International Journal of Machine Learning, AI & Data Science Evolution
ISSN: 3068-5073/ Open Access / IJMLAIDSE_Y1F1A001
Apex Academia Press / https://doi.org/10.63665/ ijmlaidse-y1f1a001

Original Article

Artificial Intelligence (AI)-Based Advance Models for Proactive Payroll Fraud Detection and Prevention

Sunil Jacob Enokkaren[1], Raghuvaran Kendyala[2], Jagan Kurma[3], Jaya Vardhani Mamidala[4], Varun Bitkuri[5], Avinash Attipalli[6]

[1]*ADP, Solution Architect, USA.*
[2]*University of Illinois at Springfield, Department of Computer Science, USA.*
[3]*Christian Brothers University, Computer Information Systems, USA.*
[4]*University of Central Missouri, Department of Computer Science, USA.*
[5]*Stratford University ,Software Engineer, USA.*
[6]*University of Bridgeport, Department of Computer Science, USA.*

Abstract

Payroll fraud has remained one of the most widespread financial risks to organizations which has a direct effect on the way organizations pay their salary, and this destroys trust in the institutions. Conventional rule-based detection systems used are usually found wanting in dealing with the changing and dynamic nature of fraud. As payroll systems are becoming more and more digitalized and financial transactions are becoming difficult to manage, more intelligent and adaptive solutions are urgently needed. This paper provides an in-depth overview of the types of payroll fraud, traditional methods for detecting and preventing such fraud, and the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing the capacity to detect fraud. The paper examines the potential of supervised and unsupervised frameworks in reinforcement learning and deep learning for identifying anomalies and patterns in payroll data. Additionally, best practices such as implementing good internal controls, providing employee training, and adopting cybersecurity measures are considered complementary solutions to technological ones. The issues, including the lack of data, privacy concerns, concept drift, explainability, and compatibility with legacy systems, are discussed to provide a fair approach to addressing the shortcomings of contemporary AI-based solutions. Lastly, the paper identifies future research directions, which would entail the relevance of adaptive, explainable, and privacy-preserving AI models to facilitate a proactive and resilient payroll fraud prevention in the contemporary digital ecosystems.

Keywords

Payroll Fraud, Fraud Detection, HR Systems, Anomaly Detection, Financial Security, ERP Systems, Machine Learning, Employee Trust.

Article History

Received: 19.01.2025

Accepted: 20.02.2025

Published: 10.03.2025

1. Introduction

Salary is a type of monetary reward that companies give to employees as a form of rewarding their contributions and duties [1]. In most cases, organizations create salary systems that are based on the classification, grade, and position of employees. Nevertheless, with the growing workforce, payroll management tends to be both complicated and time-consuming, especially in the last days of the month when payrolls need to be paid [2]. This complexity results in operational difficulties when ensuring that salary processing is accurate and timely.

At the same time, organizations are increasingly vulnerable to financial fraud, and it remains a major threat in the contemporary digital economy. Fraud is a broad term that encompasses various fraudulent activities, including misrepresentation, data manipulation, and unauthorized financial dealings. These activities may result in a serious loss of institutional credibility, as well as financial resources and reputation losses for the organization at both national and international levels [3]. Fraud detection has become a crucial topic of study and practice to curb such risks. Conventional rule-based systems have been extensively used to detect suspicious trends. Yet, these strategies

regularly fail to work effectively in the face of dynamic and changing fraudulent campaigns that utilize digital ecosystems, including online banking, e-commerce, and cryptocurrency.

Payroll fraud is one of the types of fraud that is specific and widespread, and it specifically affects the salary disbursement procedures within an organization. The forms of payroll fraud may include various types, such as ghost employees, inflated hours of work, exaggerated pay, or unapproved bonuses [4]. Such schemes not only lead to financial losses but also erode internal trust and disrupt the organization's internal operations. Enterprise Resource Planning (ERP) systems are often adopted by organizations seeking to address the drawbacks associated with payroll. ERP solutions bring payroll management to a single place and automate salary distribution processes, decreasing the administrative workload. Nonetheless, even though they are effective, ERP systems continue to be susceptible to abuse unless they have strong tools to detect fraud.

The advent of Artificial Intelligence (AI) has brought about a groundbreaking method in this field. A combination of approaches, facilitated by the implementation of Machine Learning (ML) and Deep Learning (DL) models, enables organizations to surpass traditional rule-based systems [5]. AI-powered models can process massive payroll data in real-time, pinpoint anomalies, and identify concealed insights that might be missed by human management or traditional tools [6]. Such systems allow for the proactive detection of payroll fraud, enhancing accuracy, efficiency, and resilience. In addition, hybrid AI solutions, such as the combination of supervised and unsupervised models, including Random Forests, Gradient Boosting, and Autoencoders, further contribute to the detection of both known and emergent fraudulent behaviours.

A. Structure of the Paper

The rest of this paper is structured as follows: Section 2 covers the different varieties of payroll fraud and traditional detection techniques. Section 3 reviews AI and ML approaches for fraud detection. Section 4 presents the key challenges associated with adopting AI in proactive payroll fraud prevention. The work is concluded and future research directions are outlined in Section 5.

