud behavior, class imbalance, high-dimensional attributes, and the requirement for rapid alert generation in cloud environments. This paper proposes a Hybrid Optimization Framework for Cloud-Based Financial Fraud Detection and Intelligent Alert Generation Using Deep Belief Learning (HO-DBL). The framework integrates deep belief learning with feature transformation, dimensionality optimization, supervised discrimination, risk scoring, and cloud-oriented alert orchestration. The theoretical foundation is derived from representation-learning, transfer-learning, deep neural architectures, restricted Boltzmann machine-based learning, and few-shot learning research. Existing studies demonstrate the ability of deep architectures to learn discriminative representations from complex data, while hybrid CNN-RBM approaches demonstrate the feasibility of combining complementary learning mechanisms (Cheng, 2019). The proposed framework extends these principles to financial transactions by using a deep belief learning layer for latent representation, an optimization layer for feature and decision refinement, and an intelligent alert module for prioritizing potentially fraudulent events. The framework is positioned as an adaptive architecture rather than a claim of experimentally measured superiority. Analytical findings indicate that hybrid representation and optimization can potentially improve discrimination, reduce unnecessary alerts, support rare-pattern detection, and improve operational prioritization. The study contributes an integrated conceptual architecture for real-time cloud fraud analytics and identifies future requirements for empirical benchmarking, concept-drift adaptation, explainability, and production-scale validation.

**Keywords:** Financial Fraud Detection; Deep Belief Learning; Cloud Computing; Hybrid Optimization; Intelligent Alerting; Representation Learning; Risk Scoring; Real-Time Analytics; Anomaly Detection.

## INTRODUCTION

### 1.1 Background

Financial fraud has become increasingly difficult to detect because contemporary transactions are characterized by high dimensionality, heterogeneous attributes, temporal dependencies, and rapidly changing behavioral patterns. A transaction may

appear legitimate when individual attributes are evaluated independently but become suspicious when contextual relationships among transaction amount, timing, location, account behavior, merchant characteristics, and transaction frequency are considered collectively. Consequently, fraud detection increasingly requires learning systems capable of extracting latent representations rather than relying exclusively on manually engineered rules.

Deep learning provides a theoretical basis for such representation learning. Deep architectures can transform raw or engineered inputs through multiple nonlinear layers, enabling progressively abstract representations. Deep residual learning demonstrated the effectiveness of increasingly deep representations for complex recognition tasks (He et al., 2015), while transfer-learning studies demonstrated that learned representations can be adapted to related recognition problems (Cao et al., 2013). Although many of the supplied studies originate in computer vision, their methodological significance extends to financial analytics because both domains require discriminative representations from high-dimensional and noisy observations.

Deep belief learning is particularly relevant because it can construct hierarchical latent representations through successive probabilistic learning stages. The feasibility of combining restricted Boltzmann machine-based learning with convolutional architectures has been demonstrated in gesture recognition, where complementary representation mechanisms were jointly exploited (Cheng et al., 2019). This provides a conceptual foundation for integrating deep belief representations with optimization and classification mechanisms in fraud detection.

Cloud computing further changes the operational requirements of fraud analytics. Financial institutions may process extremely large transaction streams and require elastic computational resources, centralized model services, scalable storage, and event-driven alerting. Therefore, a fraud detection architecture should not only maximize predictive discrimination but also support low-latency inference and operationally meaningful alert prioritization.

### 1.2 Problem Statement

Traditional rule-based systems can identify known fraud signatures but may struggle with previously unseen or deliberately obfuscated behaviors. Purely supervised models may similarly be constrained when fraudulent observations constitute only a small proportion of the available transaction population. Moreover, maximizing classification sensitivity without controlling false positives can overwhelm investigators with low-value alerts.

The central research problem is therefore the development of an architecture capable of learning nonlinear representations, optimizing discriminatory information, identifying rare fraudulent patterns, and converting model outputs into prioritized alerts. The study addresses this problem through a hybrid framework that combines deep belief learning and optimization within a cloud-oriented processing pipeline.

