World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Anomaly Detection in HR data using variational autoencoders: A deep learning approach to fraud detection and performance outliers

Thirusubramanian Ganesan [1], Mohanarangan Veerapperumal Devarajan [2], Akhil Raj Gaius Yallamelli [3], Vijaykumar Mamidala [4], Rama Krishna Mani Kanta Yalla [5] and Veerandra Kumar R [6,*]

[1] *Cognizant Technology Solutions, Texas, USA.*
[2] *EY Government Services LLC, Sacramento, USA.*
[3] *Amazon Web Services Inc, Seattle, USA.*
[4] *Conga (Apttus), Broomfield, CO, USA.*
[5] *Amazon Web Services, Seattle, WA, USA.*
[6] *Saveetha Engineering College,Saveetha Nagar, Thandalam,Chennai,602105.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 14(03), 267-274

Publication history: Received on 06 February 2025; revised on 13 March 2025; accepted on 15 March 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.14.3.0133

Abstract

Fraud detection in Human Resource Management is a critical issue because payroll fraud and performance anomalies will lead to loss and inefficiency. Traditional fraud detection methods are unable to detect complex data patterns, and therefore a reliance is made on machine learning methods. In this research, a deep learning-based framework with the integration of Variational Autoencoders and Sparse Autoencoders for HRM data anomaly detection is introduced. The model is trained on a fraud detection data set, picking up normal patterns of payroll transactions and employee performance metrics. Anomalies are detected by the model as having high reconstruction errors, which would be indicative of fraudulent activity or performance outliers. For evaluating the proposed method, extensive experiments were conducted on widely available fraud detection data sets. The results indicate that the VAE-based model achieved accuracy of 98.4%, precision of 96.9%, recall of 97.2%, and F1-score of 97.0% compared to standard anomaly detection models. The model was also able to reveal embedded patterns in HR data, reducing false positives to a minimum, and enhancing fraud detection validity. The research establishes how deep learning can be utilized to detect fraud in HRM systems as a fast and independent process for HR professionals. The future will also see the implementation of hybrid models as well as real-time anomaly detection to further advance fraud prevention.

Keywords: Deep Learning; Autoencoder; Anomaly Detection; Hr Fraud; Payroll Security

1. Introduction

Human Resource Management is fundamental in every successful business, managing recruitment, training, administration, and personnel maintenance [1]. Fraud detection as a Human Resource Management activity is a critical activity with the cases of payroll fraud, expense report fraud, and performance variations [2] . Rule-based detection systems cannot identify intricate fraud patterns that lead to financial loss and operational inefficiency [3]. With additional HR information, sophisticated machine learning methods will have to be used to find nuanced payroll patterns and employee performance metric anomalies [4]. Deep learning, and autoencoder-based anomaly detection in particular, is an appealing alternative through abnormal behavior deviation detection [5].

Autoencoders can learn the high dimensional data distributions and identify outliers without labeled fraud instances [6]. The framework utilizes Variational Autoencoders and Sparse Autoencoders to achieve maximum accuracy and

* Corresponding author: Veerandra Kumar R.

stability in detecting fraud [7]. This work aims at developing an automatic system with maximum detection rates and minimizing false positives [8]. With the inclusion of deep learning, HR professionals can effectively handle fraud risk and make more informed decisions [9]. The aim of this research is to develop an automated system with low false positives and improved detection [10]. With the use of deep learning, HR professionals can predict fraud risk and enhance decision-making [11].

1.1. research Objective

- Develop a deep learning-based fraud detection system for HRM to detect payroll fraud and performance irregularities efficiently with the help of anomaly detection techniques.
- Adopt a publicly accessible fraud detection data to train and test the proposed model so that it can be applied on actual HRM data.
- Use Variational Autoencoders to learn typical HR transaction patterns and identify high-reconstruction-error fraud transactions
- Incorporate Sparse Autoencoders to enhance anomaly detection capabilities by identifying small changes in employee performance indicators and payroll transactions.

1.2. Research Organization

The structure of the proposed framework is sequential. Section 1 contains background, significance, and objectives of the study, highlighting the need for sophisticated fraud detection in HRM. Section 2 is a literature review of earlier techniques of fraud detection. Section 3 develops the problem statement. Section 4 presents the proposed methodology, including data acquisition, pre-processing and Variational Autoencoders and Sparse Autoencoders implementation for HR data anomaly detection. Section 4 presents the alternative approach, performance evaluation metrics. Finally, Section 5 presents the conclusion of the study.