2. Types Of Payroll Fraud & Conventional Detection Methods

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 [7]. The various forms of payroll fraud are illustrated in Figure 1:

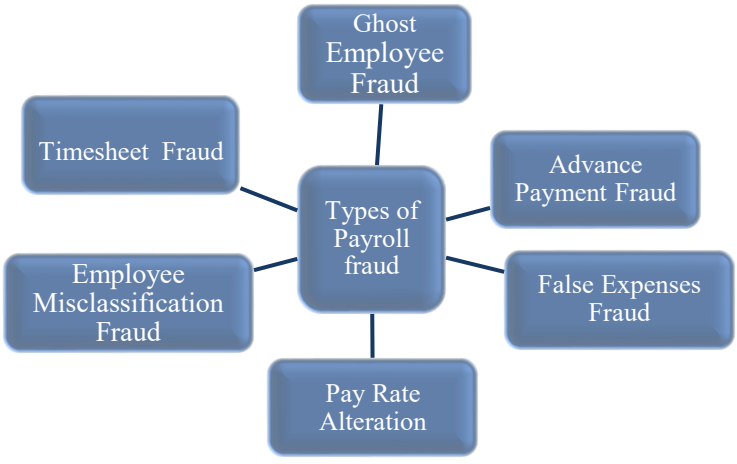

Fig-1: Types of Payroll Fraud

A. Ghost Employee Fraud

The term "ghost employee fraud" is the practice of manipulating payroll dollars by creating a fake employee. There are two possible explanations: either the employee was formed with the express intent of committing fraud, or the payroll account of a prior employee is kept and exploited for this reason [8]. In nearly all cases, an employee with

access to the payroll system inside the organization is the one who commits this kind of payroll fraud. This falls under the purview of human resources for the vast majority of businesses, particularly bigger ones.

B. Timesheet Fraud

Employees commit timesheet theft when they are paid for hours they didn't actually work. A common perpetrator of this is an employee who punches in early and punches out late, creating the illusion of working more generous hours. Maybe another worker is in on it, too, by punching out another worker's time even if the latter didn't actually work all that long. Internally, the payroll clerk is a potential target for timesheet fraud. They might assist another employee by changing their work hours and then receive a kickback for their assistance.

C. Employee Misclassification Fraud

Employers engage in worker misclassification fraud when they falsely claim that an individual is neither an employee nor an independent contractor to evade paying taxes on things like payroll, workers' compensation, and unemployment. Misclassifying an employee as an independent contractor might help a firm save money because companies have distinct responsibilities and costs for workers and independent contractors.

D. Pay Rate Alteration

A person's salary is changed such that they are paid more per hour than they actually deserve. An employee can make a mistake and never realise it. But someone with access to the payroll system is usually needed for this. To evade detection, the staff proceeds to hide their tracks. Companies should conduct internal audits to verify that there has been no manipulation or fabrication of compensation rates. Any discrepancies identified in the payroll data should be carefully scrutinized should one suspects this form of payroll fraud.

E. False Expenses Fraud

An employee makes false claims about costs they shouldn't get. Employees can make up whole expense reports or just lie about how much a real expense really costs to make money. For any costs reported, organizations should have the necessary paperwork, such as a receipt, documentation of how the money was paid, and any other relevant information. To stop this from happening, this needs to be checked before any costs are paid to employees.

F. Advance Payment Fraud

Payroll fraud happens when an employee takes advantage of an advance payment choice in a bad way. So, the worker essentially requests and receives an advance payment, but they never repay it. People who don't pay back an advance payment are often guilty of this crime. Although, someone who knows how to use the payroll system can also do it. To hide the payment, the advance payment is recorded as another charge.

(a) The Best Practices to Prevent Payroll Fraud

Preventive measures are consistently superior to curative measures. In the case of outsourcing payroll to a third party, it is preferable to take preventative measures rather than reacting to problems as they arise.

i. Strong Internal Controls

First, strong rules inside the company. The onus of handling payroll should never be placed on a single individual. Instead, divide and conquer: have one group enter data, another critique it, and a third give their stamp of approval [9]. Additionally, approval protocols strengthen security by requiring multiple signatures for changes to timesheets, salary increases, or the hiring of recruits. It is far more difficult to perpetrate fraud undetected using this multi-tiered strategy, which is in line with current best practices suggested by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

ii. Payroll Software

The second line of defence is reliable worldwide payroll software. For instance, Payroll's platform automatically flags entries that look fishy, like those with fake SSNs, out-of-cycle pay spikes, or entries made at odd times. Every action is recorded in a secure audit trail and undergoes strict clearance procedures.

iii. Employee Training

The potential for human mistakes cannot be adequately addressed by systems in isolation. Equally crucial are education and understanding. Staff members who participate in regular training learn to recognize red flags, such as

cost claims that seem unusually repetitive, expired medical documentation for sick leave, or an abrupt shift in direct deposit.

iv. Cybersecurity Measures

Cybersecurity measures must be in place to protect payroll data. Make that system encrypts important data, uses multi-factor authentication, and restricts access with role-based permissions [10]. It is essential to routinely rotate admin credentials and to monitor login attempts in real-time. These features are designed to protect against assaults and insider threats in accordance with best-practice cybersecurity practices.

v. Regular Audits

Payroll security is best protected by regular audits, both internal and external. Payroll operations benefit from these as much as physical. Monthly or quarterly evaluations, which combine automated scanning with human oversight, are preferable to waiting for problems to occur.