### 1.3 Research Relevance

The proposed framework is motivated by the need to connect machine-learning intelligence with operational fraud-response mechanisms. Existing deep-learning studies demonstrate strong representation-learning capabilities, but the supplied literature largely concentrates on image recognition, few-shot learning, and visual feature extraction. The contribution of this study is consequently to reinterpret these principles for financial fraud analytics while integrating detection and alert generation into a unified architecture.

The work is also directly related to the financial cloud architecture proposed by Lankala et al. (2025), which investigates financial fraud detection and alerting using a Deep Belief Network. The present framework extends that direction by emphasizing hybrid optimization and intelligent alert prioritization rather than treating detection as an isolated classification task (Lankala et al., 2025).

### 1.4 Objectives

The primary objective is to design a hybrid cloud-based framework for financial fraud detection using deep belief learning. Specific objectives are to develop a hierarchical transaction representation mechanism, introduce optimization for feature and decision refinement, construct an intelligent fraud-risk scoring layer, and design an alert-generation mechanism that prioritizes events according to risk severity.

### 1.5 Scope and Significance

The framework focuses on transaction-level fraud analytics in cloud environments. It is applicable conceptually to banking transactions, digital payments, online financial services, and other high-volume financial ecosystems. Its significance lies in integrating detection accuracy with operational alert management. Rather than considering every positive prediction equally important, the proposed architecture distinguishes between transaction classification and subsequent risk prioritization.

## LITERATURE REVIEW

Deep representation learning has demonstrated that complex observations can be transformed into more useful feature spaces. Belhumeur et al. (1997) established the importance of discriminative projection through class-specific representations, showing that representation quality directly affects recognition performance. Although developed for face recognition, this principle is applicable to fraud detection because transaction attributes must similarly be projected into spaces in which legitimate and fraudulent behaviors become more distinguishable.

Subsequent research expanded representation learning through deep architectures. Chen and Haoyu (2019) investigated VGG-based feature extraction combined with SVM classification, illustrating the value of separating representation learning from final discrimination. Gwyn et al. (2021) comparatively examined popular deep architectures and emphasized differences in their representational characteristics. These studies collectively suggest that a fraud detection architecture should distinguish between feature learning and decision-making rather than assuming that a single model component is optimal for both functions.

Deep residual learning introduced an alternative mechanism for learning complex representations through deeper networks (He et al., 2015). Similarly, Boonyuen et al. (2019) demonstrated the practical use of convolutional neural networks for predictive modeling from satellite imagery. Although the application domain differs substantially from finance, the underlying principle of extracting hierarchical information from complex input spaces supports the conceptual use of deep representation mechanisms in transaction analytics.

The supplied literature also provides strong evidence for hybrid and probabilistic architectures. Cheng et al. (2019) combined CNN and RBM mechanisms, demonstrating that complementary learning components can be jointly employed for recognition. This is particularly relevant to the present study because Deep Belief Networks can be treated as representation-learning components while separate optimization and classification layers refine the final decision. The framework proposed by Lankala et al. (2025)

provides the closest domain-specific foundation, explicitly applying Deep Belief Networks to financial fraud detection and alerting in cloud computing.

Another important research direction concerns learning under limited or unusual observations. Fei-Fei et al. (2006) investigated one-shot learning, while Koch (2015) examined Siamese neural networks for one-shot image recognition. Lake et al. (2011) similarly explored learning visual concepts from limited examples. Jadon and Jadon (2020) reviewed deep-learning architectures for few-shot learning, while Ren et al. (2018) proposed incremental few-shot learning using attention attractor networks. Müuller et al. (2022) further investigated few-shot learning with Siamese networks and label tuning. These studies are theoretically important for fraud detection because novel fraud types may initially have very few labeled examples.

Chen et al. (2020) explored simple Siamese representation learning, and Caron et al. (2020) demonstrated unsupervised learning through contrasting cluster assignments. Together, these studies reinforce the importance of learning useful representations without requiring extensive labeled examples. This is particularly valuable where fraud labels are sparse, delayed, or continually changing.

Studies concerning face datasets and transfer learning, including Huang et al. (2008), Cao et al. (2017), Cao et al. (2013), Chen et al. (2012), Nam et al. (2018), and Jadon and Jadon (2020), further establish that robust representation learning requires consideration of variation, scale, and domain differences. The financial equivalent involves changes in customer behavior, transaction channels, merchants, geographic patterns, and attack strategies.

