European Journal of
Technology
(EJT)



A Survey of Machine Learning Techniques for Payroll Security in ERP Tax Systems

Bose babu Ravula, Yudhveer Kandukuri, Sojy John, Naveen Shrivastava, Mahesh Marri

AJP

European Journal of Technology
ISSN 2520-0712 (online)
Vol.10, Issue 1, pp4 39 - 59, 2026

www.ajpojournals.org

A Survey of Machine Learning Techniques for Payroll Security in ERP Tax Systems

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

[1]John Wiley &Sons , Inc., Principal
[2]G2 Web Services - Open Source DBA & DevOps
[3]Recreational Equipment, Inc - Technology Lead, DevOps Engineer & Cloud Migration
[4]T-Mobile Salesforce Lead Developer
[5]Amazon Web Services, Senior Electrical Engineer

Article history

Submitted 18.09.2026 Revised Version Received 15.10.2026 Accepted 19.11.2026

Abstract

Purpose: Enterprise Resource Planning (ERP) systems are widely used to integrate payroll and tax management functionalities; however, because payroll data is sensitive and tax regulations are complex, ERP systems are highly exposed to security, fraud, and compliance risks. The traditional rule-based security and audit controls within ERP payroll and tax modules do not always identify changing fraud patterns, internal abuse, and real-time compliance infractions, whereas machine learning (ML) techniques have proved effective in augmenting payroll security and tax compliance with data-driven, adaptive intelligence. This survey aims to review how ML supports payroll security in ERP tax systems.

Materials and Methods: The survey examines the machine learning methods used for payroll security in ERP tax systems, such as supervised and unsupervised learning, deep learning (DL), anomaly detection, and user behavior analytics. It considers how these methods facilitate early fraud detection, ongoing compliance auditing, and enhanced audit preparedness in intricate ERP settings, and it discusses ERP payroll and tax system architecture, data preprocessing, privacy and governance, and integration.

Findings: The synthesis of recent studies and practical applications indicates that ML-based approaches improve detection accuracy, reduce false positives, and strengthen audit readiness, although data quality, model transparency, and privacy remain open challenges.

Implications to Theory, Practice, and Policy: The survey recommends explainable, privacy-preserving ML models combined with rule-based controls, providing practitioners and policy analysts with useful insights for designing secure, intelligent, and compliant ERP-based payroll systems.

Keywords: *Enterprise Resource Planning (ERP), Payroll Security, Machine Learning (ML), ERP Tax, Security*

JEL Codes: *M15, M41, M42, J33, H26, C45, C55*

I. INTRODUCTION

The dynamic nature of the business environment requires most business operations to be supported by integrated Information Systems (IS). ERP systems have become an integral part of contemporary organizations because they incorporate fundamental business functions such as human resources, finance, accounting, and taxation into a single information system. Payroll processing is one such essential function, as it directly controls employee pay, statutory deductions, and tax reporting [1]. HR management involves acquiring and retaining the workforce in organizations, creating appropriate working conditions, and achieving job-employee congruency [2][3]. Human resource functions are also responsible for compensating employees through job evaluations, performance evaluations, incentives, appropriate benefits packages, and cost optimization [4]. The payroll, financial, and tax modules of an ERP system improve operational efficiency; however, they also make the system more complicated and increase the severity of security breaches.

ERP payroll security is especially challenging owing to the sensitivity of payroll information and the involvement of various stakeholders, such as human resource staff, finance units, administrators, and external regulatory agencies [5][6][7]. Unauthorized access, insider misuse, payroll fraud, and tax deduction errors can result in serious financial losses, legal consequences, and reputational damage. Although legacy rule-based controls, such as role-based access control (RBAC) and segregation of duties (SoD), together with audit logs, provide a basic level of security, they are frequently inadequate for identifying advanced fraud patterns and dynamic threats that change and evolve over time [8].

These security concerns extend to payroll processing within ERP-based tax systems [9]. Payroll tax processing must comply with constantly changing statutory requirements, jurisdiction-specific tax rules, and reporting obligations. Errors or manipulation in payroll tax calculations can directly affect organizational compliance and may become the subject of regulatory investigation [10]. Traditional rule-based tax validation systems struggle to respond quickly to regulatory changes and frequently rely on post-processing audits, which delay the identification of compliance violations [11]. Static controls therefore fall short, creating a strong demand for intelligent and adaptive security systems capable of operating continuously in ERP payroll tax systems.

Machine Learning (ML) offers a promising solution to these problems by enabling data-driven, adaptive payroll security in ERP tax systems [12] [13]. ML methods can analyze vast amounts of payroll and tax data to learn typical operational behavior and automatically detect anomalies, fraudulent operations, and compliance risks in real time [14]. Supervised learning, anomaly detection, deep learning, and user behavior analytics are some of the methods that complement standard ERP controls by offering predictive and proactive security.

A. Structure of the Paper

This paper is organized as follows: Section II reviews the related literature to establish the research baseline. Section III presents ERP payroll and tax systems: architecture and security context. Section IV presents the machine learning taxonomy and architecture for payroll security, and Section V concludes the paper with future work.

II. Literature Review

This section reviews prior work on payroll security in ERP tax systems using machine learning techniques and establishes the research baseline for this survey. Table I summarizes the key studies, highlighting their focus, findings, challenges, and future directions.

Maulana et al. (2026) examined an ERP-based payroll management system built on Odoo 17 using a Service-Oriented Architecture (SOA) approach. A hybrid AHP-TOPSIS model, incorporating expert judgment, was applied to assess readiness across Human Resources (HR) and Finance. Finance achieved a readiness score of 87% ("ready"), while HR scored 73% ("almost ready"). The study reframes ERP readiness through a capacity-complexity lens, demonstrating that organizational capacity (skills, resources, and process maturity) must be balanced with system complexity. It indicates that HR needs skill and data improvements, and that Finance needs to leverage enhanced payroll-accounting integration and automation, providing actionable guidance for organizations, ERP vendors, and policymakers seeking to strengthen payroll digitalization. Overall, the research demonstrates that ERP payroll readiness must be analyzed not only at the organizational level but also across functional domains, ensuring more balanced and sustainable ERP adoption [15].