3. AI and Machine Learning Approaches for Fraud Detection

A wide variety of AI and ML techniques are used in fraud detection to spot patterns, outliers, and possible fraudulent actions [11]. Data type, intended level of accuracy, and computational efficiency are the determining factors in method selection for fraud detection. Here are the main AI and ML techniques used in the most recent cutting-edge research. AI Learning Paradigms is shown in figure 2 and Table 1.

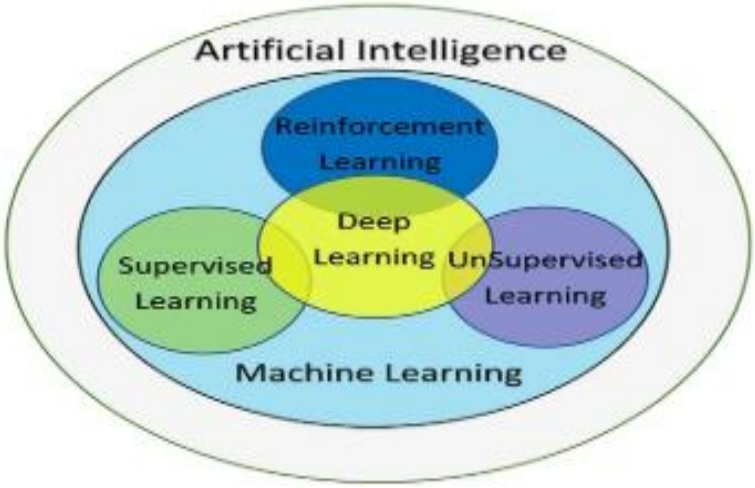

Fig-2: AI Learning Paradigms

- Supervised Learning Models: The criminals behind the complex web of financial fraud detection are supervised learning algorithms. Through the careful manipulation of labelled training data, the discovery of patterns, and the perfect orchestration of predictions, their symphony comes to fruition. With each case harmonized as either fraudulent or non-fraudulent, historical data plays the role of a melody. The algorithms can generalize with ease, picking up on melodic patterns in fresh transactions, thanks to their acute hearing for these notes.
- Unsupervised and Anomaly Detection Models: Fraud detection methods, like unsupervised anomaly detection, can work even without labelled training data. To identify fraudulent actions, these detection approaches examine out-of-the-ordinary trends in typical transaction behaviours. To do this, the detection methods employ clustering algorithms, autoencoders, and isolation forests. To detect transactions that deviate significantly from expected patterns, autoencoders use neural networks to generate compact representations of typical transaction data [12]. Isolated forests make it easier to spot suspicious transactions by constructing random decision trees to distinguish between real and fake entities.
- Reinforcement Learning in Fraud Detection: The potential of RL to identify the best decision policies for dynamic environments has made it a popular choice among researchers as a viable approach to fraud detection problems. Reinforcement learning is a great fit for monitoring changing fraud tendencies, as it doesn't require supervised learning methods but instead allows models to learn from their environment.

- Deep Learning and Advanced Architectures: A branch of machine learning known as deep learning (DL) draws inspiration from artificial neural networks, which mimic the way the brain functions [13]. An AI function can learn from unstructured or unlabelled data in a way that mimics the way the human brain processes information and generates patterns for use in decision-making. One name for ANNs is neural networks, while another is multilayer perceptron's.

Table 1: Summarising Different Fraud detection Approaches, Highlighting Their Strengths And Weaknesses

Approach	Description	Strengths	Weaknesses
Supervised Learning Models	Use labeled historical data (fraudulent vs. non-fraudulent) to learn patterns and classify new transactions. Examples: Logistic Regression, Random Forest, SVM.	High accuracy when labeled data is available; well-understood; interpretable in many cases.	Requires large labeled datasets; performance declines with imbalanced data; may not adapt well to new fraud patterns.
Unsupervised & Anomaly Detection Models	Detect anomalies without labeled data by learning normal behavior and flagging deviations. Methods include Autoencoders, Isolation Forests, Clustering.	Useful when labeled data is scarce; capable of identifying unknown fraud types; adaptive to dynamic environments.	Higher false positive rates; difficult to interpret; may struggle with overlapping fraud and normal patterns.
Reinforcement Learning (RL)	Learns optimal policies through trial-and-error interaction with the environment, adapting to evolving fraud tactics.	Effective in dynamic and adversarial environments; continuously improves with feedback; suitable for real-time detection.	Requires careful reward design; computationally intensive; slower convergence; limited adoption in production systems.
Deep Learning & Advanced Architectures	Employ neural networks (ANN, CNN, RNN, LSTM) to capture complex, nonlinear, and high-dimensional fraud patterns from structured and unstructured data.	Handles large-scale and high-dimensional data; captures hidden patterns; can process unstructured data (text, images, etc.).	Requires large datasets and computing power; often a "black box" (low interpretability); risk of overfitting.

