International Journal of Scientific Interdisciplinary Research

Volume: 7; **Issue:** 1
Pages: 37-71

AI-Based Revenue Leakage Detection Models Using Transaction-Level Financial Data: A Review

Md. Fardous[1];

[1]. *Master in Information Technology: Data Analysis & Management; Washington University of Science & Technology, Alexandria, USA; Email: fardous01@gmail.com*

Doi: 10.63125/5h2n0g69
Received: *24 November 2025;* ***Revised:*** *21 December 2025;* ***Accepted:*** *17 January 2026;* ***Published:*** *09 February 2026*

Abstract

AI-based revenue leakage detection using transaction-level financial data has gained importance due to increasing pricing complexity, automated billing processes, and high-volume digital transactions. This study quantitatively examined four detection constructs—pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring—and evaluated their relationships with overall revenue leakage detection effectiveness. A structured survey design was applied, and responses were collected from 210 participants across transaction-intensive industries, including telecommunications (22.4%), e-commerce/retail (21.0%), healthcare/insurance (18.6%), and financial services (17.1%). Most respondents reported direct involvement in revenue-cycle activities (61.0%), and 75.7% reported intermediate-to-advanced familiarity with analytics and AI tools. Descriptive results indicated consistently positive construct scores, with mean values of 4.12 (SD = 0.61) for pricing compliance detection, 4.08 (SD = 0.65) for authorization integrity, 3.94 (SD = 0.70) for temporal anomaly identification, 3.89 (SD = 0.74) for adjustment behavior monitoring, and 4.05 (SD = 0.63) for leakage detection effectiveness. Reliability analysis confirmed strong internal consistency, with Cronbach's alpha values ranging from 0.81 to 0.88 across constructs. Multiple regression analysis demonstrated that the predictors jointly explained substantial variance in leakage detection effectiveness ($R^2 = 0.62$; adjusted $R^2 = 0.61$; $F = 83.40$; $p < .001$). Pricing compliance detection produced the strongest standardized effect ($\beta = 0.38$; $t = 6.52$; $p < .001$), followed by authorization integrity ($\beta = 0.29$; $t = 5.11$; $p < .001$), adjustment behavior monitoring ($\beta = 0.21$; $t = 3.88$; $p < .001$), and temporal anomaly identification ($\beta = 0.17$; $t = 3.09$; $p = .002$). Multicollinearity remained acceptable (VIF = 1.41–1.72). Hypothesis testing supported 4 of 5 hypotheses (80%), with one interaction hypothesis rejected ($\beta = 0.06$; $p = .118$). Overall, the findings demonstrated that effective transaction-level revenue leakage detection was strongly associated with pricing integrity, governance controls, temporal monitoring, and adjustment analytics.