Gupta and Singh (2025) addressed the complexity and ever-changing nature of modern tax obligations, which may be a challenge for enterprise resource planning (ERP) systems. The potential for deep learning, reinforcement learning, and other forms of artificial intelligence (AI) to transform tax compliance systems is the focus of their study. AI/ML integration into ERP systems enables businesses to accomplish adaptive compliance, real-time transaction monitoring, and automatic anomaly detection, thereby substantially reducing risk and human effort. Measurable improvements in operational efficiency and compliance accuracy are illustrated through case studies and use cases [16].

Saha (2025) investigated Artificial Intelligence (AI) techniques to predict and prevent payroll fraud within ERP systems. AI's capabilities in data analysis, pattern recognition, and anomaly detection are applied to historical payroll data, and various machine learning algorithms are evaluated for their effectiveness in predicting payroll fraud. These include supervised models such as decision trees (DT), random forests (RF), and support vector machines (SVM), as well as unsupervised models such as clustering and anomaly detection algorithms. The study also shows that integrating Natural Language Processing (NLP) within ERP systems enhances the ability to detect fraudulent behaviors by analyzing text-based data such as emails and personnel communications. It highlights data quality, algorithm transparency, and continuous model training as key requirements for improving fraud detection accuracy [17].

Suresh Dodda (2025) introduced an innovative payroll module that analyzes employee work and attendance patterns, as well as prior payroll cycles. Additionally, a Time Optimization Module (TOM) is available as an option, which supports personnel scheduling for the intended shift, overtime prediction, and leave planning. Data provided by real-world corporate HRM systems in a variety of industries is used to train and evaluate the proposed system. The results indicate that payroll processing time has been improved by 35%, the payroll error percentage has been reduced by 90%, and time-off strategies have been improved by 27%. The Application Programming Interface (API) makes integration with existing ERP and HRIS procedures simple, so there is less impact on the working population [18].

Sarferaz (2024) integrated AI principles into the ERP reference architecture and ensured their validity regardless of the underlying ERP vendor. Using the reference procedures outlined in the previous chapter, the study derives a common reference architecture and defines the software modules for R&D, sales, supply chain, procurement, manufacturing, service, asset management, finance, and human capital management [19].

Urpanen, Lic, and Tuomisto (2024) examined a company's payroll system and its effects on organizational efficiency. The study identifies typical problems with the system's complexity, user interface design, and data processing. These problems can neutralize the benefits of the

SAP Payroll system, which include improved reporting capabilities, simplified payroll processing, and reduced training and inefficiency with mass tools. Another issue is the lack of support for specific local requirements, such as tax automation, which can lead to cumbersome processes [20].

Table 1: Comparative Analysis of Challenges in Payroll security in ERP tax system using machine learning

Author & Year	Focus Area	Key Findings	Challenges Identified	Limitations	Future Work Directions
Maulana et al. (2026)	ERP-based payroll management using Odoo 17 and SOA; readiness assessment using hybrid AHP-TOPSIS	Finance readiness scored 87% (ready), HR scored 73% (almost ready); emphasizes balancing organizational capacity and system complexity	Skill gaps in HR, data quality issues, uneven readiness across functions	Limited to HR and Finance domains; organization-specific assessment	Extend readiness analysis to other ERP modules; longitudinal readiness evaluation; integration with AI-based analytics
Gupta & Singh (2025)	AI/ML integration in ERP tax compliance systems	AI/ML enables adaptive compliance, anomaly detection, and real-time monitoring; improves compliance accuracy and efficiency	Complexity of tax regulations; integration with legacy ERP systems	Focuses on conceptual models and case studies; limited empirical validation	Development of standardized AI-enabled tax compliance frameworks; large-scale real-world deployments
Saha (2025)	AI-based payroll fraud prediction and prevention in ERP systems	Supervised and unsupervised ML models effectively detect payroll fraud; NLP enhances fraud detection via text analysis	Data quality issues; model transparency and explainability concerns	Dependence on historical labeled data; limited discussion on real-time deployment	Explainable AI integration; continuous learning models; real-time fraud detection systems
Suresh Dodda (2025)	AI-driven payroll optimization with attendance and shift analysis	Achieved 35% faster payroll processing, 90% error reduction, and 27% improvement in leave planning	Data integration from heterogeneous HR systems; reliance on historical accuracy	Focused primarily on time and attendance optimization	Expansion to tax compliance and fraud detection; cross-industry validation
Sarferaz (2024)	AI-enabled ERP reference architecture independent of vendor	Proposes a common AI-integrated ERP reference architecture across core business modules	Ensuring interoperability across vendors; architectural complexity	Lacks empirical performance evaluation	Validation through real-world ERP implementations; security-focused AI modules
Urpanen, Lic & Tuomisto (2024)	SAP Payroll system and organizational efficiency	ERP payroll improves efficiency through automation and reporting; highlights usability and training issues	System complexity; inadequate user weak local tax automation	focused on a single ERP vendor	Improved UI design; enhanced tax automation; AI-assisted reporting and analytics

Synthesis of the reviewed literature: Taken together, the reviewed studies follow three largely separate threads: ERP readiness and architecture (Maulana et al., Sarferaz, and Urpanen et al.), AI-driven tax compliance and payroll automation (Gupta and Singh; Suresh Dodda), and ML-based payroll fraud prediction (Saha). They collectively indicate that ML and AI can strengthen tax compliance, fraud detection, and payroll efficiency, whereas the limitations summarized in Table I recur across studies: limited empirical validation, dependence on historical labeled data, limited real-time deployment, and concerns about data quality and model transparency. None of the reviewed studies integrates payroll security, tax compliance monitoring, and insider-threat analytics within a single ML architecture. This gap motivates the taxonomy and architecture presented in Section IV, which organizes ML models for payroll security across the ERP layers described in Section III.

III. ERP Payroll and Tax Systems: Architecture and Security Context

This section describes the ERP payroll and tax environment as a three-layer architecture: (1) the Core ERP Transactional Layer, (2) the Tax Engine and Calculation Layer, and (3) the e-Invoicing and Compliance Layer. For each layer, the security vulnerabilities that manifest there are identified, such as privilege abuse in the transactional layer, tax calculation drift in the tax engine layer, and tampering or delay in e-invoice and filing submissions in the compliance layer. Figures 1 and 2 relate to the transactional layer, whereas Figure 3 depicts the end-to-end tax management and compliance architecture.