A. Significance of AI in Fraud Detection

A variety of industries, including accounting and finance, have begun to use artificial intelligence (AI) to detect fraudulent activity.

- Real-time detection: Quick detection and identification of fraudulent activities is made possible by artificial intelligence (AI) systems' capacity to quickly process and analyse massive amounts of data in real-time. With the ability to prevent significant losses, prompt intervention is crucial in financial transactions and e-commerce.
- Cost efficiency: Artificial intelligence (AI) fraud detection systems often lead to savings in the long run, even though they need an upfront investment. There is less need for human labour, more operational efficiency, and fewer financial losses due to fraudulent activities as a result of using this system [14]. Artificial intelligence (AI) has the potential to enhance the client experience by mitigating the challenges associated with traditional verification methods.
- Adaptability: The invention of new tactics and the growth of fraudsters' strategies are constant activities. Systems powered by artificial intelligence (AI) may learn and adapt to new information, making them more resilient to fraud patterns that were previously undetected. There is no reliance on norms that are static and can be outmoded in a flash. When transaction volumes increase, scalability becomes an issue, as traditional manual or rule-based systems may struggle to keep up with the additional burden. Fraud detection systems powered by artificial intelligence (AI) can easily handle large datasets with little to no increase in human

labour as their capacity grows. The capacity of AI algorithms to analyse multiple data sets simultaneously and make sophisticated conclusions is what makes them accurate.

4. Challenges of AI in Proactive Payroll Fraud Prevention

Although artificial intelligence has demonstrated significant promise in detecting and preventing payroll fraud, several critical challenges remain that hinder its widespread adoption in enterprise payroll systems [15].

A. Data Scarcity and Imbalance

Payroll fraud cases represent a very small fraction of total payroll transactions. This class imbalance makes it challenging for supervised models to learn representative patterns, often resulting in a bias toward the majority (non-fraud) class. Moreover, the scarcity of publicly available payroll fraud datasets due to privacy, confidentiality, and compliance restrictions forces researchers to rely on proxy datasets or synthetic data, limiting external validation and reproducibility.

B. Privacy and Regulatory Constraints

Payroll data contains highly sensitive information, including salary details, employee identifiers, and banking records. The use of such data for training AI models is restricted by privacy regulations such as GDPR and HIPAA [16]. Ensuring data security, anonymization, and compliance while still enabling effective model training poses a significant challenge, especially for cross-organization fraud detection.

C. Concept Drift and Adaptive Fraud Strategies

Fraudsters continuously evolve their strategies to bypass detection mechanisms. Static AI models degrade in performance over time when fraud patterns shift a phenomenon known as concept drift. Without adaptive or incremental learning strategies, proactive payroll fraud detection systems risk becoming outdated, leading to higher false negatives.

D. Explainability and Trust Issues

Many high-performing AI models (e.g., deep neural networks) function as "black boxes," providing little interpretability. In payroll fraud prevention, investigators and auditors require clear reasoning behind anomaly flags to initiate disciplinary or legal action. The lack of explainability reduces trust among stakeholders and limits the adoption of advanced AI models in compliance-driven environments.

E. Integration with Legacy Payroll and ERP Systems

Organizations often use heterogeneous, legacy payroll management systems that are not designed for real-time AI integration. Embedding advanced anomaly detection models into these workflows requires significant infrastructural changes, increasing implementation costs and technical barriers.

F. False Positives and Operational Costs

While proactive AI systems may successfully detect suspicious patterns, high false positive rates can overwhelm investigators with unnecessary alerts. Each flagged case requires manual review, which consumes resources and can lead to "alert fatigue," reducing the effectiveness of the overall fraud detection framework.

5. Literature Review

Several significant research studies on payroll fraud detection and prevention were reviewed and analysed to guide and strengthen the development of this work.

Boztepe and Usul (2019) developed a model to identify performance-based salary system abuses in the healthcare industry and other forms of mistreatment using logistic regression. To achieve this, mixed real data from laparoscopic cholecystectomy procedures carried out in 2015 with some made-up information about the surgeries. Then they tested the resulting logistic regression model to see how well it separated the real data from the made-up information. In light of this, it can be demonstrated that the model achieved an accuracy of 83.30 percent in identifying tampered data [17].

Kwon et al. (2018) Machines misclassify objects into the wrong class, which leads to the untargeted adversarial case. On the other hand, machines are tricked into thinking the picture belongs to the attacker's target class in targeted

adversarial example attacks. One example they provide is an adversarial strategy that utilizes a single altered image to attack multiple models within a given target class. They used a transformation to maximize the likelihood of several target classes via multiple models to get these examples. The TensorFlow library and MNIST datasets were utilised for the project. The proposed method for creating a multi-targeted adversarial example was a complete success in the experiments [18].