Keywords

AI, Revenue Leakage, Transactions, Detection, Analytics

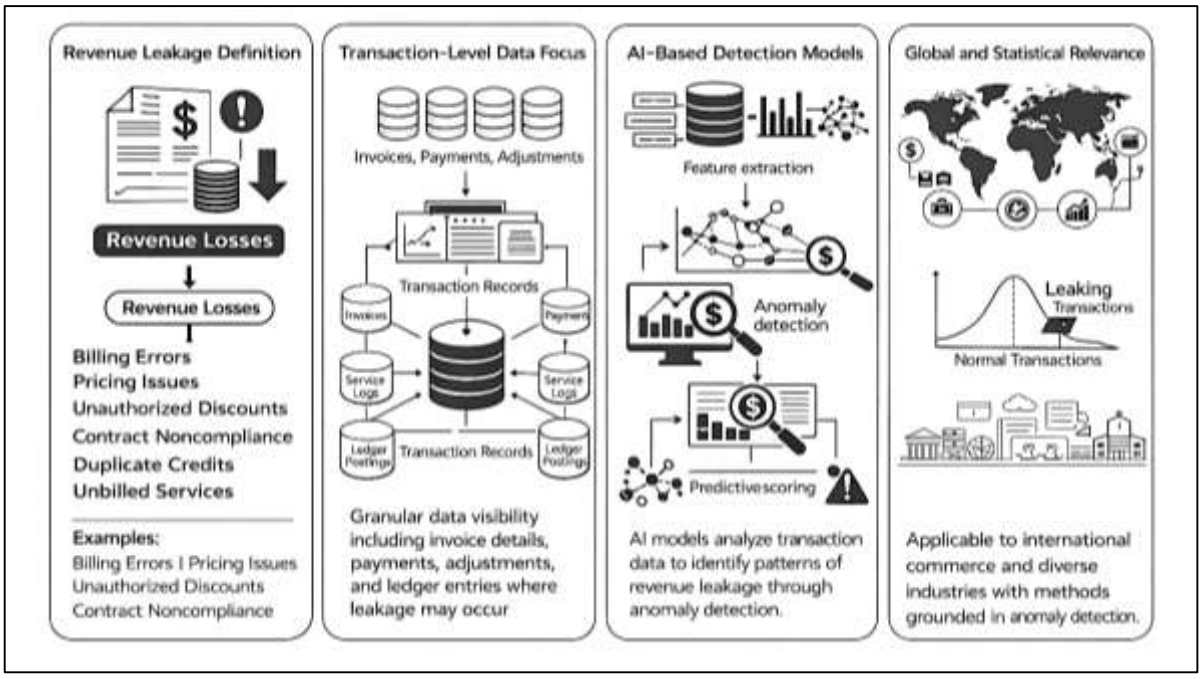
INTRODUCTION

Revenue leakage is defined as the systematic loss of earned revenue resulting from inaccuracies, inefficiencies, or failures in transactional, operational, or financial processes that prevent full revenue realization (Abed et al., 2022). These losses occur after value has been delivered but before revenue is correctly recorded, collected, or recognized. Revenue leakage manifests across billing errors, pricing inconsistencies, unauthorized discounts, contract noncompliance, incorrect tax application, duplicate credits, unbilled services, delayed invoicing, and settlement mismatches. Unlike broad financial underperformance, revenue leakage is embedded within transaction-level activities, making it difficult to detect through aggregated financial statements alone. Transaction-level financial data, which includes invoice line items, payment records, adjustments, credit notes, service logs, and ledger postings, provides the granular visibility necessary to identify these losses. In high-volume digital and enterprise environments, leakage often appears as small deviations dispersed across millions of transactions, accumulating into material financial impact over time (Kadhim & Ani, 2023; Ashraful et al., 2020; Rauf, 2018). Quantitative research treats revenue leakage as a measurable deviation between expected and realized transaction outcomes, positioning it as a data-driven control problem rather than a purely managerial or procedural issue. Artificial intelligence-based detection models formalize this perspective by representing transactions as structured data objects and estimating the probability that each object reflects revenue erosion. This framing aligns revenue leakage detection with anomaly identification, pattern recognition, and classification tasks in applied data science. The definition of revenue leakage therefore extends beyond intentional misuse to include unintentional errors, system misconfigurations, and process drift, all of which can be captured empirically through transaction attributes (Allioui & Mourdi, 2023; Haque & Arifur, 2021; Fokhrul et al., 2021). By grounding the concept in observable financial records, AI-based detection approaches enable quantitative assessment, comparison, and replication across organizational and sectoral contexts. The definitional clarity of revenue leakage at the transaction level establishes the analytical foundation for modeling, evaluation, and synthesis in quantitative review research.

Revenue leakage holds international significance due to the globalization of commerce, digital service delivery, and cross-border financial operations. Multinational organizations operate across diverse regulatory regimes, currencies, tax systems, and contractual standards, increasing transactional complexity and exposure to misalignment between operational events and financial recognition (Fahimul, 2022; Yoon et al., 2021; Zaman et al., 2021). Global supply chains generate large volumes of intercompany transactions, usage-based charges, and deferred revenue adjustments that must be reconciled accurately across systems and jurisdictions. In sectors such as telecommunications, healthcare, transportation, energy, e-commerce, and financial services, revenue leakage directly affects pricing integrity, affordability, and fiscal sustainability. Public and regulated industries face additional pressure because leakage undermines budgetary planning and accountability. The international expansion of subscription models, digital platforms, and automated billing systems has further amplified the scale and velocity of transaction data, rendering manual oversight insufficient (Hammad, 2022; Hasan & Waladur, 2022; Saadullah & Elsayed, 2020). AI-based revenue leakage detection addresses this challenge by enabling continuous evaluation of entire transaction populations rather than relying on periodic sampling. From a quantitative perspective, international datasets introduce heterogeneity in customer behavior, pricing logic, and operational workflows, requiring models that can generalize across contexts while preserving sensitivity to local deviations. Transaction-level modeling supports this requirement by isolating unit-level anomalies rather than relying on country-level aggregates. The international relevance of revenue leakage detection is also methodological, as it highlights challenges related to data integration, multilingual master data, and inconsistent accounting structures (Rashid & Praveen, 2022; Arifur & Haque, 2022; Reim et al., 2022). These challenges influence feature construction, labeling accuracy, and model validation. As organizations increasingly rely on automated systems to manage global revenue streams, AI-based detection models serve as analytical mechanisms for maintaining financial integrity across distributed operations. The global scope of revenue leakage therefore reinforces the importance of scalable, data-driven detection frameworks that operate at the level where losses originate.

AI-based revenue leakage detection models conceptualize transaction data as structured numerical and categorical inputs that encode financial, temporal, relational, and procedural information. Quantitative modeling begins by transforming raw transaction records into features that capture expected revenue behavior, such as unit pricing consistency, discount authorization depth, billing frequency, adjustment rates, and reconciliation gaps (Chang et al., 2020; Towhidul et al., 2022; Ratul & Subrato, 2022). Supervised learning approaches frame leakage detection as a classification problem in which historical cases of confirmed leakage inform model training. Unsupervised and semi-supervised approaches treat leakage as deviation from learned norms, enabling detection when labeled data is scarce or incomplete. These modeling paradigms reflect broader quantitative research in anomaly detection and imbalanced classification. Transaction-level financial data is particularly suited to these methods because it contains repeated patterns governed by business rules, making deviations statistically distinguishable (Dora et al., 2020; Rifat & Jinnat, 2022; Rifat & Alam, 2022). Quantitative studies emphasize the importance of feature engineering grounded in accounting logic, as features derived from contractual alignment and control checkpoints often outperform purely statistical outlier measures. Ensemble methods combine multiple weak signals to improve robustness, while probabilistic scoring enables prioritization rather than binary decision-making (Abdulla & Majumder, 2023; Fahimul, 2023). The quantitative literature also addresses class imbalance, recognizing that leakage events represent a small fraction of transactions. Performance evaluation therefore relies on precision-focused metrics rather than aggregate accuracy. By framing revenue leakage detection as a measurable learning task, AI-based models enable systematic comparison across algorithms, datasets, and industries (Babaei et al., 2024; Faysal & Bhuya, 2023; Habibullah & Aditya, 2023). This modeling foundation supports quantitative synthesis by providing a shared analytical language for describing detection performance and design choices.