A. Core ERP Transactional Layer

1) Payroll Processing Models and Users

An essential aspect of every HR department's work is processing payroll. Organizational efficiency is enhanced when payroll data is handled and recorded in a timely manner. There are two types of payroll systems, as shown in Figure 1; each exposes different security risks, since manual processing is prone to calculation errors and penalties, whereas computerized processing concentrates sensitive data and privileges in software.

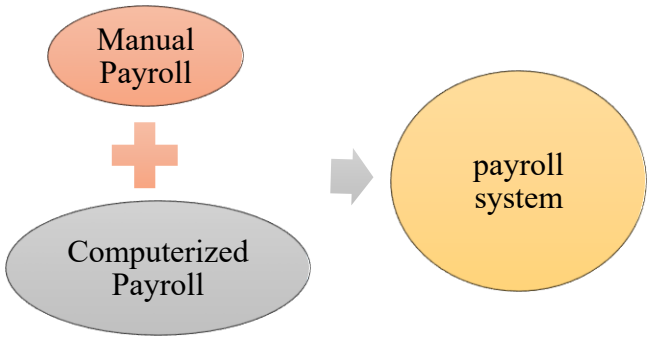


Figure1:Type of Payroll System

Manual Payroll: Payroll processing using a manual method is done by hand. This implies that calculating hours worked, statutory deductions (taxes), and involuntary deductions (health and pension benefits) from a worker's income is done only on paper. Penalties imposed by the government for incorrect tax returns may add up quickly.

Computerized Payroll: An example of a computerized payroll system would be an employer that buys payroll software and utilizes it to handle payroll. This approach is substantially faster than a manual payroll system. The automated payroll system is used by certain businesses, while

others use in-house payroll personnel [21]. Payroll employees must input all wages that are due into the system. Wage calculations, payroll data storage, and check printing are all handled by the system.

The system that keeps track of every employee's and accountant's information is called a payroll management system. This system is created to facilitate the process of locating and preserving the important data of any sort of users (i.e., workers and accountants).

Users of payroll Management System

- **Employee:** A user's details can be viewed and updated by an employee, who can also view their own pay receipt and register for leave.
- **Admin:** The administrator is a user who is responsible for management of all employee information and the addition of new employees.
- **Manager:** The manager is a user who is limited to the addition of new employees' pay papers and pay scale information.
- **Database:** A database is an ordered collection of data that is often stored and accessible electronically via a computer system. It allows you to store and manipulate data. In other words, an organization uses databases to store, manage, and retrieve information.

Because these roles hold different privileges over the same payroll records, privilege abuse, such as the unauthorized creation of ghost employees or the manipulation of pay scales through an Admin or Manager account, is the principal vulnerability of this layer.

2) **Enterprise Resource Planning (ERP) System**

ERP systems are software applications that are comprehensively designed to integrate and oversee all business functions within an organization [22]. Accounting, human resources, sales and distribution, project management, materials management, quality management, and supply chain management (SCM) are all elements of this software suite. It is a program that meets the needs of professionals in the fields of accounting, human resources, and logistics.

3) **Characteristics of ERP Software**

ERP software is a commercial product that can be bought from different vendors who specialize in the enterprise resource planning (ERP) segment of the software industry. SAP, Baan, J.D. Edwards, Oracle, and PeopleSoft were the most notable ERP vendors [23]. The great adaptability of ERP software allows it to meet the diverse needs of users in almost any economic sector. Consequently, there are now three varieties of ERP software: generic, pre-configured, and installed.

- The software, in its most comprehensive form, is generic, serves a diverse array of business sectors, and necessitates configuration prior to its use.
- Packaged, pre-configured templates have been derived from the whole program. Particular types of businesses, including those in the retail and automotive sectors as well as small and medium-sized enterprises (SMEs), are the inspiration for these templates.
- ERP software becomes visible to the majority of users during the operational installation phase, after the customization of a generic or preset package to meet the particular needs of each organization on-site.

European Journal of Technology
ISSN 2520-0712 (online)
Vol.10, Issue 1, pp4 39 - 59, 2026

www.ajpojournals.org

4) Integration of ERP for Payroll System

Figure 2 shows the integration of the Employee Module and Payroll Module in Odoo for a payroll system, with a clear division of activities between HR staff, finance staff, and employees [24]. The process begins with Activity A.1 where HR staff inputs employee data, reads the data, and summarizes salary calculations in the Employee Module. This ensures that employee records are up to date and that salary structures are accurately defined. At this layer, every change to employee data or salary structures is a potential point of privilege abuse or segregation-of-duties violation, so access to these activities must be monitored.

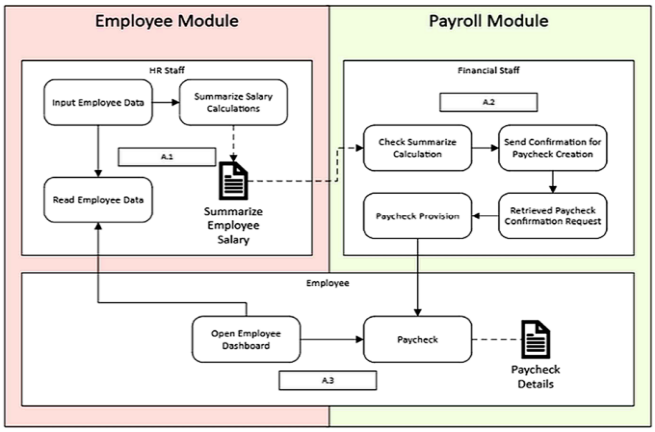


Figure 2: General Block of ERP for Payroll System

Although ERP systems offer operational integration benefits, their implementation in developing countries is not objectively assessed and often faces challenges related to limited IT resources, low digital maturity, and sector-specific requirements [25]. Moreover, there is a lack of flexible evaluation frameworks that combine multi-criteria decision-making with expert judgment to reflect diverse business environments.