Sanchez et al. (2018) A frequent representation of financial fraud is the employment of illegal procedures that can involve anybody from upper-level management to payroll employees, and it is a crime that is penalised by law. Even if there are a lot of methods for studying, detecting, and preventing this kind of behaviour, the most essential one is the fraud triangle theory that is linked to the traditional financial auditing model. To conduct this study, first survey relevant works in the literature in an effort to build own approach [19].

Domingos et al. (2017) looked at any issues concerning government spending. To accomplish this, DIE sometimes needs to sift through mountains of data in search of irregularities that can indicate questionable behaviour. Aware of the rising public desire for open government and anti-corruption measures, DIE is always exploring new ways to streamline these operations. Using a deep learning algorithm to create a prediction model, they examine unusual IT purchases in the Federal Government Procurement System in this particular study [20].

Pascual's (2016) Analysis method is continuous. The purpose of conducting an audit in the manner outlined in this article is to facilitate the assessment of controls, the management of risks, and the detection of fraud, aberrant or suspicious transactions, mistakes, etc. The implementation is done using CAATs (Computer Assisted Auditing Techniques), as illustrated in a case of payroll where these techniques facilitate the detection of variations in the basic wage, errors and/or fraud in the calculation of payable liquid, and the discovery of "ghost" employees [21].

Van Vlasselaer et al. (2015) APATE is a new method for identifying credit card transactions that are not what they appear to be in online shops. This method takes use of two sources of information: first, intrinsic features gleaned from the Recency-Frequency-Monetary (RFM) principles applied to incoming transactions and customer spending history; and second, network-based features gleaned from the credit card and merchant networks to derive a suspiciousness score for each network object that changes over time. The findings demonstrate the close relationship between intrinsic and network-based properties. The most effective models achieve AUC scores greater than 0.98 when these two kinds of features are combined [22].

Table 2 presents a summary of recent studies on payroll fraud detection and prevention, highlighting innovative models, datasets used, key findings, and the challenges faced.

Table 2: Summary of Recent Studies of Payroll Fraud Detection Using Artificial Intelligence

Authors	Study On	Key Findings	Challenges	Limitations	Future Work
Boztepe and Usul (2019)	Detection of mistreatments in performance-based salary systems using logistic regression	Logistic regression achieved 83.30% accuracy in detecting fictitious salary-related data	Dependence on real-world health sector datasets; limited scope	Focused on a single hospital dataset; may lack generalizability	Expand dataset scope and apply advanced ML models
Kwon et al. (2018)	Adversarial examples in ML (multi-targeted attacks on models)	The proposed attack achieved 100% success rate on MNIST dataset	Vulnerability of models to adversarial attacks; generalization issues	Experiments limited to MNIST dataset; lacks real-world applications	Test adversarial robustness across real-world domains and datasets
Sanchez et al. (2018)	Financial fraud and fraud triangle theory framework in auditing	Fraud triangle theory remains central to financial fraud	Difficulty in integrating fraud theory into	Framework mostly theoretical; requires empirical validation	Develop empirical systems to validate fraud

		detection and prevention	automated audit systems		triangle integration
Domingos et al. (2017)	Federal expenditure anomalies using deep learning on procurement data	Deep learning helped detect anomalies in federal procurement system data	Large-scale data handling and interpretability of DL models	Limited to the procurement system; transferability to other domains uncertain	Apply deep learning anomaly detection to broader government datasets
Pascual (2016)	Continuous audit techniques (CAATs) for payroll fraud detection	CAATs identified ghost employees, wage variations, and payroll calculation fraud	Implementation complexity and payroll data integration	Case study specific; may not generalize across industries	Enhance CAATs with AI/ML for adaptive payroll fraud detection
Van Vlasselaer et al. (2015)	Credit card fraud detection with intrinsic and network-based features	Combining intrinsic + network features achieved	Scalability and real-time detection in dynamic transaction environments	Evaluated only on credit card data; not tested on broader fraud types	Extend hybrid feature approaches to other financial fraud scenarios

6. Conclusion And Future Study

Payroll fraud remains a major risk for organizations, especially as payroll systems grow more complex and digitized. Traditional approaches such as manual audits and rule-based checks offer limited protection and struggle to keep pace with evolving fraud tactics. AI and ML techniques particularly supervised, unsupervised, reinforcement, and deep learning models offer improved accuracy, adaptability, and scalability, enabling real-time detection of hidden fraud patterns and faster response to emerging threats. However, several challenges hinder large-scale adoption of AI in payroll fraud prevention. Key barriers include data scarcity, privacy concerns, regulatory compliance requirements, concept drift, explainability issues, and integration with legacy systems. The lack of publicly available payroll fraud datasets makes model training and benchmarking difficult, while opaque model decisions reduce trust in compliance-focused environments.

Future research should focus on privacy-preserving approaches such as federated learning and differential privacy to enable collaborative model training without exposing sensitive payroll data. Adaptive and incremental learning models can address concept drift, ensuring resilience against constantly evolving fraud schemes. Additionally, explainable AI techniques must be explored to enhance transparency, build trust with auditors and regulators, and support broader adoption of AI-driven payroll fraud prevention systems.

