OPEN ACCESS

ISSN: 2996-4954

Yudhveer K, et al. (2023) 161-169
J Contemp Edu Theo Artific Intel: 2023(5):100111
DOI: 10.71010/2996-4954/JCETAI-e111

Research Article

Journal of Contemporary Education Theory & Artificial Intelligence

An Analytical Study of ML Models for Behavioral Analytics in Catching Suspicious Payroll Activity

Yudhveer Kandukuri[1], Bose babu Ravula[2], Sojy John[3], Naveen Shrivastava[4], Mahesh Marri[5]

[1]G2 Web Services - Open Source DBA & DevOps, veer.sqldba@gmail.com
[2]John Wiley &Sons, Inc., Principal, bbravula@icloud.com
[3]Recreational Equipment, Inc - Technology Lead, DevOps Engineer & Cloud Migration., sojy.john@gmail.com"
[4]T-Mobile Salesforce Lead Developer, lalausa03@gmail.com
[5]Amazon Web Services, Senior Electrical Engineer, saimaheshmarri@gmail.com

[*]**Corresponding author:** Yudhveer Kandukuri

Citation: Yudhveer K, Bose babu R, Sojy J, Naveen S, Mahesh M (2023) An Analytical Study of ML Models for Behavioral Analytics in Catching Suspicious Payroll Activity. J Contemp Edu Theo Artific Intel: ICETAI-111.

Received Date: 12 November, 2023; **Accepted Date:** 18 November, 2023; **Published Date:** 25 November, 2023

Abstract

Payroll fraud has been among the most rampant financial threats to organizations that have a direct impact on how organizations remunerate their employees, and this kills confidence in the institutions. The traditional rule-based detection mechanisms employed often fall short when addressing the dynamic and evolving nature of fraud. An analytical study of machine learning models used within a behavioral analytics framework to identify suspicious payroll activity. Behavioral analytics can be used to identify abnormal behavior in the payroll by modeling normal payroll conduct based on historical, contextual, and temporal data, it can indicate abnormal compensation patterns, unusual payment time-frames, role-based access violations, and mismatches between attendance and compensation and abnormal compensation patterns. The research effectively compares and approaches supervised, unsupervised, and DL techniques. The analysis of feature extraction and behavioral indicators will demonstrate that ML models can increase detection rates and minimize false positives. The point is that ML-based behavioral analytics is a scalable, flexible, and proactive solution for detecting payroll fraud. This critical assessment provides information on model security, operational issues, and real-world implementation issues for intelligent and secure payroll monitoring systems.

Keywords: *Behavioral Analytics, Payroll Fraud Detection, Machine Learning, Financial Security, Payroll Monitoring Systems*

I. Introduction

Organizational financial management depends on payroll systems that deal with employee compensation and benefits, as well as regulatory compliance[1][2]. As a result of increased use of digital payroll and enterprise resource planning systems, payroll activities are currently generating vast amounts of transactional and employee-related information [3]. Although it has increased efficiency and accuracy, it has also broadened the scope of payroll fraud and suspicious activity, including ghost workforce, unauthorized salary changes, and overtime manipulation [4]. Conventional payroll control systems based on fixed rules and periodic audits generally cannot handle the volume and complexity of present-day payroll data.

Behavioral analytics has become a more flexible, data-driven method for monitoring payroll [5]. Behavioral analytics shifts the emphasis from single transactions to behavioral patterns over time, and from modelling normal payroll behavior for employees, roles, and departments [6]. This strategy enables organizations to uncover previously unnoticed and evolving forms of payroll misconduct by setting behavioral standards and tracking employees who deviate from established behavioral norms. The success of behavioral analytics, however, largely depends on the ability to learn and interpret sophisticated behavioral patterns in payroll data.

Machine learning methods are essential for enhancing behavioural analytics, enabling automatic pattern discovery and adaptive learning. Supervised learning models benefit from detecting known instances of fraud when labeled data are available. In contrast, unsupervised and semi-supervised methods can detect previously unknown anomalies without clearly defined labels indicating whether the data are fraudulent. Furthermore, deep learning models, including autoencoders and recurrent neural networks, can learn complex, nonlinear, and temporal dependencies in payroll data. All these features enable machine learning-based systems to keep up with changes in payroll practices, the workforce, and fraud strategies, thereby enhancing detection accuracy and resilience. In practice, data imbalance, feature selection, model interpretability, scalability, and concept drift have a significant impact [7]. Various machine learning models have different strengths and weaknesses based on the features of payroll data and operational limitations [8] [9]. Consequently, an analytical study should be conducted systematically to determine the effectiveness of ML models in behavioural analytics for detecting suspicious payroll activity.

A. Structure of the Paper

This paper is organized as follows: Section II payroll activity and suspicious activity analysis. Section III Behavioral analytic framework for payroll monitoring Section IV. Machine learning model for behavioral analysis. The literature review is presented in Section V, and the conclusions and prospective research are discussed in Section VI.

II. Payroll Fraud and Suspicious Activity Analysis

A payroll is the procedure that an organization undergoes to compensate its employees. It encompasses information regarding the salaries, deductions, bonuses, and income of employees. Payroll fraud and suspicious activity analysis involve detecting anomalies in payroll operations that can lead to financial loss, compliance breaches, or inefficient operations. With payroll systems becoming more digital and integrated enterprise applications to improve efficiency and usability, fraudsters have also escalated and become harder to spot. This analyzes the character, trends, and payroll fraud that shape sophisticated behavioral analytics and machine learning-based detection strategies.