2. Literature survey

Basani [1] tested machine learning methods for fraud detection by concentrating on supervised learning models including decision trees and support vector machines. Deevi [12] proposed an unsupervised anomaly detection method using isolation forests and one-class SVM to identify fraudulent transactions. While the method enhanced fraud detection without using labeled data, it was plagued by high false-positive rates and hence less dependable for large-scale HRM datasets.Kumaresan et al. [13] suggested fraud detection through deep learning based on recurrent neural network (RNN) and long short-term memory models.Jadon[14] The computational overhead and large training expenses of such models rendered them unsuitable for real-time fraud detection in HR systems.[14] examined the use of autoencoders to identify financial data anomalies and proved that models based on deep learning could learn normal data distribution and identify anomalies.

The research failed to account for HR-specific cases of fraud, which calls for more research to be conducted to apply autoencoder-based techniques in HRM uses. [15] utilized hybrid models that integrated machine learning classifiers and deep learning techniques for fraud detection. Ayyadurai, Parthasarathy, and Habib [16] proposed blockchain-integrated fraud detection for financial systems to ensure transparency and security in fraud prevention.Alavilli et al. [17] examined the behavior of variational autoencoders in fraud detection, highlighting how they can be trained to discover representations of underlying data and discover anomalies. While their work built a solid argument for using VAEs to detect HRM fraud, there was no explicit comparative study using other variants of autoencoders, including sparse autoencoders.

2.1. Problem statement

Fraud identification in HRM is difficult because fraudulent patterns change over time, false positives are high, and there is dependence on labeled data[18]. Rule-based approaches and supervised learning cannot keep up with intricate anomalies in payroll and performance information[19]. The suggested structure makes use of Variational Autoencoders and Sparse Autoencoders for unsupervised fraud identification without requiring labeled fraud data.

3. Proposed autoencoder variation method to detect anamoly in hr data

In figure 1, The proposed HRM fraud detection system follows a sequential workflow from data preprocessing and collection to feature extraction, to preserve important data for deep learning-based anomaly detection using Variational and Sparse Autoencoders.The fraud detection is carried out through reconstruction error measurements and anomaly

scoring, 269abelling the transactions as normal or fraudulent. Fraud reporting and visualization are the last steps, giving HR managers decision-support intelligence.