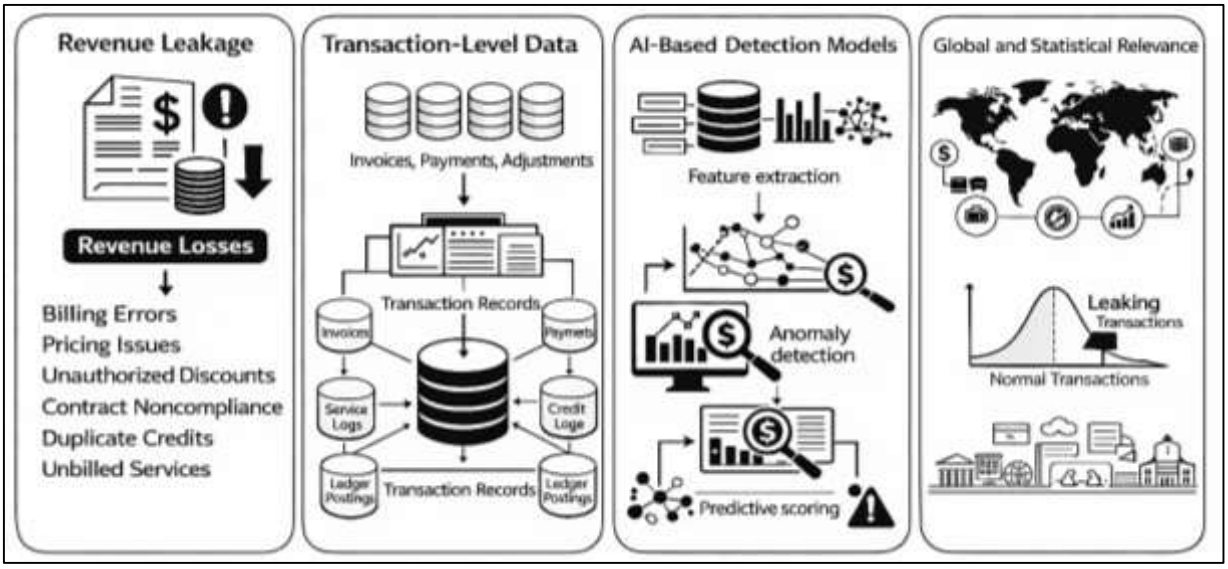
Figure 1: AI Revenue Leakage Detection



Transaction-level financial data exhibits structural characteristics that significantly influence AI-based revenue leakage detection. Transactions are inherently relational, linking customers, products, contracts, locations, employees, and systems through identifiers that form complex interaction networks (Babaei et al., 2024; Hammad & Mohiul, 2023; Haque & Arifur, 2023). Leakage frequently emerges at the intersection of these relationships, making isolated field-level analysis insufficient. Transactions are also temporal, forming sequences of events such as order creation, fulfillment, invoicing, adjustment, and settlement. Temporal ordering and timing gaps carry meaningful information about process integrity. Financial transaction data is heterogeneous, combining numerical

values, categorical codes, timestamps, and textual descriptors, which necessitates careful preprocessing and normalization (Jahangir & Mohiul, 2023; Rashid et al., 2023; Yan, 2023). Missing or delayed data introduces noise that must be addressed to avoid biased detection. Label availability is limited, as confirmed leakage cases are often identified through audits or disputes, creating selection bias. Quantitative research highlights the importance of addressing this bias through robust validation strategies. The granularity of analysis further affects detection sensitivity, as leakage may be observable at the line-item level but obscured at higher aggregation levels. These structural properties require models that balance expressiveness with interpretability, particularly in financial environments where investigation and remediation follow detection (Li et al., 2024; Khaled & Mosheur, 2023; Mostafa, 2023). Transaction-level modeling allows for precise attribution of leakage risk to specific records, enabling alignment with operational workflows. Understanding the data structure is therefore central to interpreting empirical results and comparing findings across studies.

Figure 2: AI Revenue Leakage Detection Models



The primary objective of this review is to systematically examine and synthesize AI-based revenue leakage detection models that operate on transaction-level financial data, with emphasis on how these models identify, classify, and prioritize revenue loss events embedded within large-scale financial records. This objective is grounded in the need to understand revenue leakage as a measurable and data-driven phenomenon that occurs through billing errors, pricing inconsistencies, unbilled services, unauthorized adjustments, incorrect tax application, settlement mismatches, duplicate credits, and process-level breakdowns that reduce realized revenue. The review aims to evaluate how transaction-level inputs such as invoice line items, payment histories, refund logs, credit memos, contract attributes, timestamps, account identifiers, product codes, and ledger postings are transformed into analytical features for AI modeling. A central objective is to compare detection paradigms across rule-based systems, supervised machine learning, semi-supervised learning, and unsupervised anomaly detection approaches, focusing on differences in accuracy behavior, sensitivity to rare leakage events, and robustness under class imbalance. Another objective is to assess the role of feature engineering strategies that incorporate accounting logic, reconciliation rules, authorization hierarchies, and pricing compliance indicators, and to identify how these strategies influence model interpretability and investigative usability. The review further aims to analyze evaluation practices reported in the literature, including the definition of ground truth leakage labels, validation design choices, handling of time-ordering in transaction streams, and selection of performance metrics aligned with imbalanced detection problems. An additional objective is to examine the integration requirements of these models within enterprise financial ecosystems, including data quality constraints, system interoperability, and governance considerations such as auditability, traceability, and model risk oversight. Finally, this review seeks to develop a structured taxonomy that organizes the existing body of research by data

type, industry context, algorithmic approach, and evaluation methodology, enabling clear comparison across studies and supporting a coherent understanding of how AI-based transaction analytics is currently applied to revenue leakage detection at scale.

LITERATURE REVIEW

The literature on revenue leakage detection has expanded alongside the growth of digital transactions, automated billing systems, and data-intensive financial operations. As organizations increasingly rely on high-volume, transaction-level financial data, traditional revenue assurance mechanisms have proven insufficient for identifying subtle, distributed revenue losses embedded within complex operational workflows (Marzuki et al., 2022). The literature review section examines prior scholarly and applied research that addresses the detection of revenue leakage through analytical, statistical, and artificial intelligence-based approaches. This body of work spans multiple disciplines, including accounting information systems, financial analytics, anomaly detection, fraud analytics, and applied machine learning, each contributing distinct methodological perspectives to the problem of revenue loss identification (Rifat & Rebeka, 2023; Azam & Amin, 2023). This review focuses specifically on studies that utilize transaction-level financial data as the primary analytical unit, reflecting a shift from aggregate financial ratios toward granular, data-driven detection techniques. The reviewed literature conceptualizes revenue leakage as a pattern recognition problem in which deviations between expected and realized revenue outcomes can be inferred from transactional attributes such as pricing, timing, authorization, reconciliation status, and adjustment behavior. Prior research has explored a wide range of detection models, including rule-based validation systems, supervised classification algorithms, unsupervised anomaly detection techniques, and hybrid frameworks that combine accounting logic with statistical inference (Jahangir & Hammad, 2024; Kao & Tsay, 2023; Masud & Hammad, 2024). The literature also reveals substantial variation in data preparation strategies, feature engineering practices, labeling methodologies, and performance evaluation metrics, which complicates direct comparison across studies. Differences in industry context, transaction structure, and system architecture further influence model design and reported effectiveness. This section therefore synthesizes existing research by organizing it around quantitative modeling approaches, data characteristics, validation frameworks, and operational integration considerations (Md & Sai Praveen, 2024; Rifat & Rebeka, 2024; Wu et al., 2021). By systematically structuring prior findings, the literature review establishes a coherent analytical foundation for understanding how AI-based models have been applied to revenue leakage detection using transaction-level financial data and identifies dominant methodological patterns within the field.