5) Transactional Data Flow and Security Exposure

The core ERP system is the major backbone of organizational transactions. It brings together the information of several functional modules such as sales, purchasing, finance, inventory, production, services, HR, and CRM. Every business activity, including sales invoices, procurement transactions, payroll entries, and financial corrections, creates tax-applicable information [26]. The ERP system offers standardized, structured inputs to downstream tax processing components, which allows tax processing to be automated with less manual intervention. However, because every payroll entry and financial correction originates in this layer, it is also where privilege abuse, segregation-of-duties violations, and unauthorized changes to employee or salary records enter the downstream tax flow.

B. Tax Engine and Calculation Layer

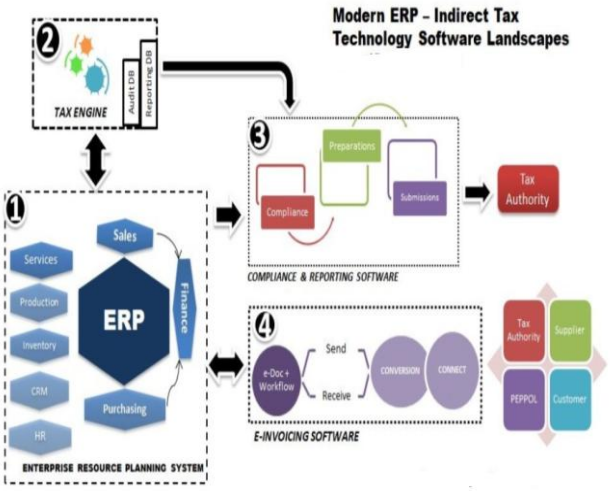


Figure 3: Tax Management and Compliance Architecture

The ERP-based tax management and compliance architecture is a multi-layered, integrated ecosystem intended to support correct tax determination, regulatory compliance, and secure communication with external stakeholders [27]. This architecture seamlessly integrates enterprise operational data, tax engines, compliance platforms, and electronic invoicing systems, as shown in Figure 3, to provide end-to-end tax transparency. The tax engine and calculation layer is described first, followed by the e-invoicing and compliance layer.

Tax engine is a special layer of computation that executes rules of indirect taxation to the transactions generated by ERP. It analyses jurisdiction-based regulations of tax, tax rates, exemptions and thresholds in order to establish correct tax liabilities. This layer embraces complex tax situations, including multi-country activities, cross-border transactions and different tax treatment of goods and services.

The tax engine also provides accountability and traceability through:

- A database which keeps all tax decisions and calculations.
- A reporting database that facilitates reconciliation, analysis, and statutory reporting.

Security vulnerabilities in this layer manifest as tax calculation drift: outdated rate tables, misconfigured exemptions or thresholds, and unauthorized rule changes can cause calculated liabilities to diverge gradually from statutory requirements across payroll cycles, often without triggering any rule-based alert.

C. e-Invoicing and Compliance Layer

The e-invoicing layer facilitates the real-time or near-real-time communication of electronic invoices between the organization and external parties. It oversees the processes of documents, digital approvals, and invoice transmission security. The conversion element ensures adherence to country-specific invoice structures and standards.

Connectivity features allow seamless integration with:

- Government tax portals
- Suppliers and customers
- Standardized networks such as PEPPOL.

Vulnerabilities in this layer include tampering with or duplication of electronic invoices and filings, unauthorized access to government portal credentials, interception of data in transit, and missed or late submissions during critical reporting cycles.

D. Security, Auditability, and Compliance Context

Security cuts across all the architectural layers. The system maintains logging and audit trails to support regulatory inspection and internal audit [28]. Nevertheless, owing to the growing volume of transactions and frequent changes in regulations, conventional rule-based compliance systems are increasingly unable to keep pace. The following security objectives must therefore be protected across all three layers:

- Sensitive financial and tax information confidentiality.
- Integrity of tax calculations and submissions.
- Availability of compliance services during critical reporting cycles.

Mapped to the three layers, confidentiality and integrity are most exposed to privilege abuse in the core transactional layer, integrity is most exposed to tax calculation drift in the tax engine layer, and availability and integrity are most exposed in the e-invoicing and compliance layer during submission and reporting cycles. These cross-layer exposures motivate the machine learning taxonomy presented in Section IV.

IV. Machine Learning Taxonomy and Architecture for Payroll Security

Machine learning offers intelligent and dynamic solutions for securing ERP payroll systems against fraud, abuse, and hacking. ML models can support traditional security controls and perform proactive threat detection by learning patterns from historical payroll and other system-related data.

ERP payroll systems deal with very sensitive financial and personal information and are therefore easy targets of fraud, abuse, and regulatory breaches. Traditional security mechanisms in ERP systems rely on predefined rules, access control rules, and periodic audits. Although these mechanisms work well against known threats, they cannot identify emerging fraud trends and sophisticated anomalies. ML provides more adaptive and intelligent security features that contribute greatly to payroll protection and regulatory compliance.

This section unifies the machine learning techniques and the ML-driven security mechanisms for ERP payroll systems into a single taxonomy and processing architecture. Payroll, tax, and system-log data are first prepared through data preprocessing (Section IV-A). Four model families then address distinct threats: supervised models for known payroll errors and tax miscalculations (Section IV-B), unsupervised models for novel ghost employees and salary anomalies (Section IV-C), deep learning and time-series models for multi-cycle tax drift and longitudinal behavior analysis (Section IV-D), and user behavior analytics (UBA) for insider threat and privilege misuse detection across HR, payroll administrator, and system administrator roles (Section IV-E). These models are operationalized through anomaly detection (Section IV-F), real-time monitoring and continuous compliance (Section IV-G), and tax compliance monitoring (Section IV-H), all under the privacy, ethics, and governance controls described in Section IV-I.

A. Data Preprocessing of Payroll System

Handle Missing Values via Imputation: Data cleaning is a crucial part of data preparation, and fixing missing values is a big deal in this context. Figure 4 shows the most common methods of numerical data imputation, which include using the mean or median.