A. Types of Payroll Fraud

Payroll fraud, also called "payroll manipulation" is when someone changes a payroll system to get more money for themselves or someone else. Falsifying timesheets, awarding bonuses without authorization, or paying fake or terminated employees are all examples of payroll fraud that either employers or employees can perpetrate. The various forms of payroll fraud are illustrated in Figure 1:

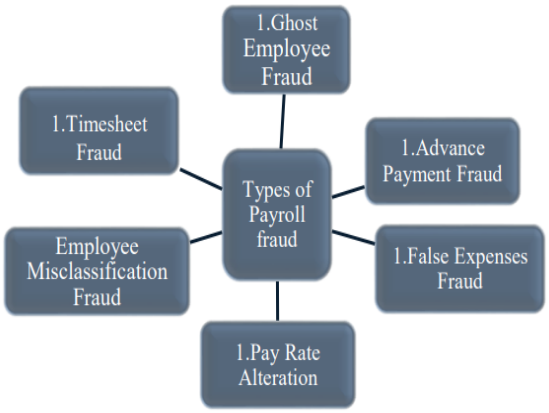


Fig 1: Types of Payroll Fraud.

1) Ghost Employee Fraud

The technique of manipulating payroll funds by fabricating an employee is known as "ghost employee fraud". There are two probable explanations: either the employee was formed with the deliberate goal of committing fraud, or the payroll account of a past employee is preserved and exploited for this reason all situations, an employee with access to the payroll system inside the firm is the one who commits this kind of payroll fraud. This is within the purview of human resources for the majority of firms, particularly larger ones.

2) Timesheet Fraud

When workers are compensated for hours they did not actually work, it is known as timesheet theft[10]. An employee who punches in early and punches out late to give the appearance of working longer hours is a common perpetrator of this. Maybe another worker is in on it the payroll clerk is a potential target for timesheet fraud.

3) Employee Misclassification Fraud

Employers engage in worker misclassification fraud when they misclassify an individual as neither an employee nor an independent contractor to avoid paying taxes on payroll, workers' compensation, and unemployment.

4) Pay Rate Alteration

A person's pay is altered so that they receive a higher hourly wage than they truly merit. An employee may make a mistake and be unaware of it; the payroll system is typically required, and staff members go on to cover their traces. Any anomalies detected in the payroll data should be thoroughly when one suspected this sort of payroll fraud.

5) False Expenses Fraud

Fraudulent claims concerning expenses they shouldn't be receiving are made by an employee. Employees can either make up full expense reports or mislead when the actual cost to make money is high. Organizations should have the required documentation for any reported expenses, including a receipt, proof of payment, and other relevant information.

6) Advance Payment Fraud

Payroll fraud occurs when an employee misuses an advance payment option. So, the worker essentially requests and receives an advance payment, but they never repay it. People that don't pay back an advance payment are typically guilty of this offence.

7) Impact of Payroll Fraud

Payroll fraud is a serious problem that can take various forms, ranging from ghost workers (individuals listed on the payroll who do not exist) to fabricated hours, inflated salaries, and unauthorised bonuses [11][12]. These fraudulent acts may lead to considerable financial losses, destroy confidence within the business, and damage its image in the industry, possibly generating long-term harm that extends beyond the financial effect as depicted in Figure 2

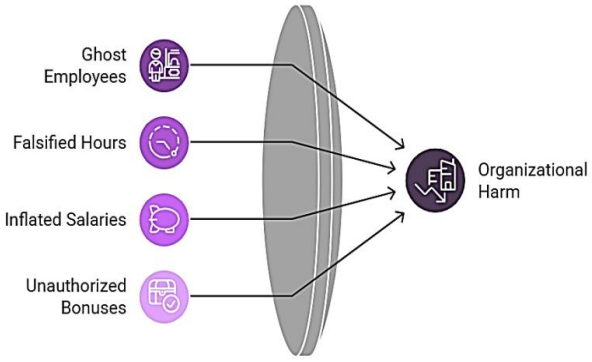


Fig 2: FImpact of Payroll Fraud.

Conventional approaches to identifying and avoiding payroll fraud often depend on rule-based systems, periodic human audits, or the ever-evolving strategies used by fraudsters. Traditional approaches to monitoring and identifying fraudulent activity are becoming increasingly inadequate as organisations expand and payroll data complexity increases [13]. Fraudsters often find ways to modify payroll data unnoticed, exploiting flaws in outdated systems that cannot keep up with the demands of current payroll operations.

C. Characteristics of Suspicious Payroll Activity

Suspicious payroll activity is defined as the deviation from the usual payroll behavior that could be an indication of possible fraud, abuse, or irregularity of the system. These are usually latent and spread across multiple payroll features, so early detection is critical for minimizing risks. Show in Characteristics of Suspicious Payroll Activity Figure 1.

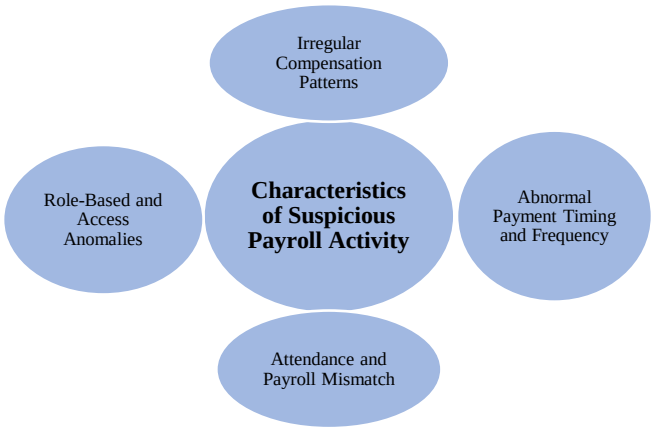


Fig 3: Characteristics of Suspicious Payroll Activity.