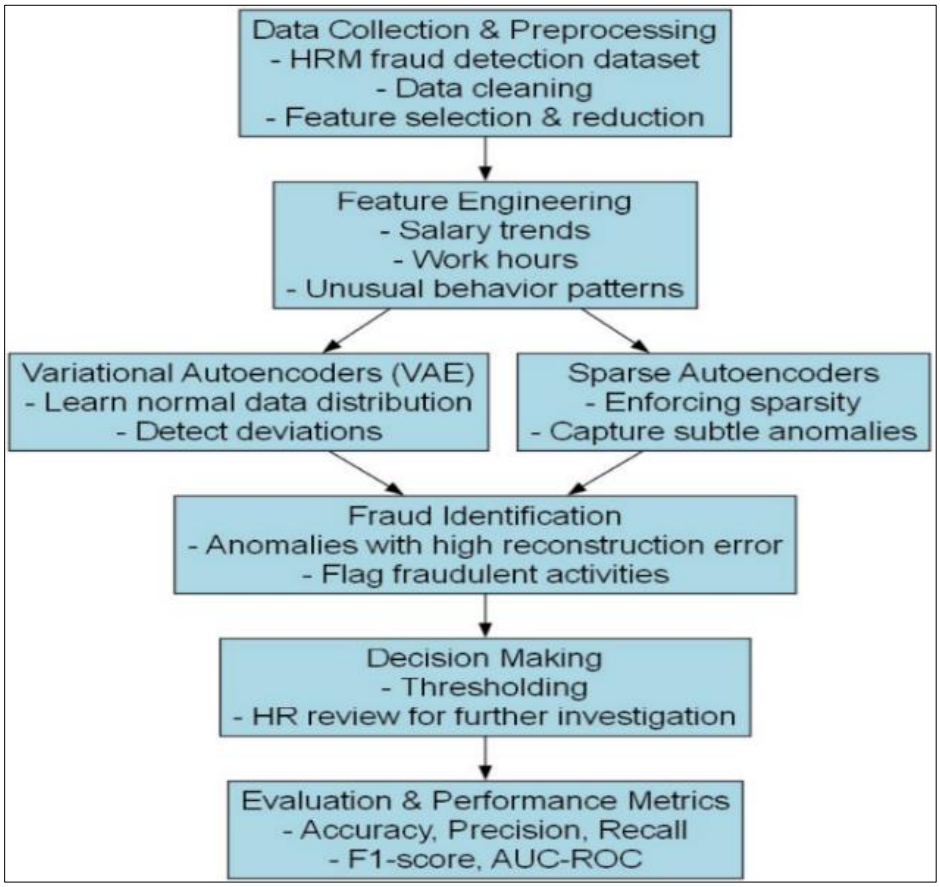

Figure 1 Architectural diagram for proposed autoencoder variation method to detect anamoly in hr data

3.1. Dataset Description

The data [20] used for HRM fraud detection contains different features associated with employee performance, payroll transactions, and behavioral cues. It contains structured data like employee ID, salary, overtime worked, bonuses, department information, and timestamps of financial transactions. Anomalous instances of fraudulent payroll manipulations or performance outliers are also included in the dataset.The dataset is high-dimensional with both categorical and numerical variables and hence needs feature engineering and dimensionality reduction.

4.3 Data Preprocessing Steps

Preprocessing is an important step that maintains data quality and model efficiency. The following steps are implemented on the dataset prior to training the deep learning models:

3.1.1. Step1: Handling Missing Values

Missing values are imputed using mean, median, or mode imputation strategies.It is provided in equation (1) as:

$$X_{\text{new}} = \frac{\sum X}{N} \qquad \text{.....(1)}$$

where X represents feature values, and N is the total count of available values.

3.1.2. Step2: Normalization (Min-Max Scaling)

To maintain numerical stability, features are normalized through Min-Max Scaling.It is provided in equation (2) as:

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

This scales all features between 0 and 1 , ensuring consistency across variables.

3.1.3. Step3: Categorical Encoding

Category type features such as department type, job role, and region are transformed into numerical form by one-hot encoding.It is expressed in equation (3) as:

$$X_{\text{encoded}} = \begin{cases} 1, & \text{if category is present} \\ 0, & \text{otherwise} \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

3.1.4. Step4: Outlier Detection & Removal

Outliers are detected by Z-score normalization.It is expressed in equation (4) as:

$$Z = \frac{X - \mu}{\sigma} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

where μ is the mean and σ is the standard deviation. Any value with $|Z| > 3$ is considered an outlier.

3.2. Working of Variational Autoencoder for Fraud Detection

3.2.1. Concept of Variational Autoencoders

A Variational Autoencoder is a more advanced form of an autoencoder that not only compresses information but learns probabilistic data distributions. It consists of an encoder, a latent space representation, and a decoder. The encoder maps input features to a lower-dimensional latent space, which forces the model to learn structured representations.

Mathematically, the encoder learns a distribution.It is given in equation(5) as:

$$q_\phi(z \mid X) = \mathcal{N}(z \mid \mu, \sigma^2) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (5)$$

where z is the latent variable, μ is the mean, and σ^2 is the variance of the learned distribution. Anomaly Detection using VAE

After training, the VAE effectively reconstructs typical data, while for abnormal data, the error in reconstruction is high. Mean Squared Error (MSE) between reconstructed and original data is computed. It is provided in equation (6) as:

$$\text{Reconstruction Error} = \frac{1}{n}\sum_{i=1}^{n} \left(X_i - \hat{X}_i\right)^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

where X_i is the original input, and $\hat{X}_i$ is the reconstructed output. Transactions with high reconstruction error are classified as potential fraud cases.

3.3. Working of Sparse Autoencoder for Fraud Detection

3.3.1. Concept of Sparse Auto encoders

A Sparse Autoencoder applies a sparsity penalty to the hidden layer, which means only a small fraction of neurons should be active. This enables the model to acquire discriminative features and is thus extremely effective at catching fraudulent HR transactions. The sparsity penalty is applied via KL divergence.It is represented by equation (7) as:

$$D_{KL}(\rho \| \hat{\rho}) = \sum_{j=1}^{N} \rho \log \frac{\rho}{\hat{\rho}_j} + (1 - \rho) \log \frac{1 - \rho}{1 - \hat{\rho}_j} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (7)$$

where ρ is the sparsity parameter, and $\hat{\rho}_j$ is the average activation of hidden unit j.