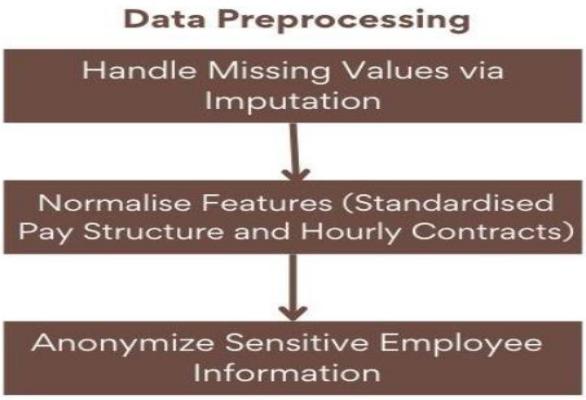


Figure 4: Data Preprocessing

- Normalize Features (Standardized Pay Structure and Hourly Contracts): It is important to standardize the data after it is complete to make sure that all the characteristics are on the same scale [29]. There may be large discrepancies in the scales of such characteristics as salary log run times.
- Anonymize Sensitive Employee Information: The Human Resources department handles a lot of sensitive information, such as the names, home addresses, social security numbers, and other personal details of workers. Compliance with the governing regulations of GDPR or HIPAA requires the concealing of particular and identifiable employee data.

B. Supervised Models for Known Payroll Errors and Tax Miscalculations

Labeled datasets, in which each transaction is individually designated as normal or anomalous, are the foundation of supervised learning algorithms for payroll anomaly detection. These methods train models to generalize to new types of transactions by analysing past payroll data. The labeled training data must be of high quality and representativeness for supervised approaches to be effective. In ERP payroll systems, supervised models are best suited to classifying known payroll errors and tax miscalculations, such as incorrect deductions, duplicate payments, and misapplied tax rates.

- **Gradient Boosted Trees (XGBoost, Light GBM):** Payroll records often include missing values and mixed data types, which these models handle properly through native support. Their additive character captures the intricate interplay of characteristics including department, payment schedule, and employee position.
- **Random Forests:** They provide strong performance with minimal hyperparameter tuning. Their ensemble structure reduces the likelihood of incorrect predictions in payroll data caused by overfitting.

1) Payroll Processing Engine (PPE)

An effective payroll system relies on the Payroll Processing Engine (PPE), and making the right selection when it comes to the ML models used for payroll calculation is very important. Random Forest (RF), Gradient Boosting (GB), and Support Vector Machine (SVM) models have become increasingly popular among the supervised models employed in the solutions for tasks such as anomaly detection, payroll error correction, and even employee performance evaluation. The ability to identify mistakes and do predictive analysis makes these supervised learning models well-suited to certain parts of payroll, which in turn improves the accuracy of payroll and the system as a whole.

C. Unsupervised Models for Novel Ghost Employees and Salary Anomalies

In situations when there is a lack of labeled data or when new fraud patterns arise, unsupervised learning works quite well for payroll anomaly detection [30]. These algorithms find deviations by understanding the fundamental structure of payroll data without depending on predetermined labels. In ERP payroll systems, they are particularly suited to detecting novel ghost employees and unusual salary anomalies for which no historical labels exist.

1) Clustering-Based Anomaly Detection

Payroll transactions that are comparable are grouped together by clustering algorithms, which identify abnormalities as outliers. Particularly successful are K-means and DBSCAN. The distance to centroids is used to measure anomalies in K-means, which partitions data into k clusters. The objective function minimizes

$$j = \sum_{i=1}^{k} \sum_{x \in c_i} \|x - \mu_i\|^2 \qquad (1)$$

where Ci denotes cluster i and μ_i its centroid in Equation (1). Transactions that deviate from their centroid by more than a certain Mahalanobis distance are marked.

- DBSCAN recognizes dense areas and flags solitary spots as anomalous. It uses two parameters: neighbourhood radius (ε) and minimum points (minPts). Points that do not fulfill the density requirement are categorized as noise.

2) Dimensionality Reduction Techniques

Dimensionality reduction should be performed prior to anomaly identification on payroll data that has high dimensionality (e.g., many compensation components). Principal Component Analysis (PCA) plots data along orthogonal axes of highest variance. In Equation (2), anomalies have a large reconstruction error when projected back to their original space.

$$Error = \|x - ww^T x\|^2 \qquad (2)$$

where W contains the principal components. Payroll entries are highlighted if their error values fall inside the top percentile.

3) Isolation Forests, One-Class SVM, and Autoencoders

Isolation Forests isolate anomalies through random partitioning of the feature space; payroll records that require unusually few partitions to isolate, such as unusually high allowances for a given role, receive high anomaly scores. One-Class SVM learns a boundary around normal payroll behavior and flags records that fall outside it, which is useful when only legitimate payroll history is available. Autoencoders are neural networks trained to reconstruct normal payroll records; a large reconstruction error indicates a potential ghost employee or salary anomaly that the model has not seen before.

D. Deep Learning and Time-Series Models for Multi-Cycle Tax Drift and Longitudinal Analysis

Deep learning models can be applied in ERP payroll systems to identify sophisticated fraudulent trends and security risks that conventional machine learning models cannot capture [31]. These models can automatically acquire high-level representations from large amounts of payroll and system data and are therefore appropriate for high-level security analysis. Recurrent and time-series architectures are particularly suited to detecting multi-cycle tax drift and analyzing longitudinal behavior.

1) **Artificial Neural Networks (ANNs)**

Artificial Neural Networks are made of several layers that are interconnected and learn the nonlinear relationships of payroll data. ANNs are also used in the payroll security to examine data in salary structures, allowances, deductions, and user activities to match suspicious transactions [32]. They work well in detecting intricate fraud schemes with numerous variables as well as minor variations to the regular payroll.

2) **Recurrent Neural Networks (RNNs)**

Recurrent Neural Networks are able to examine sequential data and are ideal in the analysis of payroll time-series. RNNs can be used to study past historical payroll cycles and determine anomalous trends, including slow increases in salary rates or recurring tax evasion throughout history [33].

3) **Long Short-Term Memory (LSTM)**

LSTM networks are a more sophisticated version of RNNs that overcome the vanishing gradient problem and capture long-term dependencies. In payroll security, LSTMs can model multi-cycle sequences of tax deductions and salary changes, so that gradual tax drift and longitudinal behavior changes are detected as deviations from the learned sequence.

4) **Time Optimization Module (TOM)**

Reinforcement learning (RL) is used by the Time Optimization Module (TOM) to plan personnel shifts in order to maximize operational productivity and minimize employee dissatisfaction with overtime. In this sense, state, action, and reward are the three main components of the RL framework. In TOM, the state contains aspects such as the strain on the present workforce, the desired shift, and the current tasks, the action is the assignment of shifts, and the reward reflects the productivity gained and the overtime dissatisfaction avoided.