Despite these advances, a clear research gap remains. Much of the supplied literature addresses visual recognition, whereas only Lankala et al. (2025) directly addresses financial fraud detection and cloud alerting. The literature therefore provides strong methodological components but limited integration of deep belief learning, optimization, risk scoring, and intelligent cloud alert management. The proposed HO-DBL framework addresses this gap by treating fraud detection as a multi-stage intelligence pipeline.

## METHODOLOGY

### 3.1 Proposed Research Framework

The proposed HO-DBL framework consists of six interconnected stages: transaction acquisition, preprocessing and normalization, deep belief representation learning, hybrid optimization, fraud classification and risk scoring, and intelligent alert generation.

Conceptually, the architecture follows:

Financial Transactions → Cloud Data Ingestion → Preprocessing → Deep Belief Representation → Hybrid Optimization → Fraud Classification → Risk Scoring → Intelligent Alerting → Investigator Feedback

The architecture is designed so that representation learning and operational decision-making are not collapsed into a single model. This separation improves conceptual flexibility and allows each component to be optimized according to its function.

### 3.2 Transaction Data Acquisition and Preprocessing

The first stage receives transaction records from heterogeneous financial sources. Relevant variables may include transaction amount, timestamp, merchant category, transaction frequency, channel, geographic information, device characteristics, account history, and aggregated behavioral indicators.

Numerical attributes are normalized to prevent high-magnitude variables from dominating model learning. Categorical attributes can be encoded into numerical representations, while temporal attributes may be transformed into behavioral indicators such as transaction frequency or deviation from historical patterns.

A critical issue is class imbalance. Fraud typically represents a much smaller proportion of transactions than legitimate activity. Therefore, model evaluation should not depend exclusively on overall accuracy. Precision, recall, F1-score, false-positive rate, and area-based discrimination measures should be evaluated jointly.

### 3.3 Deep Belief Representation Layer

The core learning component uses a stacked probabilistic representation mechanism inspired by Deep Belief Networks. The objective is to transform transaction features into increasingly informative latent representations.

At a simplified level, an RBM models the relationship between visible transaction variables (v) and latent variables (h). Its energy function can be represented as:

[

E(v,h)=-a^Tv-b^Th-v^TWh

]

where (a) and (b) represent visible and hidden biases and (W) represents the interaction weights.

The resulting hidden representation can encode nonlinear relationships that are difficult to capture through manually defined rules. Stacking multiple representation layers allows the framework to learn progressively abstract transaction patterns.

This design is conceptually consistent with the hybrid CNN-RBM strategy explored by Cheng et al. (2019). However, instead of visual patterns, the proposed framework applies latent representation learning to transaction behavior.

### 3.4 Hybrid Optimization Layer

Deep representation alone does not guarantee optimal fraud discrimination. The proposed optimization layer therefore performs feature selection, latent-dimension refinement, threshold calibration, and model-parameter optimization.

A generalized optimization objective can be represented as:

[

J=\alpha L_{classification}+\beta L_{false-positive}+\gamma C_{latency}+\delta C_{complexity}

]

where (L_{classification}) measures detection error, (L_{false-positive}) penalizes excessive false alerts, (C_{latency}) represents inference-delay cost, and (C_{complexity}) controls computational burden. The coefficients (\alpha,\beta,\gamma,\delta) determine the operational priorities.

This multi-objective formulation is important because a fraud system optimized solely for recall may generate excessive alerts, whereas a system optimized solely for precision

may miss emerging fraud.

### 3.5 Fraud Classification and Risk Scoring

The optimized latent representation is supplied to a classification layer that estimates the probability of fraud:

[

P(F=1|x)=\sigma(f_{\theta}(z))

]

where (x) denotes the transaction input, (z) represents the learned latent representation, (f_{\theta}) denotes the classifier, and (\sigma) represents the probability transformation.

Instead of treating this probability as the final output, the framework converts it into an operational risk score. Risk can incorporate model confidence, transaction deviation, historical account behavior, and contextual indicators.

For example, a transaction with moderate fraud probability but a substantial deviation from historical behavior may receive a higher operational priority than a transaction with the same probability but no behavioral deviation.