- **Irregular Compensation Patterns:** Suspicious payrolls will be magnified by unusual modifications of salary, bonuses or incentives. Abrupt salary increases, unapproved regular salary increases, or pay rates that are not in line with the job position can indicate unauthorized changes or insider abuse in the payroll system.
- **Abnormal Payment Timing and Frequency:** The payroll transactions usually have pre-defined cycles like monthly or biweekly. The presence of payments that are not made during the cycles, recurring off-cycle disbursements or multiple payments in a pay period may also reflect duplicate payments, misuse of the system or an attempt to hide fraudulent transactions.
- **Attendance and Payroll Mismatch:** The differences in the recorded attendance and payroll payments are not an exception to this type of suspicious activity. Examples include full payment of salary even during prolonged absence, excessive overtime without equivalent work hours, or compensation issued to non-existent or inactive employees, often related to ghost employee fraud.
- **Role-Based and Access Anomalies:** The payroll conduct has strong associations with roles and permissions of the employees. Such suspicion can be created by unusual compensation habits that do not correspond to the norms of the role or by the unwarranted entry of the bank or approval of payroll transactions by unauthorized persons. These irregularities are likely to show control bypass, privilege abuse, or insider threats during payroll operations.

D. Need for Analytical and Behavioral Approaches in Payroll Monitoring

The conventional modes of payroll tracking are rule-based audits and periodic checks and these methods are not effective in identifying the complex and dynamic fraud patterns that happen in the modern payroll systems[14]. Because payroll data are larger and more dynamic, suspicious activities are often manifested through deviant behavioral patterns rather than as explicit rule breaches. A behavioral approach models normal payroll behavior and detects anomalies based on patterns, trends, and contextual relationships among employees, roles, and times. These methods can detect known and previously unseen payroll fraud in continuous, adaptive, and more accurate ways by leveraging machine learning and behavioral analytics, as shown in Table I, while minimizing false positives and improving the overall effectiveness of payroll monitoring.

TABLE 1: COMPARISON OF ANALYTICAL AND BEHAVIORAL APPROACHES IN PAYROLL MONITORING.

Aspect	Traditional Approach	Analytical & Behavioural Approach
Detection Method	Rule-based and threshold checks	Behaviour-based pattern analysis
Fraud Coverage	Detects known fraud types only	Detects known and unknown fraud
Adaptability	Static and manually updated	Adaptive and self-learning
Data Handling	Limited data analysis	Handles large, complex payroll data
Accuracy	High false positives	Improved accuracy and precision
Response Time	Periodic audits	Continuous and real-time monitoring

III. Behavioral Analytics Framework for Payroll Monitoring

Behavioral analytics offers a data-driven method for detecting suspicious payroll behavior by modeling normal payroll and employee behavior and identifying deviations. Behavioral analytics uses machine learning to continuously learn, evolve, and identify sophisticated fraud patterns in payroll transactions, unlike rule-based systems.

A. Behavioral Modeling in Payroll Systems

In payroll systems, behavioral modeling is the systematic expression of normal and abnormal employee payroll behavior using historical, contextual, and temporal data from payroll transactions that are characteristic of the system and occur regularly, and to detect insidious irregularities that could indicate fraudulent or suspicious behavior [15]. Behavioral models are more dynamic and adaptive to changing workforce and payroll practices, unlike fixed rule-based mechanisms, as shown in Figure 4.

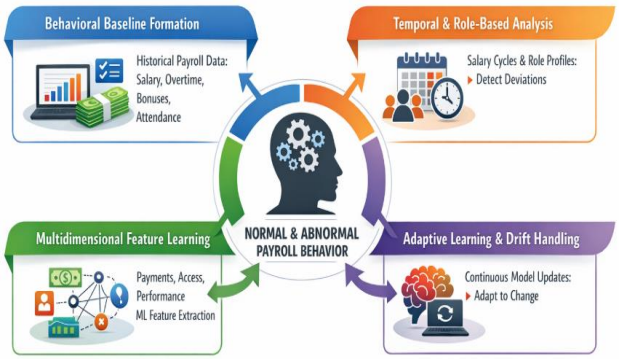


Fig 4: Behavioral Modeling in Payroll System.

- **Behavioral Baseline Formation:** Formation of the Baseline Behaviors: It starts with behavioral modeling of the normal payroll conduct based on historical information, such as value of salaries paid, the trend of overtime, bonuses and attendance [16]. These are built at the employee, position, and department levels to depict desired payroll behavior.
- **Temporal and Role-Based Behavior Analysis:** Payroll behavior does fluctuate and depend on time and position in the organization[17]. Temporal modeling is used to model periodic salary cycles and non-regular payment times,

whereas role-based profiling is used to model anticipated compensation patterns. The non-observation of these patterns is a sign of possible suspicious behavior.

- **Multidimensional Feature Learning:** Multidimensional behavioral models combine several aspects of payment, frequency, access right and performance measures. Machine learning converts these features to behavioral representations that have the potential to identify complex, non-linear patterns of fraud.
- **Adaptive Learning and Drift Handling:** Payroll behavior changes over time as a result of policy changes and workforce activities[18]. Behavioral models are always up-to-date, so they can be retrained and learn with time, and hence prevent false positives with proper detection.