E. User Behavior Analytics (UBA) for Insider Threat and Privilege Misuse Detection

User Behavior Analytics (UBA) is a machine learning–driven security approach that focuses on monitoring and analyzing user activities within ERP payroll systems to identify abnormal or potentially malicious behavior [34]. In payroll environments, authorized users such as HR staff, payroll administrators, and finance managers have access to highly sensitive data, making insider threats and privilege misuse a significant security concern. UBA models learn normal behavior patterns by analyzing historical system logs, including login times, access frequency, transaction types, and role-based privileges across ERP roles such as HR users, payroll administrators, and system administrators, as shown in Table 2.

European Journal of Technology
ISSN 2520-0712 (online)
Vol.10, Issue 1, pp4 39 - 59, 2026

www.ajpojournals.org

Table 2: User Behavior Analytics (UBA) in ERP Payroll Systems

ERP Role	Typical Payroll Responsibilities	UBA Features Applied	Monitored Behaviors	Potential Risks Detected
HR User	Employee data management, salary structure updates, leave and allowance handling	Behavioural profiling, Access pattern analysis	Frequent employee record edits, abnormal salary adjustments	Ghost employee creation, unauthorized salary changes
Payroll Administrator	Payroll execution, overtime processing, payslip generation	Anomaly detection, Temporal behaviour analysis	Payroll runs outside schedule, repeated manual overrides	Payroll manipulation, duplicate payments
Finance User	Tax deductions, statutory compliance, payroll accounting	Risk scoring, Cross-module behaviour correlation	Irregular tax modifications, mismatched ledger postings	Tax evasion, compliance violations
System Administrator	User access control, role assignment, system configuration	Privilege usage monitoring, Session analysis	Excessive privilege escalation, unusual login patterns	Insider threats, system misuse
Compliance/Audit Officer	Payroll audits, compliance verification, reporting	Explainable alerts, Audit trail analysis	Repeated high-risk alerts, override approvals	Audit failures, regulatory penalties
Third-Party Vendor/User	Payroll outsourcing, support services	Restricted behaviour monitoring, Boundary analysis	Access beyond authorized scope	Data leakage, external misuse

F. Anomaly Detection for Payroll Fraud Prevention

Payroll anomalies put a heavy financial and operational strain on businesses, whether they are the result of fraud, mistakes, or inefficient systems. Figure 5 shows the direct financial losses from payroll theft alone.

European Journal of Technology
ISSN 2520-0712 (online)
Vol.10, Issue 1, pp4 39 - 59, 2026

www.ajpojournals.org

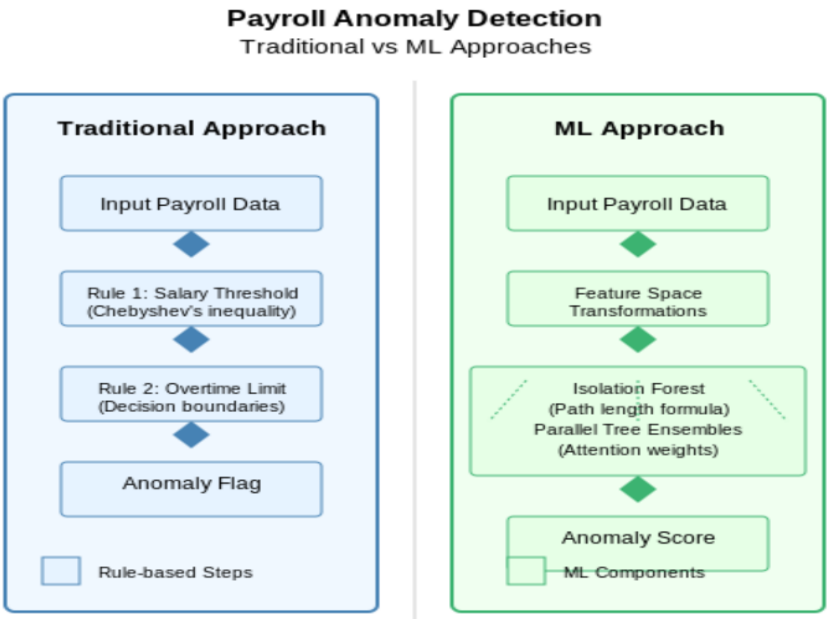


Figure 5: Payroll Anomaly Detection

Traditional payroll anomaly detection relies heavily on rule-based systems and statistical thresholds. These methods define explicit conditions to flag anomalies. Machine learning approaches transform anomaly detection into a pattern recognition problem. Supervised methods like Random Forests leverage labeled historical data to learn decision boundaries (Section IV-B), while unsupervised methods detect deviations without labels (Section IV-C).

- Key Payroll Features for Anomaly Detection: Raw payroll data can be augmented with derived features that expose anomalies.
- Relative Salary Deviation: Measures how much an employee's salary deviates from their department or role average. Calculated as Equation (3)

$$Deviation_i = \frac{s_i - \mu_d}{\sigma_d} \qquad (3)$$

where s_i is the salary of employee, i, μ_d is the mean salary for their department, and σd is the standard deviation.

- Payment Frequency Anomalies: Flags employees receiving payments outside regular cycles (biweekly vs. monthly).
- Bonus-to-Salary Ratio: Identifies disproportionately large bonuses relative to base salary.
- Temporal Features: Payroll timestamps can be decomposed into day-of-week, month-end, or holiday-adjacent indicators to detect timing-based fraud.

G. Real-Time Monitoring and Continuous Compliance

Machine learning-based security and compliance management represents a paradigm shift in the manner in which ERP payroll systems control security and regulatory requirements [35]. The conventional payroll controls are based on regular audits and after-process checks, which frequently discover fraud or errors in the payroll only after the payroll has been executed. By contrast, real-time monitoring, made possible by machine learning, automatically assesses payroll operations in real time, so that any activity that poses a security or compliance threat is immediately identified and acted upon:

- Real time monitoring entails the real time analysis of payroll transactions, user activities, and system activities when performing payroll. With information about payroll entering the ERP system, machine learning models will compare each transaction with pre-learned behavioral patterns.
- Continuous compliance helps to make sure that payroll procedures are in line with the statutory requirements, internal policies, and taxation. Rather than authorizing compliance at a scheduled time, the ML models check tax deductions, statutory contributions and regulatory thresholds in all payroll cycles.
- Implementation of real-time monitoring: ML-based evaluations are triggered by payroll events such as salary adjustments, overtime approvals, or changes to the tax configuration. In case of an anomaly or compliance violation, the system raises an alert, flags or blocks the transaction, and routes it for human review.