### 3.6 Intelligent Alert Generation

The alert module converts risk scores into operational categories such as low, medium, high, and critical. Thresholds should be configurable according to organizational risk tolerance.

The proposed mechanism is:

[

Alert_i=

\begin{cases}

Critical,&R_i\geq T_3\

High,&T_2\leq R_i<T_3\

Medium,&T_1\leq R_i<T_2\

Low,&R_i<T_1

\end{cases}

]

This design separates automated detection from automated response prioritization. High-confidence critical events can be escalated immediately, while lower-risk observations can be accumulated for secondary analysis.

The integration of fraud detection and alert generation follows the central direction of Lankala et al. (2025), but the present framework emphasizes optimization of the entire analytical-to-alert pipeline rather than classification alone.

### 3.7 Cloud Deployment Architecture

The framework is designed for cloud deployment using logically separated data ingestion, model-serving, analytics, and alert-management services. Transaction streams enter a scalable ingestion layer, after which preprocessing and representation services generate optimized features.

The inference service then produces fraud probabilities and risk scores. Alert events are forwarded to an orchestration layer that can integrate with case-management systems, notification mechanisms, and investigator dashboards.

Cloud deployment offers elasticity, but it also introduces latency, security, model-versioning, and computational-cost considerations. Consequently, optimization must consider both statistical performance and infrastructure efficiency.

### 3.8 Evaluation Strategy

Because the present work proposes an integrated framework rather than reporting a newly executed benchmark experiment, its results are expressed as analytical framework findings rather than fabricated empirical measurements. A complete empirical evaluation should compare the proposed architecture against conventional classifiers, standalone Deep Belief Networks, and non-optimized deep-learning configurations.

A suitable evaluation protocol should include precision, recall, F1-score, false-positive rate, detection latency, alert volume, and computational cost. Particular attention should be given to minority-class recall because a model with high overall accuracy may still perform poorly on fraudulent transactions.

## RESULTS

The analytical evaluation of the proposed framework identifies several principal findings. First, the integration of hierarchical representation learning and optimization provides a stronger conceptual basis for fraud discrimination than an isolated classification model. Deep learning studies demonstrate that layered representations can capture complex patterns, while the RBM-based hybrid approach of Cheng et al. (2019) illustrates the value of combining complementary learning mechanisms. Within financial transactions, this suggests that latent representations can capture interactions among transaction variables that may remain invisible to fixed rules.

Second, the optimization layer addresses an important operational weakness of fraud detection systems: the trade-off between fraud sensitivity and alert volume. A detection architecture that identifies a large proportion of fraudulent transactions but simultaneously produces excessive false positives can impose significant investigative costs. The proposed multi-objective optimization explicitly incorporates classification quality, false-positive control, latency, and computational complexity. Therefore, its intended outcome is not simply greater sensitivity but a more balanced detection-alerting system.

Third, the framework is theoretically better suited to rare and emerging fraud patterns than approaches dependent exclusively on large quantities of labeled examples. The supplied few-shot and representation-learning literature demonstrates that useful representations can support learning under limited supervision (Fei-Fei et al., 2006; Koch, 2015; Ren et al., 2018). This principle is important in financial environments where newly emerging fraud categories may initially contain few confirmed examples.

Fourth, intelligent alert generation changes the operational meaning of a fraud prediction. Instead of producing an undifferentiated binary decision, the proposed

system assigns risk levels and prioritizes events. This can reduce investigator workload by directing immediate attention toward transactions with the highest combined risk. The approach is consistent with the financial fraud detection and alerting direction established by Lankala et al. (2025), while extending it through an explicit optimization layer.

Fifth, cloud deployment introduces a trade-off between scalability and inference complexity. A deep architecture can improve representational capacity but may increase computational requirements. Consequently, the optimization layer should be viewed as both a statistical and infrastructure mechanism. The desired outcome is a model that provides adequate discrimination without producing unacceptable latency or resource consumption.