B. Feature Extraction and Behavioral Indicators

Behavioral analytics in payroll monitoring involves feature extraction, which transforms raw payroll data into meaningful behavioral indicators. Factors such as salary levels, payment frequency, overtime use, bonuses, attendance history, job descriptions, access to historical activities, and time-series trends are used to model normal payroll behavior [19]. Any deviation from these acquired patterns, such as non-payment, distorted compensation arrangements, or non-correspondence between pay and performance, is considered a sign and symptom of suspicious conduct. These features can be extracted to effectively identify payroll fraud and anomalous procedures using machine learning models, with higher accuracy and fewer false positives, as indicated in Table II.

TABLE II: FEATURE EXTRACTION AND BEHAVIORAL INDICATORS FOR PAYROLL MONITORING.

Feature Category	Extracted Features	Behavioural Indicators	Suspicious Activity Detected
Salary Attributes	Basic salary, net pay, gross pay, salary increments	Sudden salary spikes, unusual increments	Salary inflation, unauthorized pay raises
Payment Frequency	Number of payments per cycle, off-cycle payments	Abnormal payment timing, repeated payments	Duplicate or early payroll transactions
Overtime Patterns	Overtime hours, overtime pay rate	Excessive or inconsistent overtime claims	Overtime abuse, policy violations
Bonus and Incentives	Bonus frequency, bonus amount, incentive approvals	Irregular bonus distribution	Unauthorized or inflated bonuses
Attendance Behavior	Work hours, leave records, absenteeism rate	Mismatch between attendance and pay	Ghost employees, false attendance
Role-Based Features	Job role, designation level, department	Pay inconsistency with role	Role-based payroll manipulation
Access and Approval Logs	Payroll access frequency, approver identity	Self-approval, unusual access times	Insider fraud, access misuse
Performance Metrics	Productivity scores, KPIs	High compensation with low performance	Performance-pay mismatch
Temporal Features	Payroll date, pay cycle, seasonal trends	Off-cycle or irregular timing	Suspicious transaction timing
Behavioral Deviation Scores	Anomaly score, reconstruction error	High deviation from baseline behaviour	Potential payroll fraud

C. Key Benefits of AI-Powered Payroll Fraud Detection

Several advantages are offered by AI-driven payroll fraud detection systems that substantially improve precision, effectiveness, and efficiency of identifying and preventing payroll fraud. These systems provide a more proactive, dynamic, and real-time alternative to conventional methods of fraud detection. Figure 5 shows the main advantages of using AI to identify payroll fraud in organizations.

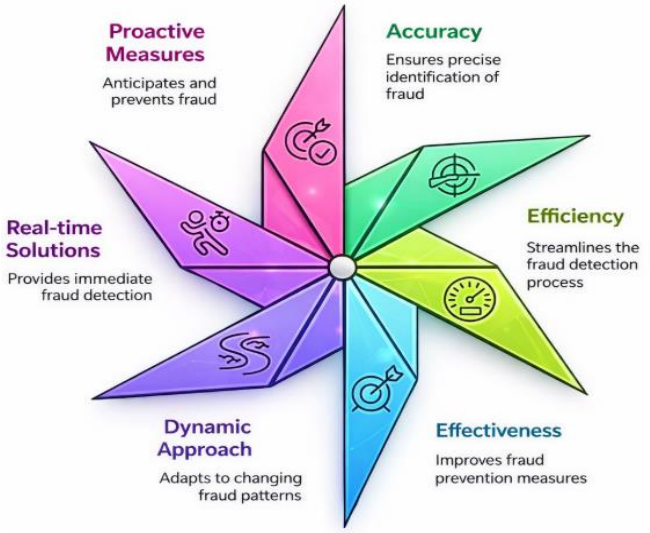


Fig 5: Enhancing Payroll Fraud Detection with AI.

D. Increased Accuracy and Efficiency

AI-powered systems significantly increase the efficiency and accuracy of payroll fraud detection. Traditional methods typically rely on routine manual audits, which can be time-consuming, error-prone, and unable to keep pace with the increasing complexity and breadth of modern payroll systems [20]. These human procedures are limited in their capacity to identify small errors or abnormalities that may indicate fraud. When a previously undiscovered fraudulent action or method is used, AI models may evolve, recognising new patterns of suspicious behaviour and increasing detection rates.

E. Real-Time Fraud Prevention

The capacity of real-time fraud prevention with AI-powered payroll fraud detection. Annual audits and end-of-cycle reviews, both traditional fraud-detection activities, usually provide useful information. Preventing fraud from manipulating payroll systems, which can lead to substantial financial losses and wasted time and resources in attempting to fix the fraudulent conduct, is crucial for organisations to reduce their risk exposure and avoid large-scale financial harm.

F. Proactive Fraud Detection

A proactive AI solution can alert HR or payroll teams to suspicious behaviours, enabling them to investigate and take appropriate action before any fraudulent payments are executed [21]. This predictive capability suggests that organisations are no longer required to wait for fraud to occur before taking action. AI protects the business from costly errors and damage to its financial stability, keeping it one step ahead of offenders.

G. Cost Savings and Operational Efficiency

AI-powered payroll fraud detection solutions can lead to substantial cost savings for your organization. Traditional fraud detection methods may require significant manual labour, including analyzing payroll data, examining transactions, and investigating inconsistencies. AI technologies can help organizations reduce the costs associated with fraud, in areas such as:

- Financial losses due to unapproved bonuses, ghost workers, and overpayments.
- The reputational damage that is associated with a fraud case that has been identified.
- Legal repercussions or penalties that result from noncompliance with regulatory standards.

H. Scalable Fraud Detection Across Large Organizations

AI-driven payroll fraud detection solutions are highly scalable, making them suitable for enterprises of any size. The growing volume of transactions and the diversity of payroll arrangements between nations and currencies may be a significant challenge for major organisations with global workforces and complex payroll data when using standard fraud detection systems.