H. Machine Learning-Based Tax Compliance Monitoring in ERP Payroll Systems

Tax compliance monitoring based on machine learning improves ERP payroll systems by allowing constant and data-driven verification of tax computations, statutory deductions, and regulatory compliance. With payroll data, ML models can learn normal taxation behavior and can automatically identify abnormalities, inconsistencies and possible non-compliance across payroll periods and across jurisdictions [36]. Unlike conventional rule-based checks, ML methods can respond to regulatory change, minimize false positives via learning and feedback and offer predictive risk information that can be used to respond to proactive audit preparedness. Table 3 demonstrates that machine learning-based solutions considerably improve accuracy, flexibility and efficiency in the compliance of payroll taxes in contrast to traditional rule-based systems.

European Journal of Technology
ISSN 2520-0712 (online)
Vol.10, Issue 1, pp4 39 - 59, 2026

www.ajpojournals.org

Table 3: Machine Learning-Based Tax Compliance Monitoring Enhances ERP Payroll

Compliance Area	Description	Payroll Data Used	ML Techniques	Key Outputs	Compliance Benefit
Tax Deduction Validation	Verifies correctness of income tax, social security, and statutory deductions	Salary, exemptions, contribution records	Supervised classificatio, Hybrid rule-ML models	Validated deduction values, alerts	Prevents incorrect deductions and penalties
Anomaly Detection in Tax Calculations	Identifies unusual or suspicious tax computation patterns	Payroll history, tax values, adjustments	Isolation Forest, One-Class SVM, Autoencoders	Anomaly scores, flagged records	Detects fraud and miscalculations early
Regulatory Rule Compliance Checking	Ensures adherence to jurisdiction-specific tax laws	Tax rules, payroll configuration data	Decision Trees, Knowledge-driven ML	Compliance status reports	Reduces risk from regulatory changes
Audit Risk Scoring	Predicts likelihood of payroll records being audited	Historical audit data, payroll summaries	Logistic Regression, Gradient Boosting	Risk scores, audit indicators	Enables proactive audit preparation
Cross-Cycle Consistency Analysis	Analyzes tax consistency across payroll cycles	Time-series payroll and tax data	LSTM, Time-series anomaly detection	Trend deviations, drift indicators	Detects long-term compliance drift
Employee-Level Tax Risk Profiling	Identifies employees with abnormal tax behavior	Employee profiles, tax deductions	Clustering (K-Means, DBSCAN)	Risk clusters, outlier profiles	Focuses compliance efforts on high-risk cases
Jurisdictional Tax Comparison	Detects inconsistencies across regions and countries	Multi-location payroll data	Multivariate anomaly detection	Jurisdiction variance reports	Supports multi-country compliance
Real-Time Compliance Monitoring	Evaluates tax compliance during payroll execution	Live payroll transaction streams	Online ML models, Streaming analytics	Instant alerts, blocked transactions	Enables immediate corrective action
False Positive Reduction	Differentiates legitimate exceptions from violations	Historical alerts, investigator feedback	Ensemble learning, Active learning	Refined alert models	Improves operational efficiency
Explainability and Audit Support	Provides transparent justification for ML decisions	Model outputs, feature importance data	SHAP, LIME (XAI techniques)	Explanation reports	Enhances regulatory trust

I. Privacy, Ethics, and Governance for ERP Payroll Systems

ERP payroll applications present serious issues about privacy, ethics, and governance, since financial and personal information of employees is very sensitive. Data privacy with strong measures of access control, encryption, and adherence to the regulations of data protection should be practiced to avoid inadvertent exposure of data. Ethics demand that the ML models should be just, neutral and transparent, so that the automated decision-making process should not discriminate or cause unfair results to employees. The use of governance frameworks is important because it establishes accountability, model validation processes, auditability, and human control.

V. Conclusion and Future Work

This survey has examined machine learning–based solutions for improving payroll security and tax compliance in ERP systems, whose importance is growing in increasingly complex and data-intensive enterprise environments. ERP payroll systems rely on traditional rule-based security and audit controls that provide critical baseline protection but lack the flexibility needed to identify advanced fraud, insider abuse, and emerging tax compliance risks. The reviewed literature (Maulana et al., Gupta and Singh, Saha, and Suresh Dodda) shows that ML and AI can strengthen tax compliance, payroll fraud prediction, and payroll automation, while also revealing common limitations in empirical validation, real-time deployment, and transparency. The proposed taxonomy organizes the discussed ML algorithms into supervised models for known payroll errors and tax miscalculations, unsupervised models for novel ghost employees and salary anomalies, deep learning and time-series models for multi-cycle tax drift, and user behavior analytics for insider threat and privilege misuse.

Together, these methods show good potential for enabling proactive fraud detection, real-time surveillance, and ongoing compliance; they enhance detection accuracy, minimize false positives, and improve audit readiness with minimal manual effort by using historical and real-time payroll data. However, practical concerns remain, especially regarding data quality, model transparency, privacy protection, and seamless adoption within existing ERP systems and regulatory provisions. Future work should therefore focus on explainable and trustworthy AI models to increase regulatory acceptance, privacy-preserving learning approaches such as federated learning, and hybrid security systems that integrate domain knowledge with adaptive ML intelligence. In addition, large-scale empirical assessments across varied industries and jurisdictions are necessary to guarantee the high assurance, scalability, and sustainability of ML-based payroll security in ERP tax systems.

REFERENCES

[1] A. Terminanto, H. A. Swantoro, and A. N. Hidayanto, "Configurations and implementation of payroll system using open source erp: a case study of Koperasi PT Sri," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 277, no. 1, p. 12036, Dec. 2017, doi: 10.1088/1757-899X/277/1/012036.

[2] 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.

[3] C. Tayal, "Secure Data Integration Frameworks for Omni- channel Healthcare Marketing Systems," *Int. J. Eng. Res. Technol.*, vol. 14, no. 10, 2025, doi: 10.5281/zenodo.18080743.