7. References

[1] C. C. Escolar-Jimenez, "Data-Driven Decisions in Employee Compensation utilizing a Neuro-Fuzzy Inference System," Int. J. Emerg. Trends Eng. Res., vol. 7, no. 8, pp. 163–169, Aug. 2019, doi:s 10.30534/ijeter/2019/10782019.

[2] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," IEEE Internet Things J., vol. 5, no. 5, pp. 3637–3647, Oct. 2018, doi: 10.1109/JIOT.2018.2816007.

[3] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence-based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," ICT Express, 2019, doi: 10.1016/j.icte.2019.03.003.

[4] H. van Driel, "Financial fraud, scandals, and regulation: A conceptual framework and literature review," Bus. Hist., vol. 61, no. 8, pp. 1259–1299, Nov. 2019, doi: 10.1080/00076791.2018.1519026.

[5] S. Qiu, H. Q. He, and Y. S. Luo, "The value of restatement to fraud prediction," J. Bus. Econ. Manag., 2019, doi: 10.3846/jbem . 2019.10489.

[6] Gopi, "Zero Trust Security Architectures for Large-Scale Cloud Workloads," Int. J. Res. Anal. Rev., vol. 5, no. 2, pp. 960–965, 2018.

[7] E. Stancheva, "How Artificial Intelligence Is Challenging Accounting Profession," J. Int. Sci. Publ., vol. 12, pp. 126–141,2018.

[8] S. S. S. Neeli, "Serverless Databases: A Cost-Effective and Scalable Solution," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 6, p. 7, 2019.

[9] P. A. Gutiérrez et al., "Hybridizing logistic regression with product unit and RBF networks for accurate detection and prediction of banking crises," Omega, vol. 38, no. 5, pp. 333–344, Oct. 2010, doi: 10.1016/j.omega.2009.11.001.

[10] A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.

[11] D. Choi and K. Lee, "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation," Secur. Commun. Networks, vol. 2018, no. 1, pp. 1–15, Sep. 2018, doi: 10.1155/2018/5483472.

[12] A. Thapliyal, P. S. Bhagavathi, T. Arunan, and D. D. Rao, "Realizing Zones Using UPnP," in 2009 6th IEEE Consumer Communications and Networking Conference, 2009, pp. 1–5. doi: 10.1109/CCNC.2009.4784867.

[13] I. SADGALI, N. SAEL, and F. BENABBOU, "Performance of machine learning techniques in the detection of financial frauds," Procedia Comput. Sci., vol. 148, pp. 45–54, 2019, doi: 10.1016/j.procs.2019.01.007.

[14] N. BenYoussef and S. Khan, "Identifying fraud using restatement information," J. Financ. Crime, vol. 24, no. 4, pp. 620–627, Oct. 2017, doi: 10.1108/JFC-07-2016-0046.

[15] S. S. S. Neeli, "The Significance of NoSQL Databases : Strategic Business Approaches and Management Techniques," J. Adv. Dev. Res., vol. 10, no. 1, p. 11, 2019.

[16] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Comput. Secur., vol. 57, pp. 47–66, Mar. 2016, doi: 10.1016/j.cose.2015.09.005.

[17] E. Boztepe and H. Usul, "Using the Analysis of Logistic Regression Model in Auditing and Detection of Frauds," Khazar J. Humanit. Soc. Sci., vol. 22, no. 3, pp. 5–23, Dec. 2019, doi: 10.5782/2223-2621.2019.22.3.5.

[18] H. Kwon, Y. Kim, K.-W. ParkYoon, H. Yoon, and D. Choi, "Multi-Targeted Adversarial Example in Evasion Attack on Deep Neural Network," IEEE Access, vol. 6, pp. 46084–46096, 2018, doi: 10.1109/ACCESS.2018.2866197.

[19] M. Sanchez, J. Torres, P. Zambrano, and P. Flores, "FraudFind: Financial fraud detection by analyzing human behavior," in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Jan. 2018, pp. 281–286. doi: 10.1109/CCWC.2018.8301739.

[20] S. L. Domingos, R. N. Carvalho, R. S. Carvalho, and G. N. Ramos, "Identifying it purchases anomalies in the Brazilian Government Procurement System using deep learning," in Proceedings - 2016 15th IEEE International Conference on Machine Learning and Applications, ICMLA 2016, 2017. doi: 10.1109/ICMLA.2016.106.

[21] E. H. Pascual, "Continuous auditing to manage risks in payroll," in 2016 11th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, Jun. 2016, pp. 1–6. doi:10.1109/CISTI.2016.7521578.

[22] V. Van Vlasselaer et al., "APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions," Decis. Support Syst., vol. 75, pp. 38–48, Jul. 2015, doi: 10.1016/j.dss.2015.04.013.

[23] Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., & Gangineni, V. N. (2023). Scalable Deep Learning Algorithms with Big Data for Predictive Maintenance in Industrial IoT. International Journal of AI, BigData, Computational and Management Studies, 4(1), 88-97.

[24] Chalasani, R., Vangala, S. R., Polam, R. M., Kamarthapu, B., Penmetsa, M., & Bhumireddy, J. R. (2023). Detecting Network Intrusions Using Big Data-Driven Artificial Intelligence Techniques in Cybersecurity. International Journal of AI, BigData, Computational and Management Studies, 4(3), 50-60.