Revenue Leakage in Transaction-Level Financial Systems

Revenue leakage in transaction-level financial systems is most effectively conceptualized as the loss of legitimately earned revenue caused by failures in capturing, pricing, billing, collecting, reconciling, or recording transactional events in a manner consistent with the economic exchange that actually occurred (Sai Praveen, 2024; Zhou et al., 2021). At this level, revenue leakage is not defined as a broad decline in profitability or a general shortfall in financial performance, but rather as a measurable discrepancy embedded within specific transaction records. Transaction-level definitions emphasize that revenue leakage can occur even when products are delivered, services are provided, or contractual obligations are fulfilled, because the financial representation of those events may be incomplete, inaccurate, delayed, or misaligned with authorized revenue rules (Shehwar & Nizamani, 2024; Shoflul Azam & Amin, 2024). This conceptualization becomes increasingly relevant in environments where organizations process millions of transactions across digital platforms, subscription billing systems, point-of-sale networks, enterprise invoicing systems, or claims-based reimbursement systems. In such settings, leakage is rarely concentrated in one visible event; it tends to appear as small, distributed losses across numerous records, which collectively accumulate into financially material outcomes. Transaction-level revenue leakage is therefore framed as a record-specific control failure rather than a purely strategic or managerial weakness (Begum, 2025; Faysal & Aditya, 2025; Nicholls et al., 2021). The literature also conceptualizes leakage as a multi-causal phenomenon, meaning that the same leakage outcome may originate from different underlying mechanisms, such as system misconfiguration, workflow drift, data quality inconsistencies, unauthorized adjustments, incomplete billing triggers, or reconciliation mismatches across systems. Importantly, transaction-level definitions

treat leakage as inclusive of both intentional and unintentional forms, since the primary analytical goal is detection and correction rather than attribution of motive. This definition supports the development of AI-based detection models because it enables leakage to be operationalized as an observable pattern in structured financial data. When leakage is defined at the transaction level, it becomes possible to model it using measurable attributes such as billed amount, expected amount, pricing rules, discount depth, adjustment frequency, payment status, timing gaps, and reconciliation flags (Staszkiewicz & Werner, 2021). By anchoring the concept in the microstructure of financial events, transaction-level definitions provide a stable foundation for quantitative analysis and enable consistent comparison across industries where revenue cycles differ but transactional integrity remains a universal requirement.

Figure 3: Transaction-Level Revenue Leakage Framework

Aspect	Description	Examples
Pre-Billing Leakage	Billable activities are not captured or transmitted into the billing system	• Uncaptured services • Missing usage logs • Integration failures
Billing-Stage Leakage	Invoices are generated incorrectly or with inaccurate details	• Missing line items • Misapplied taxes • Incorrect pricing
Post-Billing Leakage	Excessive credits or unauthorized adjustments reduce recorded revenue	• Excessive refunds • Unauthorized write-offs • Credit memo misuse
Settlement-Stage Leakage	Discrepancies occur during payment reconciliation or settlement	• Payment mismatches • Delayed settlements • Chargeback exposure

The literature consistently distinguishes revenue leakage from billing error, under collection, and pricing noncompliance by focusing on the origin of the deviation and the point in the revenue cycle where financial loss is introduced. Billing error is generally defined as an incorrect representation of charges on an invoice or billing statement, including missing line items, incorrect quantities, duplicate charges, incorrect customer mapping, and misapplied tax codes (Hammad & Hossain, 2025; Jahangir, 2025; Vashisth et al., 2024). Billing errors are often directly observable within invoice data because they produce internal inconsistencies between billing outputs and operational inputs such as service logs or delivery records. Under collection, in contrast, refers to the failure to realize cash inflow after correct billing has occurred (Jamil, 2025; Md Syeedur, 2025). This includes partial payments, late payments, unpaid balances, chargebacks, settlement shortfalls, and disputed transactions that result in reduced cash realization. Under collection is typically more visible in payment and accounts receivable records than in invoicing data, and its causes often relate to customer behavior, credit risk policies, payment processing mechanisms, or dispute management practices. Pricing noncompliance is conceptualized as deviation from authorized pricing rules, such as contract rates, rate cards, discount thresholds, promotion policies, or pricing governance frameworks. Pricing noncompliance can occur through manual overrides, incorrect configuration of pricing logic, inconsistent application of contract terms, or unauthorized discounting (Amin, 2025; Towhidul & Rebeka, 2025; Tatulli et al., 2023). It often appears as a systematic pattern across transactions associated with particular products, channels, or sales roles. Revenue leakage is broader than all three concepts because it includes them while also capturing additional loss mechanisms that do not fall neatly into any single category. For example, revenue leakage includes unbilled service delivery, delayed invoicing that results in write-offs, incorrect revenue allocation, excessive adjustments, and reconciliation failures between operational systems and financial ledgers. The distinction matters in transaction-level modeling because each

category generates different data signals and requires different feature representations. A billing error may be detected through invoice integrity checks, while under collection requires settlement and payment timeline analysis. Pricing noncompliance requires contract-aware features and authorization hierarchy variables (Ratul, 2025; Rifat, 2025; Zhou et al., 2023). Revenue leakage detection models must therefore be designed with conceptual clarity regarding which type of deviation is being targeted, because combining these categories without distinction can reduce interpretability and inflate false positives. The literature emphasizes that a well-defined separation of these constructs improves analytical precision, enables more accurate labeling strategies, and supports better alignment between detection outputs and operational remediation workflows.