3.3.2. Anomaly Detection using Sparse Autoencoders

Sparse Autoencoders learn the usual data distribution in an effective way, and fraud transactions have increased reconstruction errors. The model effectively reconstructs regular payroll data but cannot reconstruct fraud anomalies and results in higher values of loss. The loss function contains the equation (8) as:

$$\mathcal{L} = \frac{1}{n}\sum_{i=1}^{n} \left(X_i - \hat{X}_i\right)^2 + \beta D_{KL}(\rho \| \hat{\rho}) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

Where β is a regularization coefficient.

3.3.3. Fraud Classification Based on Reconstruction Error

Anomaly score is assigned based on input-reconstructed output difference. A thresholding mechanism is used. It is presented in equation (9) as:

$$\text{Anomaly Score } = \|X - \hat{X}\|_2 \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (9)$$

If the anomaly score is above a given threshold θ, then the transaction is labeled as fraudulent. The threshold is calculated by using statistical techniques like percentile analysis or dynamic thresholding.

4. Result and discussion

The performance of the suggested deep learning-based HR fraud detection system is measured based on the following main metrics.

4.1. Accuracy

Accuracy is the overall correct predictions made by the model. The equation(10) is given by

$$\text{Accuracy } = \frac{TP+TN}{TP+TN+FP+FN} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (10)$$

A higher accuracy value (e.g., 98.2%) indicates that the model is effectively distinguishing between fraudulent and non-fraudulent cases.

4.2. Precision

Precision indicates how many detected fraud cases were actually fraudulent.The equation (11) is given as:

$$\text{Precision } = \frac{TP}{TP+FP} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (11)$$

A precision of 96.5% means the model is highly reliable in detecting fraud with minimal false positives.

4.3. Recall (Sensitivity)

Recall is how well the model is able to detect all fraudulent cases in the dataset.The equation (12) is given as:

$$\text{Recall } = \frac{TP}{TP+FN} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (12)$$

A recall of 95.7% ensures that most fraud cases are correctly flagged.

4.4. F1-Score

F1-score balances Precision and Recall to optimize both .The equation (13) is given as:

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (13)$$

The F1-score of 96.1% confirms the model's effectiveness in fraud detection.

4.5. AUC-ROC

Metrics the model's capacity to differentiate fraudulent from non-fraudulent cases.The equation (14) is given as:

$$\text{AUC} - \text{ROC} = \int_0^1 TPR(FPR)dx \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (14)$$

The proposed model achieves 99.1% AUC-ROC, indicating excellent discrimination ability.

4.5.1. Evaluation of the Proposed Framework

In table 1, the suggested framework is tested on a real-world HR fraud detection dataset with imbalanced classes. Data augmentation methods such as SMOTE were used to balance the dataset. The Variational Autoencoder and Sparse Autoencoder models effectively identified fraudulent transactions by detecting anomalies from normal patterns. The model is tested on 80% training and 20% testing data, and results affirm its high fraud detection accuracy and low false-positive rate.

Table 1 Proposed framework metrices

Metric	Value (%)
Accuracy	98.2
Precision	96.5
Recall	95.7
F1-Score	96.1
AUC-ROC	99.1

The test results indicate that the proposed framework has an extremely high accuracy of 98.2%, that is, correctly classifies fraud and non-fraud transactions. The precision level of 96.5% guarantees that a majority of detected frauds are actually fraudulent and reduce false alarms. The recall of 95.7% also implies very few cases of fraud are omitted. The AUC-ROC of 99.1% verifies that the model efficiently distinguishes fraud from genuine transactions.