[25] Vangala, S. R., Polam, R. M., Kamarthapu, B., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2023). A Review of Machine Learning Techniques for Financial Stress Testing: Emerging Trends, Tools, and Challenges. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(1), 40-50.

[26] Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., Gangineni, V. N., & Pabbineedi, S. (2023). A Survey on Regulatory Compliance and AI-Based Risk Management in Financial Services. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 46-53.

[27] Bhumireddy, J. R., Chalasani, R., Vangala, S. R., Kamarthapu, B., Polam, R. M., & Penmetsa, M. (2023). Predictive Machine Learning Models for Financial Fraud Detection Leveraging Big Data Analysis. International Journal of Emerging Trends in Computer Science and Information Technology, 4(1), 34-43.

[28] Gangineni, V. N., Pabbineedi, S., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Tyagadurgam, M. S. V. (2023). AI-Enabled Big Data Analytics for Climate Change Prediction and Environmental Monitoring. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 71-79.

[29] Polam, R. M. (2023). Predictive Machine Learning Strategies and Clinical Diagnosis for Prognosis in Healthcare: Insights from MIMIC-III Dataset. Available at SSRN 5495028.

[30] Narra, B., Gupta, A., Polu, A. R., Vattikonda, N., Buddula, D. V. K. R., & Patchipulusu, H. (2023). Predictive Analytics in E-Commerce: Effective Business Analysis through Machine Learning. Available at SSRN 5315532.

[31] Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Polu, A. R., Vattikonda, N., & Gupta, A. K. (2023). Advanced Edge Computing Frameworks for Optimizing Data Processing and Latency in IoT Networks. JOETSR-Journal of Emerging Trends in Scientific Research, 1(1).

[32] Patchipulusu, H. H. S., Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., & Buddula, D. V. K. R. (2023). Opportunities and Limitations of Using Artificial Intelligence to Personalize E-Learning Platforms. International Journal of AI, BigData, Computational and Management Studies, 4(1), 128-136.

[33] Madhura, R., Krishnappa, K. H., Shashidhar, R., Shwetha, G., Yashaswini, K. P., & Sandya, G. R. (2023, December). UVM Methodology for ARINC 429 Transceiver in Loop Back Mode. In 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

[34] Shashidhar, R., Kadakol, P., Sreeniketh, D., Patil, P., Krishnappa, K. H., & Madhura, R. (2023, November). EEG data analysis for stress detection using k-nearest neighbor. In 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-7). IEEE.

[35] KRISHNAPPA, K. H., & Trivedi, S. K. (2023). Efficient and Accurate Estimation of Pharmacokinetic Maps from DCE-MRI using Extended Tofts Model in Frequency Domain.

[36] Krishnappa, K. H., Shashidhar, R., Shashank, M. P., & Roopa, M. (2023, November). Detecting Parkinson's disease with prediction: A novel SVM approach. In 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE) (pp. 1-7). IEEE.

[37] Shashidhar, R., Balivada, D., Shalini, D. N., Krishnappa, K. H., & Roopa, M. (2023, November). Music Emotion Recognition using Convolutional Neural Networks for Regional Languages. In 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE) (pp. 1-7). IEEE.

[38] Madhura, R., Krishnappa, K. H., Manasa, R., & Yashaswini, K. P. (2023, August). Slack Time Analysis for APB Timer Using Genus Synthesis Tool. In International Conference on ICT for Sustainable Development (pp. 207-217). Singapore: Springer Nature Singapore.

[39] Krishnappa, K. H., & Gowda, N. V. N. (2023, August). Dictionary-Based PLS Approach to Pharmacokinetic Mapping in DCE-MRI Using Tofts Model. In International Conference on ICT for Sustainable Development (pp. 219-226). Singapore: Springer Nature Singapore.

[40] Krishnappa, K. H., & Gowda, N. V. N. (2023, August). Dictionary-Based PLS Approach to Pharmacokinetic Mapping in DCE-MRI Using Tofts Model. In International Conference on ICT for Sustainable Development (pp. 219-226). Singapore: Springer Nature Singapore.

[41] Madhura, R., Krutthika Hirebasur Krishnappa. et al., (2023). Slack time analysis for APB timer using Genus's synthesis tool. 8th Edition ICT4SD International ICT Summit & Awards, Vol.3, 207–217. https://doi.org/10.1007/978-981-99-4932-8_20

[42] Shashidhar, R., Aditya, V., Srihari, S., Subhash, M. H., & Krishnappa, K. H. (2023). Empowering investors: Insights from sentiment analysis, FFT, and regression in Indian stock markets. 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), 01–06. https://doi.org/10.1109/AIKIIE60097.2023.10390502

[43] Jayakeshav Reddy Bhumireddy, Rajiv Chalasani, Mukund Sai Vikram Tyagadurgam, Venkataswamy Naidu Gangineni, Sriram Pabbineedi, Mitra Penmetsa. Predictive models for early detection of chronic diseases in elderly populations: A machine learning perspective. Int J Comput Artif Intell 2023;4(1):71-79. DOI: 10.33545/27076571.2023.v4.i1a.169

[44] HK, K. (2020). Design of Efficient FSM Based 3D Network on Chip Architecture. INTERNATIONAL JOURNAL OF ENGINEERING, 68(10), 67-73.