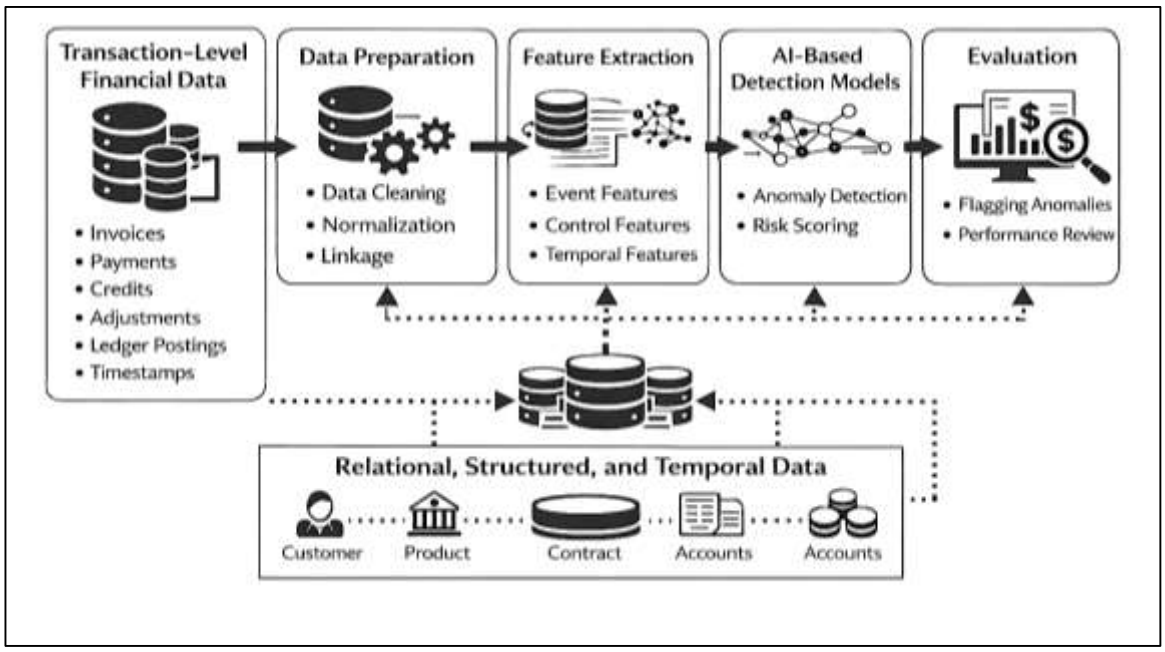
Transaction-Level Financial Data

Transaction-level financial data forms the empirical foundation for revenue leakage detection research because it captures revenue-related events at the level where operational activity becomes financially represented (Li et al., 2022). The literature describes transaction-level datasets as structured collections of discrete records that document economic exchanges, obligations, and settlements through standardized fields such as transaction identifiers, counterparties, product or service codes, quantities, unit prices, totals, tax and fee attributes, timestamps, approval markers, status flags, and system source indicators. These datasets are typically generated through enterprise systems and digital platforms that record business activity continuously, producing high volumes of entries that may span invoices, receipts, claims, subscriptions, and ledger postings. The transactional structure is often hierarchical, with headers representing a document-level entity such as an invoice or claim, and line items representing the granular revenue components that drive pricing and revenue allocation. This hierarchical design supports analytical decomposability, allowing researchers to model leakage at multiple levels of granularity, including line-item, document, customer, product, or account level. Studies also characterize transaction datasets as relational because they connect entities across master data tables, including customers, vendors, contracts, products, locations, and employees, which enables the detection of leakage patterns associated with specific relationships rather than isolated numeric values (Q. Zhang et al., 2024). The literature further emphasizes that transaction-level datasets contain both "event" attributes that describe what happened and "control" attributes that describe how the event was authorized, processed, and posted, such as discount approvals, exception codes, adjustment reasons, billing triggers, and reconciliation status. This dual nature is central to leakage detection because revenue loss is frequently associated with control failure rather than with a single incorrect amount. Researchers routinely treat the dataset as a representation of the end-to-end revenue cycle, where each record includes enough contextual signals to infer whether the transaction reflects compliant revenue capture. In many industries, transaction-level financial data also contains cross-system identifiers that allow linkage between operational events and financial outcomes, such as order numbers, shipment numbers, service session identifiers, or usage event markers (Gupta et al., 2023b). The literature recognizes that the analytic value of transaction datasets is not merely their size but their structured repeatability, which enables detection models to learn normal patterns and highlight deviations. This foundation supports a quantitative lens where revenue leakage is not examined through broad financial aggregates, but through the micro-level structure of financial evidence embedded in individual records(Wilkoff & Yildiz, 2023) .

Transaction-level revenue leakage research repeatedly centers on the core financial artifacts that shape realized revenue, namely invoice line items, payments, credits, adjustments, and ledger postings. Invoice line items are treated as the most critical unit of analysis because they represent the priced components of delivered value and contain the pricing logic where revenue deviations often originate. Line items typically include quantities, unit prices, discount amounts, tax codes, fee components, and references to products or services, creating a detailed representation of how revenue is constructed (Staszkiewicz & Werner, 2021). Payment records, by contrast, represent realized cash flows and provide evidence about whether billed revenue was collected in full, partially collected, delayed, disputed, or reversed. The literature treats payments as both a validation mechanism and a leakage signal because persistent gaps between invoiced amounts and settled amounts can indicate under collection, reconciliation failures, or dispute-related revenue erosion. Credits and credit memos represent reductions in billed amounts and are frequently analyzed as leakage-sensitive artifacts because they