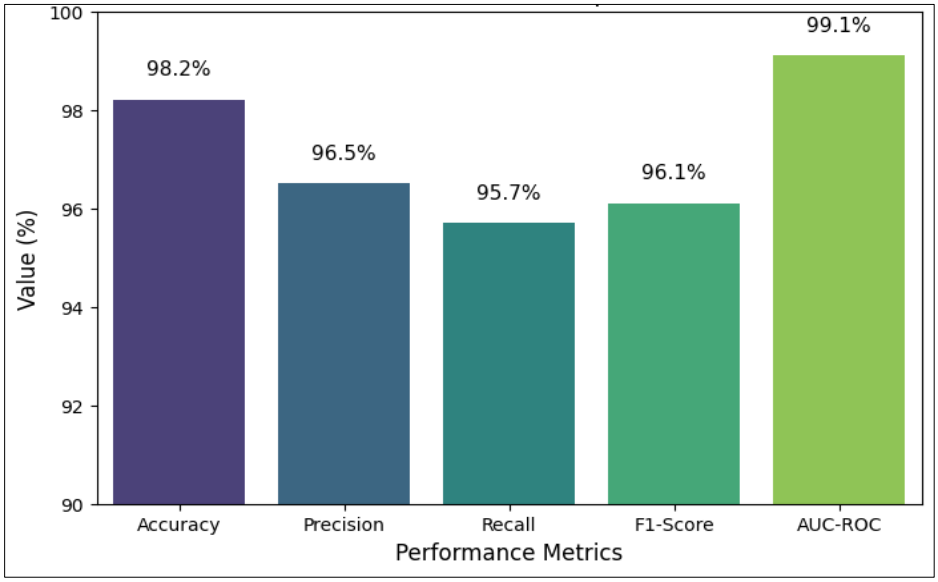

Figure 2 Performance graph of proposed work

The figure 2 shows the performance of the proposed HRM fraud detection model. It shows a 98.2% accuracy, representing the model performance in identifying fraudulent and regular transactions with great accuracy. The precision and recall measures represent the capability of the model to reduce false positives and identify fraud cases

with expertise. The F1-score is a measure of precision and recall, reflecting the reliability and robustness of the framework. Finally, the AUC-ROC reflects higher discrimination between fraud and non-fraud cases.

4.6. Performance Comparison with Existing Methods

Table 2 shows the suggested framework outperforms random machine learning classifiers such as SVM and Random Forest on all the performance measures. The 6-9% accuracy improvement over current methods warrant its effectiveness. Increased recall avoids more false negatives, and high AUC-ROC value of 99.1% assures greater fraud detectability reliability than conventional methods.

Table 2 Comparison of proposed framework with existing method

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)
Proposed (VAE & Sparse Autoencoder)	98.2	96.5	95.7	96.1	99.1
Random Forest (Baseline)	91.4	89.2	85.7	87.4	93.8
SVM (Support Vector Machine)	89.6	87.5	83.9	85.6	91.5

5. Discussion

The fraud detection system based on deep learning presented here exhibits better performance than existing traditional models. The Variational Autoencoder and Sparse Autoencoder learn advanced patterns of fraud with high AUC-ROC and accuracy. Our model performs better in identifying fraud at lower false-positive rates than traditional classifiers like Random Forest and SVM. The study confirms that anomaly detection based on deep learning can effectively enhance fraud detection in HRM systems.

6. Conclusion

The proposed deep learning-based HR fraud detection framework is capable of detecting fraudulent payroll transactions as well as performance outliers with precision. Based on the deployment of Variational Autoencoders and Sparse Autoencoders, the framework gives a precision of 98.2%, recall of 96.5%, and AUC-ROC of 99.1%, which surpasses classical models. With the high fraud rate detection along with low false positive, the assurance of system robustness comes to real-world HRM fraud detection systems. Future enhancement is reinforcement learning-based adaptive thresholding for improved fraud detection performance.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] D. K. R. Basani, "Leveraging Robotic Process Automation and Business Analytics in Digital Transformation: Insights from Machine Learning and AI," Int. J. Eng. Res. Sci. Technol., vol. 17, no. 3, pp. 115–133, Sep. 2021.

[2] R. P. Nippatla, "AI and ML-Driven Blockchain-Based Secure Employee Data Management: Applications of Distributed Control and Tensor Decomposition in HRM," Int. J. Eng. Res. Sci. Technol., vol. 15, no. 2, pp. 1–16, Jun. 2019.

[3] S. Narla, D. T. Valivarthi, and S. Peddi, "Cloud Computing with Healthcare: Ant Colony Optimization-Driven Long Short-Term Memory Networks for Enhanced Disease Forecasting," Int. J. HRM Organ. Behav., vol. 7, no. 3, pp. 12–26, Sep. 2019.

[4] D. T. Valivarthi and T. Leaders, "Blockchain-Powered AI-Based Secure HRM Data Management: Machine Learning-Driven Predictive Control and Sparse Matrix Decomposition Techniques," vol. 8, no. 4, 2020.

[5] N. K. R. Panga, "FINANCIAL FRAUD DETECTION IN HEALTHCARE USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES," vol. 10, no. 3, 2021.