Finally, the literature suggests that representation robustness is essential under distributional variation. Studies of recognition across pose, age, resolution, and unconstrained environments (Cao et al., 2017; Nam et al., 2018; Huang et al., 2008) provide an analogous theoretical lesson: a model trained on one distribution may not remain equally effective under changing conditions. In fraud detection, this corresponds to behavioral drift and new attack strategies. Thus, continuous monitoring and periodic model adaptation should be incorporated into practical deployment.

## DISCUSSION

The findings indicate that the primary contribution of HO-DBL is architectural integration rather than the introduction of a single novel neural operator. This distinction is important because financial fraud detection is not solely a classification problem. It is a decision-support problem in which statistical prediction, computational efficiency, operational prioritization, and investigator capacity interact.

From a theoretical perspective, the framework combines principles from discriminative representation learning, probabilistic latent modeling, deep architectures, and limited-data learning. Belhumeur et al. (1997) established the importance of class-discriminative representations, while later deep-learning research demonstrated that hierarchical representations can capture increasingly complex patterns (He et al., 2015). The proposed architecture transfers these principles to transaction data and adds an optimization stage intended to make learned representations operationally useful.

A significant implication concerns the role of hybridization. Cheng et al. (2019) showed that CNN and RBM components can be integrated to exploit complementary characteristics. In the proposed fraud architecture, hybridization occurs at a broader level: deep belief learning extracts latent information, optimization refines the representation and decision boundary, and alert intelligence converts probabilistic outputs into operational actions. This modular design may be more adaptable than a monolithic classifier because individual components can be improved independently.

The framework also addresses the tension between rare-event detection and false-positive management. Few-shot learning research demonstrates the importance of learning from limited examples (Lake et al., 2011; Jadon & Jadon, 2020). However, recognizing rare fraud cannot simply mean lowering the classification threshold. Doing so may increase false positives. The proposed risk-scoring mechanism therefore provides a second decision layer through which contextual information can influence alert severity without necessarily changing the underlying fraud probability.

The relationship with Lankala et al. (2025) is particularly significant. Their work establishes a domain-specific foundation for using Deep Belief Networks in cloud-based financial fraud detection and alerting. The proposed HO-DBL framework builds on that

research direction by emphasizing hybrid optimization and differentiated alert management. The contribution should therefore be understood as an architectural extension that seeks to improve the connection between model intelligence and operational response (Lankala et al., 2025).

Nevertheless, several limitations remain. First, the current study does not claim experimentally validated numerical superiority because no new transaction dataset or benchmark experiment was supplied. Second, Deep Belief Networks may involve higher computational costs than lightweight models, creating challenges for extremely high-throughput environments. Third, concept drift may reduce model effectiveness when fraud strategies evolve. Fourth, risk scores may be difficult to explain to investigators unless additional interpretability mechanisms are integrated. Finally, cloud deployment introduces security, privacy, governance, and latency requirements that cannot be solved exclusively through model optimization.

Future empirical research should therefore benchmark HO-DBL using highly imbalanced financial datasets, evaluate performance under temporal distribution shifts, compare alternative optimization strategies, and measure the relationship between alert reduction and fraud-recovery performance. Such evaluation would establish whether the conceptual benefits translate into measurable production improvements.

## CONCLUSION

This paper proposed a Hybrid Optimization Framework for Cloud-Based Financial Fraud Detection and Intelligent Alert Generation Using Deep Belief Learning. The framework integrates transaction preprocessing, hierarchical deep belief representation, multi-objective optimization, fraud classification, risk scoring, and cloud-based alert orchestration. Its central contribution is the integration of predictive intelligence with operational alert prioritization.

The literature indicates that deep representation learning, probabilistic architectures, hybrid neural systems, and few-shot learning provide complementary foundations for addressing complex and sparse recognition problems. By transferring these principles to financial transaction analytics, HO-DBL provides a structured approach for identifying nonlinear fraud patterns while controlling alert volume and computational requirements.

The framework extends the direction of Deep Belief Network-based financial fraud detection and alerting established by Lankala et al. (2025) by explicitly introducing hybrid optimization and risk-sensitive alert generation. However, empirical validation remains essential. Future research should evaluate the framework against real-world transaction datasets, assess robustness to concept drift, investigate explainable risk scoring, and quantify cloud-scale latency and resource consumption. These developments can strengthen the practical viability of intelligent, adaptive, and scalable financial fraud detection systems.