IV. Machine Learning Models for Behavioral Analysis

Three primary methodologies can be used to systematically categorise ML approaches for fraud detection: supervised, unsupervised, and DL [22]. Each technique provides various benefits and disadvantages based on the particular fraud detection situation and accessible data features in indicated in Figure 6.

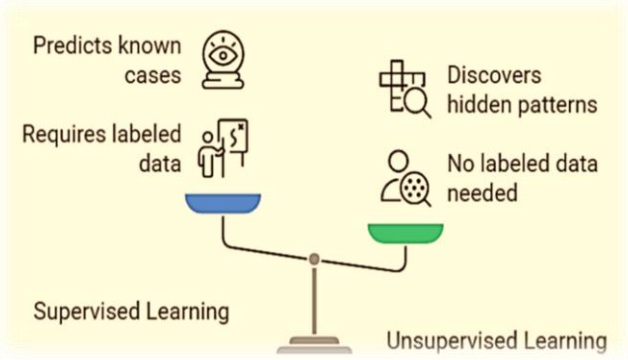


Fig 6: Supervised and Unsupervised Learning Approach.

A. Supervised Learning

The most common method for detecting fraud is supervised learning. Models are trained on painstakingly annotated datasets that clearly label transactions as either fraudulent or lawful, enabling the computer to identify discriminative patterns.

1) Random Forest (RF)

The most widely used supervised technique for fraud detection is RF. By combining several decision trees, this ensemble approach successfully reduces overfitting tendencies while increasing classification accuracy. RF models have consistently demonstrated high accuracy in identifying financial statement and credit card fraud.

2) Logistic Regression (LR)

The interpretability and simplicity of Logistic Regression. It forecasts the likelihood of a fraudulent transaction by analysing its feature properties. LR demonstrated exceptional performance on binary classification tasks commonly used in fraud detection.

3) Support Vector Machine (SVM)

Support Vector Machines divide data points along a hyperplane that maximises the margin between different classes. SVM works well for both linear and nonlinear classification using a variety of kernel functions, making it appropriate for a range of fraud detection tasks.

B. Unsupervised Learning

Unsupervised learning methods are used crudely. These algorithms identify patterns and anomalies without requiring labelled training data, making them especially efficient at detecting new fraud patterns that may not be reflected in previous labelled datasets.

1) Isolation Forest

An isolation forest is formed, which separates observations by randomly selecting features and split values between their maximum and minimum. It is especially beneficial for spotting anomalies, which often signify fraudulent transactions.

2) Autoencoder

Autoencoders depict neural networks that train to compress and reconstruct data, with reconstruction errors serving as anomaly scores. They are especially beneficial for reducing dimensionality and discovering intricate patterns in transaction data.

3) K-Means Clustering

K-means, which splits data into k clusters and assigns each observation to the cluster with the closest mean, can be used to detect clusters of linked transactions; transactions that fall outside established groupings may indicate fraudulent behaviour.

C. Deep Learning Approaches

Deep learning algorithms are a rapidly evolving area of fraud detection. These intricate approaches may be used alone or in conjunction with traditional ML techniques.

1) Long Short-Term Memory (LSTM)

LSTMs are certain forms of RNN capable of learning long-term associations in data via internal mechanisms called gates that govern information flow valuable for analysing sequential transaction data, identifying temporal trends that may expose fraudulent behaviour.

2) Convolutional Neural Networks (CNNs)

CNNs are a valuable tool for detecting deception in structured data. The primary concept is to view organised financial data as a grid, akin to a photograph, and to apply convolutional filters (kernels) to it. They automatically learn hierarchical features from data, with the first layer capturing basic patterns and successive layers combining them to discover more complex associations, which is critical for detecting sophisticated fraud practices.

3) Generative Adversarial Networks (GANs)

GANs consist of a generator and a discriminator. GANs can generate synthetic fraud samples to enhance fraud-detection classifier training, which is especially useful.

D. Challenges of AI in Proactive Payroll Fraud Prevention

Although AI has proven tremendous potential in identifying and preventing payroll fraud, some important difficulties remain that restrict its general use in enterprise payroll systems as outlined below:

1) Data Scarcity and Imbalance: Payroll fraud instances

Represent a very small fraction of total payroll transactions. This class imbalance makes it difficult for supervised models to learn representative patterns, often resulting in a bias toward the majority (non-fraud) class [23]. Moreover, the lack of publicly available payroll fraud datasets, due to privacy, secrecy, and compliance requirements, leads researchers to rely on proxy datasets or synthetic data, which limits external validation and repeatability.

2) Privacy and Regulatory Constraints:

Payroll data comprises highly sensitive information, including salary details, employee IDs, and banking records [24]. The use of such data for training AI models is restricted by privacy restrictions such as GDPR and HIPAA. Ensuring data confidentiality, anonymisation, and compliance while still enabling effective model training is a substantial challenge, especially for cross-organisational fraud detection.

3) Concept Drift and Adaptive Fraud Strategies:

Fraudsters regularly refine their tactics to evade detection mechanisms [25]. Static AI models decline in performance over time as fraud patterns shift, a process called notion drift. Without adaptive or incremental learning methodologies, proactive payroll fraud detection systems risk becoming outdated, resulting in more false negatives.

4) Explainability and Trust Issues

Many high-performing AI models behave as “black boxes,” providing minimal interpretability. In payroll fraud prevention, investigators and auditors want clear reasons behind anomaly flags to start disciplinary or legal action sophisticated AI models in compliance-driven environments.