can reflect legitimate corrections, customer satisfaction actions, contract adjustments, or misuse. Transaction-level studies emphasize that credit activity often includes reason codes, authorization levels, and patterns of repetition that allow detection models to separate routine corrections from anomalous refund or credit behavior. Adjustments, including rebills, reversals, write-offs, manual journal entries, and post-invoice modifications, are widely discussed as high-risk transaction classes because they alter the revenue outcome after the original billable event. The literature describes adjustments as essential to analyze because they are both necessary in real systems and vulnerable to process weakness, inconsistent governance, and improper handling (Yousuf et al., 2025; Azam, 2025; Wu et al., 2021). Ledger postings translate transactional activity into the accounting system, recording revenue recognition, receivable balances, and related accounts. Researchers treat the linkage between subledger transactions and general ledger postings as a primary integrity pathway, because mismatches between operational billing records and ledger postings create both reporting risk and operational leakage (Tasnim, 2025; Zaheda, 2025b). The literature commonly highlights that these transaction artifacts do not exist independently; they form chains where an operational event generates a billable item, an invoice aggregates items, payments settle invoices, and ledger postings record outcomes. Leakage emerges when any link in this chain is missing, duplicated, misclassified, or incorrectly valued (Klein et al., 2023; Zaheda, 2025a; Zulqarnain, 2025). The combined analysis of invoices, payments, credits, adjustments, and postings supports more reliable detection because it provides multiple perspectives on the same revenue event. Transaction-level research therefore frames these artifacts as complementary sources of evidence and emphasizes that effective leakage detection requires modeling across them rather than treating revenue capture as a single-table problem.

Figure 4: Transaction-Level Revenue Leakage Detection

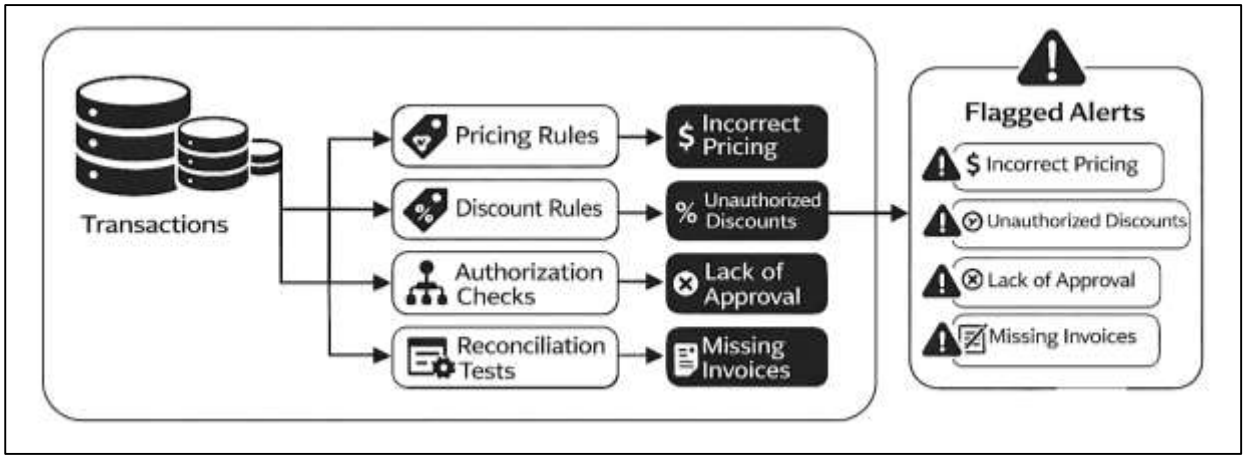


Rule-Based Revenue Leakage Detection Models

Rule-based revenue leakage detection models using transaction-level data are commonly conceptualized as structured control mechanisms that operationalize organizational policies into deterministic tests applied directly to invoices, payments, credits, and ledger postings (Huong et al., 2024). Within the literature, business-rule encoding is presented as the translation of pricing policies, contract terms, discount governance, tax logic, approval hierarchies, and reconciliation requirements into explicit conditions that can be automatically checked against transaction attributes. Pricing rules often include validations that compare billed unit prices to authorized rate cards, contract schedules, service tiers, or location-based price tables, while discount rules verify that discount depth remains within permitted bounds for a given role or customer category. Authorization checks are frequently

encoded through approval-chain requirements, where specific discount levels, credits, write-offs, or adjustments require matching authorization markers or workflow statuses. Reconciliation checks focus on completeness and consistency across systems, such as ensuring that all fulfilled orders have corresponding invoice line items, that invoice totals reconcile with subledger postings, and that settled payment amounts align with recorded receivables after accounting for authorized adjustments (Li et al., 2022). The literature treats these rules as practical embodiments of internal controls, because they reflect organizational definitions of "correct" transaction behavior. Rule libraries are typically organized into domains such as pricing integrity, billing completeness, exception handling, tax and fee compliance, credit management, and payment reconciliation. This structure supports targeted detection because each rule category aligns with a specific leakage origin and produces interpretable outputs suitable for audit review. Transaction-level rule encoding also relies on standardized reference data such as contract tables, approved discount matrices, tax jurisdiction mappings, and chart-of-account rules. As a result, the literature emphasizes that rule effectiveness depends not only on the logic itself but also on the quality and stability of reference data. The rules are applied across high volumes of transactions, and each rule evaluation produces a binary result or an exception category flag that indicates whether the transaction meets compliance criteria (Gupta et al., 2023a). This approach is widely viewed as foundational in revenue assurance contexts because it mirrors the control logic of financial governance and allows detection to be aligned directly with documented policies. Rule-based systems therefore remain prominent in the literature because they provide a clear and controllable method for detecting revenue leakage risks at the level of individual transactions while preserving operational interpretability.

Figure 5: Rule-Based Revenue Leakage Detection



The literature repeatedly emphasizes several strengths of rule-based detection models, particularly their alignment with internal control compliance, interpretability, and operational traceability. A primary strength is that rule-based systems express organizational expectations explicitly, enabling direct mapping between detection outputs and control objectives such as authorization, completeness, accuracy, and reconciliation (Kute et al., 2021). Because each rule corresponds to a specific policy requirement, the resulting exceptions are inherently interpretable, supporting rapid validation and remediation by finance, audit, and billing teams. This interpretability is repeatedly cited as a practical advantage in environments where stakeholders require clear explanations for alerts and must document corrective actions. Rule-based systems also support standardization of revenue assurance practices by applying the same validation logic consistently across all transactions, reducing reliance on individual reviewer judgment. The literature describes this consistency as beneficial for governance because it allows organizations to demonstrate uniform control application across business units and time periods. Another strength is that rule-based detection can be implemented with limited historical labels, since rules do not require training data (Nicholls et al., 2021). This is particularly important in revenue leakage contexts where confirmed leakage cases may be sparse, selectively documented, or