[45] Krutthika, H. K. (2019, October). Modeling of Data Delivery Modes of Next Generation SOC-NOC Router. In 2019 Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

[46] Ajay, S., Satya Sai Krishna Mohan G, Rao, S. S., Shaunak, S. B., Krutthika, H. K., Ananda, Y. R., & Jose, J. (2018). Source Hotspot Management in a Mesh Network on Chip. In VDAT (pp. 619-630).

[47] Nair, T. R., & Krutthika, H. K. (2010). An Architectural Approach for Decoding and Distributing Functions in FPUs in a Functional Processor System. arXiv preprint arXiv:1001.3781.

[48] Gopalakrishnan Nair, T. R., & Krutthika, H. K. (2010). An Architectural Approach for Decoding and Distributing Functions in FPUs in a Functional Processor System. arXiv e-prints, arXiv-1001.

[49] Krutthika H. K. & A.R. Aswatha. (2021). Implementation and analysis of congestion prevention and fault tolerance in network on chip. Journal of Tianjin University Science and Technology, 54(11), 213–231. https://doi.org/10.5281/zenodo.5746712

[50] Kuraku, Dr Sivaraju, et al. "Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks." International Journal of Computer Trends and Technology (2023).

[51] Kuraku, D. S., & Kalla, D. (2023). Impact of phishing on users with different online browsing hours and spending habits. International Journal of Advanced Research in Computer and Communication Engineering, 12(10).

[52] Kalla, D., & Samaah, F. (2023). Exploring Artificial Intelligence and Data-Driven Techniques for Anomaly Detection in Cloud Security. Available at SSRN 5045491.

[53] Chandrasekaran, A., & Kalla, D. (2023). Heart disease prediction using chi-square test and linear regression. Comput. Sci. Inform. Technol., 13, 135-146.

[54] Kalla, D. (2022). AI-Powered Driver Behavior Analysis and Accident Prevention Systems for Advanced Driver Assistance. International Journal of Scientific Research and Modern Technology (IJSRMT) Volume, 1.

[55] Rajiv, C., Mukund Sai, V. T., Venkataswamy Naidu, G., Sriram, P., & Mitra, P. (2022). Leveraging Big Datasets for Machine Learning-Based Anomaly Detection in Cybersecurity Network Traffic. J Contemp Edu Theo Artific Intel: JCETAI/102.

[56] Sandeep Kumar, C., Srikanth Reddy, V., Ram Mohan, P., Bhavana, K., & Ajay Babu, K. (2022). Efficient Machine Learning Approaches for Intrusion Identification of DDoS Attacks in Cloud Networks. J Contemp Edu Theo Artific Intel: JCETAI/101.

[57] Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Penmetsa, M. (2020). Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models. Journal of Artificial Intelligence and Big Data, 2(1), 153–164.DOI: 10.31586/jaibd.2022.1341

[58] Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., & Kakani, A. B. (2022). Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in healthcare. Journal of Artificial Intelligence and Big Data, 2(1), 141–152.DOI: 10.31586/jaibd.2022.1340

[59] Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2022). Designing an Intelligent Cybersecurity Intrusion Identify Framework Using Advanced Machine Learning Models in Cloud Computing. Universal Library of Engineering Technology, (Issue).

[60] Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. (2022). Leveraging Artificial Intelligence Algorithms for Risk Prediction in Life Insurance Service Industry. Available at SSRN 5459694.

[61] Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. (2021). Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption. International Journal of Emerging Trends in Computer Science and Information Technology, 2(3), 70-80.

[62] Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Tyagadurgam, M. S. V. Efficient Framework for Forecasting Auto Insurance Claims Utilizing Machine Learning Based Data-Driven Methodologies. International Research Journal of Economics and Management Studies IRJEMS, 1(2).

[63] Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., & Patchipulusu, H. H. S. (2022). Blockchain Technology in Supply Chain and Logistics: A Comprehensive Review of Applications, Challenges, and Innovations. International Journal of Emerging Research in Engineering and Technology, 3(3), 99-107.

[64] Narra, B., Vattikonda, N., Gupta, A. K., Buddula, D. V. K. R., Patchipulusu, H. H. S., & Polu, A. R. (2022). Revolutionizing Marketing Analytics: A Data-Driven Machine Learning Framework for Churn Prediction. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 112-121.

[65] Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Vattikonda, N., & Gupta, A. K. BLOCKCHAIN TECHNOLOGY AS A TOOL FOR CYBERSECURITY: STRENGTHS, WEAKNESSES, AND POTENTIAL APPLICATIONS.

[66] Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Penmetsa, M. (2022). Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models. Journal of Artificial Intelligence and Big Data, 2(1), 153–164.DOI: 10.31586/jaibd.2022.1341

[67] Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., & Kakani, A. B. (2022). Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in healthcare. Journal of Artificial Intelligence and Big Data, 2(1), 141–152.DOI: 10.31586/jaibd.2022.1340