5) Integration with Legacy Payroll and ERP Systems

Organisations commonly use diverse, outdated payroll management systems that are not suited to real-time AI integration. Embedding advanced anomaly detection models into these procedures requires significant infrastructure changes, increasing implementation costs and technical challenges.

V. Literature Review

This section reviews prior work on advances in machine learning based suspicious payroll activity. Table III summarizes key studies, highlighting their focus, findings, challenges, and future directions.

Thirusubramanian Ganesan et al., (2025 payment fraud and performance irregularities will cause inefficiency and loss. An HRM data anomaly detection system based on DL that incorporates Variational Autoencoders and Sparse Autoencoders is relied upon since traditional fraud detection methodologies fail to identify complicated data patterns. The system learns typical patterns in payroll transactions and employee performance metrics from a dataset used for fraud detection. The model identifies anomalies as instances of fraudulent behaviour or substantial reconstruction flaws. Additionally, the method improved the validity of fraud detection by revealing, at least to some extent, embedded patterns in HR data [26].

Bamiduro, (2025) AI technologies are revolutionising payroll administration systems AI-driven payroll solutions. AI dramatically enhances automation, accuracy, and compliance, while also improving data security through modern methods such as ML, robotic process automation, and blockchain integration. Nevertheless, given the high costs, regulatory complexity, and ethical problems, a comparative approach provides real guidelines for organisations wishing to apply AI ethically and effectively in payroll management [27].

Saha, (2025) AI strategies to forecast and prevent payroll fraud within ERP systems. To identify irregularities, anomalies, and suspicious activity that might indicate fraud, AI's data analysis, pattern recognition, and anomaly detection capabilities are applied to historical payroll data. Various ML techniques, including supervised and unsupervised learning methods, are useful for predicting payroll fraud. In contrast to unsupervised models such as clustering and anomaly detection algorithms, supervised models such as decision trees and RF are used to categorise fraud cases based on labelled training data. Furthermore, the integration of Natural Language Processing (NLP) within ERP systems enhances the ability to detect fraudulent behaviours by analysing text-based data such as emails and personnel communications [28].

Singireddy (2024) Reports That Advanced deep learning algorithms are used to automatically identify fraudulent activity in payroll and financial management systems. Computers do the hard work in identifying patterns, gaining insights, making decisions, and taking action; nevertheless, when trained only on genuine transaction data, models are unable to assess or forecast fraud. The literature describes a self-training active-learning ensemble of models that utilise transaction authentication data. The system directly exploits fraud tendencies in a data source that is primarily unlabelled and requires minimal retraining when a pattern changes [29].

Enokkaren et al., (2024) payroll systems are becoming more and more digitalised and financial transactions are becoming difficult to manage, more intelligent and adaptive solutions are urgently a the types of payroll fraud, traditional methods for detecting and preventing such fraud, and the role of AI and ML in enhancing the capacity to detect fraud supervised and unsupervised frameworks in reinforcement learning and deep learning for identifying anomalies and patterns in payroll data. such as applying solid internal controls, offering employee training, and adopting cybersecurity measures are regarded complementary solutions the absence of data, privacy concerns, idea drift, explainability, and compatibility with legacy systems to deliver AI-based solution[30].

Ravichandran, Inaganti and Muppalaneni (2023), The application of AI and ML to improve payroll fraud detection within HR systems methodology, beginning with data collection and continuing through model training, anomaly detection, and automated fraud response mechanisms, is a huge step forward in protecting organisations' financial integrity from this growing problem. Organisations can significantly reduce the likelihood

of financial losses and enhance the accuracy of payroll systems by implementing AI to facilitate real-time monitoring, proactive fraud detection, and automated remedies. AI-powered systems that prevent payroll fraud, thereby facilitating significant cost reductions and operational efficiency[31]

TABLE IV. COMPARATIVE ANALYSIS OF MACHINE LEARNING BASED PAYROLL FRAUD DETECTION

Author & Year	Key Findings	Focus Area	Challenges	Future Work
Thirusubramanian Ganesan et al. (2025)	Deep autoencoder models effectively detect payroll and performance anomalies using reconstruction error.	Deep learning–based HR and payroll anomaly detection	Model interpretability, data availability	Explainable and real-time deep learning models
Bamiduro (2025)	AI improves payroll automation, accuracy, and compliance through ML and RPA.	AI-driven payroll management systems	Cost, regulatory, and ethical issues	Cost-efficient and ethical AI payroll frameworks
Saha (2025)	ML models successfully identify payroll fraud within ERP systems using supervised and unsupervised learning.	ML-based payroll fraud detection in ERP	Labeled data dependency, system integration	Hybrid ML and NLP-based fraud detection
Singireddy (2024)	Active learning ensemble models adapt well to evolving fraud patterns with minimal retraining.	Deep learning ensembles for fraud detection	Imbalanced data, transparency	Adaptive and explainable fraud models
Enokkaren et al. (2024)	AI/ML frameworks enhance payroll fraud detection beyond traditional methods.	AI and ML approaches for payroll fraud	Privacy, concept drift, legacy systems	Privacy-aware and explainable AI solutions
Ravichandran et al. (2023)	AI enables real-time payroll fraud detection and automated response.	AI-powered payroll fraud prevention	Scalability, data quality	Real-time and scalable AI systems

VI. Conclusion and Future Work

Machine learning models used in a behavioral analytics system to identify suspicious payroll behavior in a current payroll system. With the growing use of digital and automated payroll operations, complex, evolving and subtle types of fraudulent activities have become difficult to detect using traditional rule-based methods of detecting fraudulent activities based upon modeling normal payroll behavior and detecting deviations across compensation patterns, payment timings, attendance records, and access privileges. Behavioral indicators and feature extraction are very important for maximizing detection and minimizing false positives. Adaptive learning measures are needed to respond to evolving payroll policy, workforce trends, and fraud schemes. Scalable and accurate payroll fraud detection based on ML has the potential to enhance financial security and governance in organizations with practical implications of investigative value to researchers and practitioners aiming to create robust, intelligent, and future-ready payroll monitoring systems due to their high sensitivity to imbalance in data, privacy concerns, concept drift, interpretability, and the need to integrate with legacy payroll systems. Future studies should include explainable AI models to increase trust and regulatory compliance, and privacy-sensitive learning methods to protect sensitive payroll information. Hybrid and self-adaptive models with real-time learning and automated ERP fusion are promising approaches for improving intelligent payroll fraud detection systems.