difficult to label reliably. Rule-based systems also provide immediate responsiveness to policy requirements: when a new pricing policy or approval rule is introduced, it can be encoded directly without waiting for sufficient training examples. Transaction-level rule checks are also computationally efficient for many common validations, making them suitable for high-volume processing. Many studies describe the practical role of rules in establishing baseline integrity checks that remove obvious errors and produce structured exception logs (Cheng et al., 2023). These logs can be used as compliance evidence, control testing artifacts, or operational performance indicators. The literature also notes that rules are especially effective for detecting known leakage modes with clear definitions, such as unauthorized discounts, invalid tax codes, duplicate credits, and missing mandatory approval markers. In these cases, the rule logic directly captures the violation condition and produces high precision because violations correspond closely to actionable issues. Rule-based detection is also compatible with audit workflows because it produces deterministic outputs that can be reviewed, sampled, and traced back to source records. This traceability reduces interpretive ambiguity and supports faster investigation (Ara & Ara, 2024). As a result, rule-based models are often positioned as foundational mechanisms in transaction-level revenue leakage detection systems, functioning either as standalone controls or as part of layered detection architectures that include more advanced analytics.

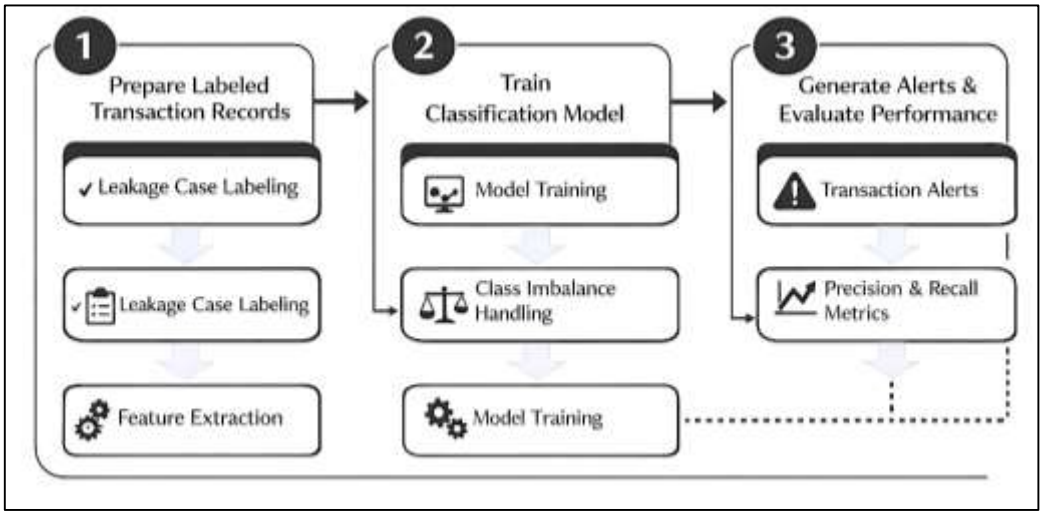
Models for Revenue Leakage Classification

The literature on supervised machine learning for revenue leakage detection commonly frames the task as a classification problem in which transaction-level records are assigned to predefined outcome categories based on observed patterns in financial and process attributes. In the binary formulation, transactions are labeled as either leakage-related or non-leakage, reflecting a decision-oriented structure that supports investigation prioritization and operational triage (Machado & Karray, 2022). In multi-class formulations, leakage is subdivided into categories such as pricing noncompliance, billing omission, unauthorized discounting, adjustment misuse, reconciliation mismatch, or under collection-related exposure, enabling more granular diagnostic outputs. This classification framing is grounded in the recognition that transaction-level datasets contain repetitive structures governed by business rules, and that leakage cases often reflect identifiable deviations within those structures. Supervised classification is therefore positioned as a method for learning decision boundaries from examples rather than encoding logic manually, allowing models to capture complex interactions among features that may not be obvious through rule-based checks alone. Studies in this area emphasize that classification design depends heavily on how leakage is conceptualized operationally, since the target label must represent a definable event that investigators can confirm and remediate. The literature also notes that classification outcomes are frequently treated as risk scores rather than absolute judgments, because the practical purpose of detection systems is often to rank transactions for review under limited investigative resources (Machado & Karray, 2022). Transaction-level classification is particularly relevant in environments where revenue processes are highly automated, producing large populations of records that cannot be reviewed manually. The literature further treats supervised classification as a bridge between traditional control validation and modern data-driven detection, because classification models can incorporate both rule-derived indicators and statistical patterns learned from historical outcomes. This framing allows supervised approaches to align with internal assurance objectives while expanding detection capacity beyond deterministic conditions. Research syntheses often categorize supervised leakage detection studies by whether they focus on event-level detection, document-level integrity, customer-level risk profiling, or adjustment-level misuse classification, reflecting different definitions of the unit of prediction. Even within a transaction-level scope, some studies treat line items as the predicted unit because leakage often originates in pricing and quantity fields, while others treat invoices or claims as the predicted unit because documents represent operational control points. Overall, the literature presents classification as the dominant supervised learning structure for revenue leakage detection because it provides a clear mapping between modeled outputs and operational actions, enabling quantitative evaluation, systematic comparison, and replicable model development using transaction-level financial data (Kazova et al., 2024).

A central theme in the supervised learning literature is the reliance on labeled transaction histories, where model training depends on historical records that have been annotated as leakage cases or

confirmed non-leakage cases through audit outcomes, dispute resolution, corrective billing actions, or internal investigation decisions. Studies emphasize that label construction is one of the most challenging components of leakage classification because revenue leakage is often underreported, inconsistently documented, or detected only after substantial delay (Khan et al., 2022). Confirmed leakage labels may originate from formal audit findings, recovered revenue events, identified billing corrections, credit reversals, or post-hoc reconciliation discoveries, each reflecting different operational pathways of confirmation. The literature discusses that these labels can vary in reliability because confirmation may depend on investigative capacity, sampling strategies, or organizational focus areas, creating a situation where the dataset reflects both leakage occurrence and detection likelihood. These influences supervised model behavior because models learn from available labels, which may not represent the full universe of leakage events. As a result, many studies emphasize careful sampling and curation of training sets to ensure that labeled positives are sufficiently representative of leakage patterns and not overly concentrated in a narrow subset of transaction types. Transaction histories used for training often include both raw transaction attributes and derived variables generated through linkage across billing, operational, and accounting systems.