[4] P. Iancu *et al.*, "EMSYS - Human Resources and Payroll Management Integrated Information System," vol. 29, pp. 1633–1638, 2012, doi: 10.3303/CET1229273.

[5] S. Matende and P. Ogao, "Enterprise Resource Planning (ERP) System Implementation: A Case for User Participation," *Procedia Technol.*, vol. 9, pp. 518–526, 2013, doi: 10.1016/j.protcy.2013.12.058.

[6] A. Meshram, "Hybrid Cloud Strategy For Mission Critical Financial Software Applications," *Int. J. Adv. Res. Comput. Commun. Eng*, vol. 14, no. 12, 2025.

[7] S. Gondi, "Fintech Transformation: Ai And Rpa Bots For Multi-Agency Payment Reconciliation In Erp," *Int. J. Appl. Math.*, vol. 38, no. 10s, pp. 304–331, Nov. 2025, doi: 10.12732/ijam.v38i10s.944.

[8] D. Shah, S. Khade, and S. Pawar, "Anomaly Detection in Time Series Data of Sensex and Nifty50 With Keras," in *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2021, pp. 433–438. doi: 10.1109/ESCI50559.2021.9396979.

[9] M. R. N. M. Qureshi, "Evaluating Enterprise Resource Planning (ERP) Implementation for Sustainable Supply Chain Management," *Sustain.*, vol. 14, no. 22, 2022, doi: 10.3390/su142214779.

[10] 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.

[11] T. tiên Nguyễn and T. T. Trương, "A literature review of ERP system, challenges and opportunities of ERP implementation on organization," *Tạp Chí Khoa Học Trường Đại Học Quốc Tế Hồng Bàng*, vol. 4, pp. 35–44, Jun. 2023, doi: 10.59294/HIUJS.VOL.4.2023.384.

[12] R. Palwe, "Adaptive human: AI decision support for high-stakes financial advice," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, pp. 385–392, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.226.

[13] 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.

[14] R. Kenge, "A Research Study on the ERP System Implementation and Current Trends in ERP," *Shanlax Int. J. Manag.*, vol. 8, pp. 34–39, 2020, doi: 10.34293/management.v8i2.3395.

[15] T. Maulana, W. Agustika, A. Budiyono, and R. Ardelia, "Feasibility of Enterprise Resource Planning System Architecture for Payroll System with Service-Oriented Architecture," *Int. J. INFORMATICS Vis.*, vol. 10, no. January, pp. 42–56, 2026, doi: 10.62527/joiv.10.1.3639.

[16] P. Gupta and V. Singh, "Enhancing Tax Technology with AI/ML: Monitoring ERP Transactions for Real-Time Compliance and Efficiency," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 5, pp. 1317–1321, May 2025, doi: 10.22214/ijraset.2025.70477.

[17] 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.

[18] 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, no. 3, 2025, doi: 10.63282/3050-9262.IJAIDSML-V6I3P113.

[19] S. Sarferaz, "ERP Reference Architecture," in *Embedding Artificial Intelligence into ERP Software*, Cham: Springer Nature Switzerland, 2024, pp. 71–91. doi: 10.1007/978-3-031-54249-7_4.

[20] L. Urpanen, P. Lic, and A. Tuomisto, "Usability of SAP ERP HCM and Workarounds: A Case Study on Payroll Productivity and Organizational Efficiency from an Employee Perspective," 2024.

[21] D. Singh, C. Rajasthan, and S. C. Jain, "Working process of Payroll in SAP HR Module," *Int. J. Emerg. Res. Manag. Technol.*, pp. 51–57, 2013.

[22] S. K. Das, "Smart Investing: Understanding Participant Default Investment Allocations in Retirement Plans," *Adv. Consum. Res.*, vol. 2, no. 04, pp. 3871–3878, 2025.

[23] F. A. Tuli and S. Kaluvakuri, "Implementation of ERP Systems in Organizational Settings: Enhancing Operational Efficiency and Productivity," *Asian Bus. Rev.*, vol. 12, no. 3, pp. 89–96, 2022, doi: 10.18034/abr.v12i3.676.

[24] C. Patel, "Customer Experience Optimization Using Machine Learning : A Systematic Review," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 176–187, 2023, doi: 10.56472/25832646/JETA-V3I8P120.

[25] M. Haddara and O. Zach, "ERP Systems in SMEs: An Extended Literature Review," *Int. J. Inf. Sci.*, vol. 2, no. 6, pp. 106–116, 2012, doi: 10.5923/j.ijis.20120206.06.

[26] 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.

[27] P. Chandrashekar, "Data-Driven Loan Default Prediction: Enhancing Business Process Workflows with Machine Learning," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, pp. 18–26, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P103.

[28] 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.

[29] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[30] T. Shah, "The Role of Customer Data Platforms (CDPs) in Driving Hyper-Personalization in FinTech," *Int. Res. J. Eng. Sci. Technol. Innov.*, 2025.

[31] A. Parupalli, "Business-Oriented Employee Performance Assessment via Machine Learning in ERP Systems," *TIJER – Int. Res. J.*, vol. 11, no. 11, 2024.

[32] S. Meenugu, "AI and ML in payroll automation: A technical perspective," *World J. Adv. Eng. Technol. Sci.*, vol. 15, pp. 1542–1552, 2025, doi: 10.30574/wjaets.2025.15.1.0379.

[33] E. Swathi, "A Study on Developing a Payroll Management System based on Employee Performance for Dinakara Life Sciences Pvt . Ltd .," vol. 8, no. October, pp. 31–38, 2022.

[34] H. P. Kapadia, "Reducing Cognitive Load in Online Financial Transactions," *Int. J. Curr. Sci.*, vol. 12, no. 2, pp. 732–797, 2022.

[35] G. Mantha, "Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency," *North Am. J. Eng. Res.*, vol. 5, no. 3, 2024.

[36] M. M. Aliyu, S. I. Zimit, A. Ahmad, and A. I. Fagge, "Integrated Payroll System A Design Science Approach," *Irjet*, vol. 8, no. 6, pp. 759–767, 2021.

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.

7. 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.
8. 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.
9. 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.
10. 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.
11. 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
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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