References

1. K. Mahajan, S. Shukla, and N. Soni, “A Review of Computerized Payroll System,” *IJARCCE*, vol. 4, no. 1, pp. 67–70, Jan. 2015, doi: 10.17148/IJARCCE.2015.4113.
2. R. Das, R. M. Sirazy, R. S. Khan, and S. Rahman, “A Collaborative Intelligence (CI) Framework for Fraud Detection in U.S. Federal Relief Programs,” *Appl. Res. Artif. Intell. Cloud Comput.*, 2023.
3. S. K. Das, “Transforming Loan and Distribution Processing in Retirement Systems : A QA Automation Approach,” *Int. J. Bus. Manag. Sci.*, vol. 05, no. 05, pp. 9–26, 2025.
4. O. O. Elumilade, I. A. Ogundej, G. O. Achumie, E. Hope Omokhoa, and B. M. Omowole, “Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security,” *J. Adv. Educ. Sci.*, 2022.
5. Z. Yusuf, A. Nawawi, and A. S. A. P. Salin, “The effectiveness of payroll system in the public sector to prevent fraud,” *J. Financ. Crime*, vol. 30, no. 2, pp. 404–419, 2020, doi: 10.1108/JFC-08-2017-0075.
6. F. Al Riyadh, “Optimization Strategies and Activities of Payroll Management : Ascent Group,” no. February, 2024.
7. A. Gupta, “A Strategic approach - Enterprise-Wide Cyber Security Quantification via Standardized Questionnaires and Risk Modeling impacting financial sectors globally,” *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 3, no. 1, mar. 2022, doi: 10.63282/3050-9416.IJAIBDCMS-V3I1P110.
8. J. B. Madavarapu, “Payroll Management System,” 2014.
9. T.Shterma, V.Fatkhutdinov, M.Prodanchuk, O.Bernaziuk, and Yu.Synytsia, “Organizational-Legal And Accounting-Analytical Aspects,” 2024.
10. J. R. Vummadi, H. Volikatla, and S. Dodda, “Smart HR for Smart Enterprises: A Machine Learning-Based Approach to Payroll Automation and Time Optimization,” *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 6, 2025, doi: 10.63282/3050-9262.IJAIDSML-V6I3P113.
11. G. Mantha, “Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency,” *North Am. J. Eng. Res.*, vol. 5, no. 3, 2024.
12. H. P. Kapadia, “Reducing Cognitive Load in Online Financial Transactions,” *Int. J. Curr. Sci.*, vol. 12, no. 2, pp. 732–797, 2022.