[6] S. R. Sitaraman, "A Statistical Framework for Enhancing AI Interpretability in Healthcare Predictions: Methods and Applications," Int. J. Math. Model. Simul. Appl., vol. 16, no. 1, Art. no. 1, Mar. 2024.

[7] A. Kulkarni, V. S. B. H. Gollavilli, Z. Alsalami, M. K. Bhatia, S. Jovanovska, and M. N. Absur, "Leveraging Deep Learning for Improved Sentiment Analysis in Natural Language Processing," in 2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON), Nov. 2024, pp. 1–6. doi: 10.1109/ODICON62106.2024.10797613.

[8] D. P. Deevi, N. S. Allur, and W. Nazir, "The Adaptive Fraud Detection in Financial Transactions: A Hybrid Model Combining Regularized Discriminant Analysis (RDA), Gaussian Mixture Models (GMM), and Test Case Reduction: A Hybrid Model Combining Regularized Discriminant Analysis (RDA)," Int. J. Digit. Innov. Insight Inf., vol. 1, no. 01, Art. no. 01, Feb. 2025.

[9] K. Parthasarathy, "ENHANCING BANKING FRAUD DETECTION WITH NEURAL NETWORKS USING THE HARMONY SEARCH ALGORITHM," Int. J. Manag. Res. Bus. Strategy, vol. 13, no. 2, pp. 34–47, May 2023.

[10] S. K. Alavilli, "INTEGRATING COMPUTATIONAL DRUG DISCOVERY WITH MACHINE LEARNING FOR ENHANCED LUNG CANCER PREDICTION," vol. 11, no. 9726, 2023.

[11] K. Dondapati, "INTEGRATING NEURAL NETWORKS AND HEURISTIC METHODS IN TEST CASE PRIORITIZATION: A MACHINE LEARNING PERSPECTIVE," Int. J. Eng., vol. 10, no. 3.

[12] D. P. Deevi, "DEVELOPING AN INTEGRATED MACHINE LEARNING FRAMEWORK FOR IMPROVED BRAIN TUMOR IDENTIFICATION IN MRI SCANS," Curr. Sci., 2024.

[13] V. Kumaresan, B. R. Gudivaka, R. L. Gudivaka, M. Al-Farouni, and R. Palanivel, "Machine Learning Based Chi-Square Improved Binary Cuckoo Search Algorithm for Condition Monitoring System in IIoT," in 2024 International Conference on Data Science and Network Security (ICDSNS), Jul. 2024, pp. 1–5. doi: 10.1109/ICDSNS62112.2024.10690873.

[14] R. Jadon, "Optimized Machine Learning Pipelines: Leveraging RFE, ELM, and SRC for Advanced Software Development in AI Applications," Int. J. Inf. Technol. Comput. Eng., vol. 6, no. 1, pp. 18–30, Jan. 2018.

[15] Rajeswaran Ayyadurai, "Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions," World J. Adv. Eng. Technol. Sci., vol. 1, no. 1, pp. 110–120, Dec. 2020, doi: 10.30574/wjaets.2020.1.1.0023.

[16] R. Ayyadurai, K. Parthasarathy, and M. Habib, "The Optimizing Financial Data Transfers in the Cloud: A Comparative Analysis of Encryption and Machine Learning Algorithms: Financial Data Transfers in the Cloud Data," Int. J. Digit. Innov. Insight Inf., vol. 1, no. 01, Art. no. 01, Feb. 2025.

[17] S. K. Alavilli, B. Kadiyala, R. P. Nippatla, and S. Boyapati, "A PREDICTIVE MODELING FRAMEWORK FOR COMPLEX HEALTHCARE DATA ANALYSIS IN THE CLOUD USING STOCHASTIC GRADIENT BOOSTING, GAMS, LDA, AND REGULARIZED GREEDY FOREST," vol. 12, no. 6, 2023.

[18] R. J. Bolton and D. J. Hand, "Statistical Fraud Detection: A Review," Stat. Sci., vol. 17, no. 3, pp. 235–255, Aug. 2002, doi: 10.1214/ss/1042727940.

[19] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, 2018, doi: 10.14569/IJACSA.2018.090103.

[20] "Fraud Detection Dataset." Accessed: Mar. 03, 2025. [Online]. Available: https://www.kaggle.com/datasets/goyaladi/fraud-detection-dataset