## REFERENCES


1. Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997).Eigenfaces vs. Fisherfaces: Recognition using class specificlinear projection .IEEE Transactions on Pattern Analysisand Machine Intelligence, 19(7), 711–720.

2. Boonyuen, K., Kaewprapha, P., Weesakul, U., & Srivihok, P.(2019). Convolutional neural network inception-v3: Amachine learning approach for leveling short-range rainfall forecast model from satellite image. InInternational Conference on Swarm Intelligence 2019: Advances inSwarm Intelligence, 105–115.

3. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2017).Vggface2: A dataset for recognising faces across pose and age.arXiv Preprint: 1710.08092.

**4.** Cao, X., Wipf, D., Wen, F., Duan, G., & Sun, J. (2013). A practicaltransfer learning algorithm for face verification. In2013 IEEEInternational Conference on Computer Vision, 3208–3215.

**5.** Caron, M., Misra, I., Mairal, J., Goyal, P., Bojanowski, P., & Joulin, A.(2020). Unsupervised learning of visual features by contrastin gcluster assignments.ar Xiv Preprint:2006.09882.

**6.** Cheng, W., Sun, Y., Li, G., Jiang, J., & Liu, H. (2019). Jointlynet work: A network based on CNN and RBM for gesturerecognition.Neural Computing & Applications,31(1),309–323.

**7.** Chen, D., Cao, X., Wang, L., Wen, F., & Sun, J. (2012). Bayesianface revisited: A joint formulation. In12th Euorpean Conference on Computer Vision, 566–579.

**8.** Chen, H., & Haoyu, C. (2019). Face recognition algorithm based onVGG network model and SVM.Journal of Physics:Conference Series,1229(1), 012015.

**9.** Chen, X., & He, K. (2020). Exploring simple Siamesere presentation learning.ar Xiv Preprint: 2011.10566.

**10.** Fei-Fei, L., Fergus, R., & Perona, P. (2006). One-shot learning ofobject categories.IEEE Transactions on Pattern Analysisand Machine Intelligence,28(4), 594–611.

**11.** Gwyn, T., Roy, K., & Atay, M. (2021). Face recognition using populardeep net architectures: A brief comparative study.FutureInternet,13(7), 164.

**12.** He, K., Zhang, X., Ren, S., & Sun, J. (2015). Deep residual learningfor image recognition.arXiv Preprint: 1512.03385.

**13.** Huang, G. B., Ramesh, M., Berg, T., &Learned-Miller, E.(2008). Labeledfaces in the wild: A database for studying face recognition inunconstrained environments. InWorkshop on Faces in'Real-Life'Images: Detection, Alignment, and Recognition.

**14.** Jadon, S., & Jadon, A. (2020). An overview of deep learning architecturesin few-shot learning domain.arXiv Preprint:2008.06365.

**15.** Koch, G. R. (2015).Siamese neural networks for one-shot imagerecognition. Master's Thesis, University of Toronto.

**16.** Lake, B. M., Salakhutdinov, R., Gross, J., & Tenenbaum, J. B.(2011). One shot learning of simple visual concepts. InProceedings of the Annual Meeting of the Cognitive ScienceSociety,33(33), 2568–2573.

**17.** Müuller, T., Pérez-Torr´o, G., & Franco-Salvador, M. (2022).Few-shot learning with Siamese networks and label tuning.arXiv Preprint: 2203.14655.

**18.** Nam, G. P., Choi, H., Cho, J., & Kim, I.-J. (2018). PSI-CNN: Apyramid-based scale-invariant CNN architecture for facerecognition robust to various image resolutions. Applied Sciences,8(9), 1561.

**19.** Ren, M., Liao, R., Fetaya, E., & Zemel, R. S. (2018). Incrementalfew-shot learning with attention attractor networks.ar Xiv Preprint: 1810.07218.

**20.** S. R. Lankala, M. R. Marri, A. Jain, G. G. Battu, U. Lakhina and S. Singla, "Optimal Financial Fraud Detection and Alerting Mechanism in Cloud Computing Using Deep Belief Network," 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2025, pp. 743-748, doi: 10.1109/ETNCC66224.2025.11299665