13. D. Patel, "Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 576–583, 2023, doi: 10.14741/ijcet/v.13.6.10.
14. T. Shah, "Leadership in digital transformation: Enhancing customer value through AI-driven innovation in financial services marketing," *Int. J. Sci. Res. Arch.*, vol. 15, no. 3, pp. 618–627, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1767.
15. A. Parupalli, "Business-Oriented Employee Performance Assessment via Machine Learning in ERP Systems," *TIJER – Int. Res. J.*, vol. 11, no. 11, 2024.
16. Z. Zhang and T. B. Trafalis, "Time-series Analysis for Detecting Structure Changes and Suspicious Accounting Activities in Public Software Companies," *Procedia Comput. Sci.*, vol. 20, pp. 466–471, 2013, doi: 10.1016/j.procs.2013.09.304.
17. S. B. Shah, "Advanced Framework for Loan Approval Predictions Using Artificial Intelligence-Powered Financial Inclusion Models," in *2025 IEEE Integrated STEM Education Conference (ISEC)*, 2025, pp. 1–10. doi: 10.1109/ISEC64801.2025.11147327.
18. A. M. Ahmed, C. N. Mohammed, and A. M. Ahmad, "Web-based payroll management system: design, implementation, and evaluation," *J. Electr. Syst. Inf. Technol.*, vol. 10, no. 1, p. 17, 2023, doi: 10.1186/s43067-023-00082-5.
19. R. Palwe, "Adaptive human: AI decision support for high-stakes financial advice," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, 2025.
20. S. B. Shah, "Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection," in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, IEEE, Apr. 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.
21. K. S. Hebbar, H. Parnerkar, and S. Gondi, "AI-Driven Real-Time Fraud Detection Using Kafka Streams In Fintech," *Int. J. Appl. Math.*, vol. 38, no. 6s, pp. 770–782, Oct. 2025, doi: 10.12732/ijam.v38i6s.433.
22. A. A. Compagnino *et al.*, "An Introduction to Machine Learning Methods for Fraud Detection," no. Ml, pp. 1–32, 2025.
23. S. Amrale, "A Novel Generative AI-Based Approach for Robust Anomaly Identification in High- Dimensional Dataset," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, 2024, doi: 10.48175/IJARSCT-19900D.
24. V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions: A Case Study Using Real-Time Data Streams," vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.
25. R. Dattangire, D. Biradar, R. Burle, L. Dewangan, and A. Joon, "Machine Learning Approaches to Safeguarding Health Insurance Against Fraudulent Claims," in *Advances in Data-Driven Computing and Intelligent Systems*, 2026, pp. 341–353.
26. T. Ganesan, M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, and V. K. R, "Anomaly Detection in HR data using variational autoencoders: A deep learning approach to fraud detection and performance outliers," *World J. Adv. Eng. Technol. Sci.*, vol. 14, no. 3, pp. 267–274, Mar. 2025, doi: 10.30574/wjaets.2025.14.3.0133.
27. A. Bamiduro, "AI driving payroll management systems: A multi-case study analysis," *World J. Adv. Res. Rev.*, vol. 28, no. 2, pp. 2065–2072, 2025, doi: 10.30574/wjarr.2025.28.2.3900.
28. B. Saha, "Leveraging AI to Predict Payroll Fraud in Enterprise Resource Planning (ERP) Systems," *SSRN Electron. J.*, vol. 11, no. 4, 2025, doi: 10.2139/ssrn.5224746.
29. Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., Ragireddy, U. K., & Addepalli, P. V. (2022). A Review of Frameworks, and Impact on the Software Development Life Cycle with Artificial Intelligence in Software Engineering. *American International Journal of Computer Science and Technology*, *4*(1), 44-53.
30. Manoharan, P., Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., & Shyam, D. (2022). Understanding the Use of Agile Development Practices Alongside Quantum Computing in Modern Engineering Projects. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 136-143.
31. Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., & Syed, M. H. (2022). Intelligent Predictive System of Cloud Resource Utilization Forecasting with Advanced Deep Learning. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 143-151.
32. Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., & Manoharan, P. (2022). A Survey of Statistical Process Control and Its Applications in Manufacturing Quality Assurance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 127-135.
33. Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., & Ragireddy, U. K. (2022). Survey on Blockchain Integration with Sap S/4hana for Transparent and Secure Supply Chains. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 161-170.
34. Mylavarapu, K. B., Pilli, J., Jannu, P. K., Mohammad, J. A., & Panchali, S. H. (2022). Comparative Performance of Machine Learning Techniques for Sentiment and Insight Analysis in Amazon Product Reviews. *American International Journal of Computer Science and Technology*, *4*(1), 54-64.
35. Mohammad, J. A., Panchali, S. H., Mylavarapu, K. B., Pilli, J., & Jannu, P. K. (2022). An Ensemble Machine Learning Approach for Reliable Fake News Detection on Social Media Platforms. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 152-161.
36. Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., & Mylavarapu, K. B. (2022). Review of Supply Chain–Integrated CRM Systems for Business Agility. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 155-163.
37. Panchali, S. H., Mylavarapu, K. B., Pilli, J., Jannu, P. K., & Mohammad, J. A. (2022). Predictive Maintenance in Smart Manufacturing: A Review of Machine Learning and Digital Twin Approaches. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 150-160.
38. Jannu, P. K., Mohammad, J. A., Panchali, S. H., Mylavarapu, K. B., & Pilli, J. (2022). Heat Dissipation Strategies for High-Performance Computing: A Review of Air and Liquid Cooling Efficiency. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 145-153.

39. Taluri, R. (2022). Cloud Data Engineering Strategies for Large-Scale Financial Data Integration and Intelligent Corporate Performance Reporting. International Journal of Emerging Research in Engineering and Technology, 3(4), 176-188. https://doi.org/10.63282/3050-922X.IJERET-V3I4P119
40. Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., Chilakapati, V. K., & Keshireddy, S. R. (2022). Machine Learning-Driven Threat Analysis for Enhancing Security in Data Center Networking. *American International Journal of Computer Science and Technology*, *4*(1), 65-76.
41. Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., & Chilakapati, V. K. (2022). Towards Secure and Reliable IoT: A Review on Anomaly Detection and Predictive Analytics in Sensor Networks. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 140-149.
42. Pathani, A. K., Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., & Kavuluri, H. V. R. (2022). Effective Monitoring of Sensor-Actuator Integration Methods for Real-Time Controlling in Smart Device Networks. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 144-154.
43. Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., & Dasari, A. (2022). Review on Network Virtualization and SDN in Industrial IoT (IIoT). *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 162-172.
44. Dasari, S., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., & Pathani, A. K. (2022). Networking Paradigms for Large-Scale IoT Deployments: A Survey on Reliability, Latency, and Scalability. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 136-144.
45. Taluri, R. (2021). Cloud-Native Architectures for Enterprise Financial Data Management, Analytics, and Regulatory Reporting Compliance. International Journal of Emerging Trends in Computer Science and Information Technology, 2(2), 101-111. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I2P112
46. J. Singireddy, "Deep Learning Architectures for Automated Fraud Detection in Payroll and Financial Management Services: Towards Safer Small Business Transactions," *J. Artif. Intell. Big Data Discip.*, 2024, doi: 10.70179/kehvpn52.
47. S. J. Enokkaren, R. Kendyala, J. Kurma, J. V. Mamidala, and V. Bitkuri, "Artificial Intelligence (AI) -Based Advance Models for Proactive Payroll Fraud Detection and Prevention," *Int. J. Mach. Learn. AI Data Sci. Evol.*, vol. 1, no. 1, pp. 1–11, 2024.
48. N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "AI-Powered Payroll Fraud Detection: Enhancing Financial Security in HR Systems," *J. Comput. Innov. Appl.*, 2023.

Copyright: © 2023 *Yudhveer K. This Open Access Article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*