Figure 6: Supervised Revenue Leakage Detection Framework

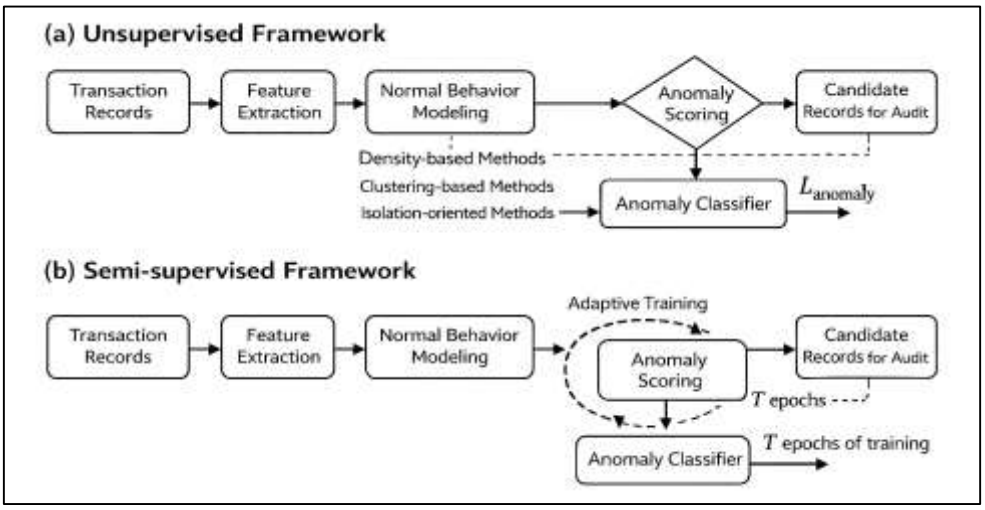


Anomaly Detection Approaches

Unsupervised and semi-supervised anomaly detection approaches in revenue leakage research are grounded in the idea that most transaction-level financial records reflect routine, policy-compliant behavior, and that leakage-related events appear as statistically uncommon deviations from this dominant pattern (Bauw et al., 2020). The literature conceptualizes "normal behavior" not as a single static profile but as a set of distributions shaped by product categories, customer segments, contract types, service tiers, billing cycles, and operational channels. Transaction distributions are therefore modeled within contextual groupings, because a value pattern that is abnormal for one cohort may be normal for another. Studies describe normal behavior modeling as an empirical characterization of typical transaction amounts, unit prices, discount depths, tax rates, adjustment frequencies, timing gaps, and reconciliation states. These patterns can be learned directly from historical data without requiring confirmed leakage labels, which makes unsupervised methods particularly attractive in leakage contexts where labeled cases are limited or biased (Zhang et al., 2023). Semi-supervised variants refine this idea by training on a curated set of transactions assumed to be clean or low risk, then scoring deviations observed in broader populations. The literature emphasizes that financial transactions have structured regularities, such as stable price bands for specific products, repeated invoice structures for subscription services, and recurring settlement patterns across payment channels. When records deviate from these regularities, they can be treated as anomaly candidates. Normal behavior modeling also extends beyond numeric distributions to categorical and relational patterns, such as unusual combinations of product codes and tax jurisdictions, atypical discount codes for certain customer

classes, or rare sequences of credits and rebills (Molan et al., 2023).

Figure 7: Unsupervised Revenue Leakage Detection Framework



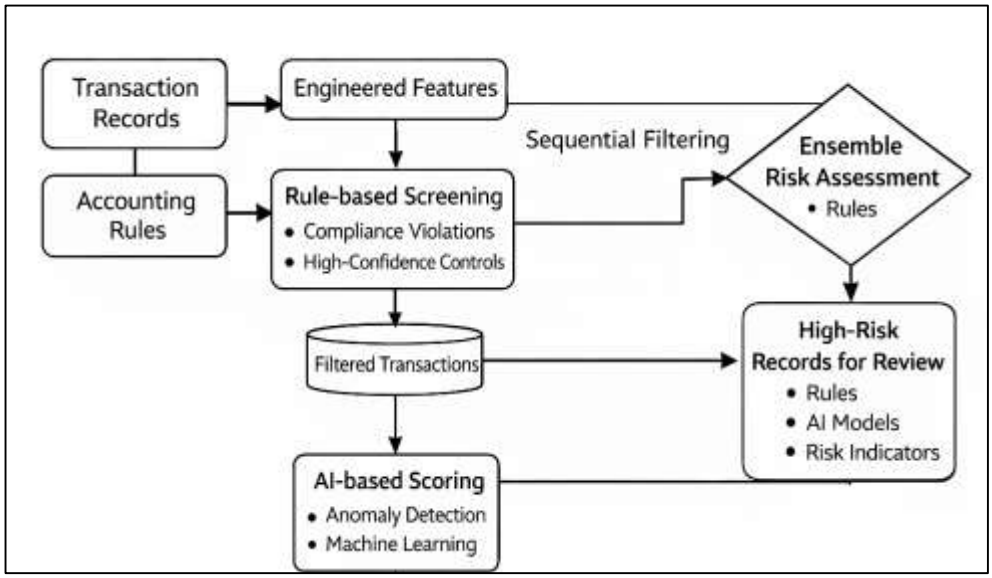
Research also highlights the importance of capturing process-based normality, such as typical lag times between service delivery and invoicing or expected timing between invoice issuance and payment settlement. By modeling the distribution of these timing attributes, anomaly detection methods can identify records that reflect abnormal process flow. The literature treats this distribution-based framing as essential for leakage detection because leakage often occurs through dispersed micro-irregularities that are difficult to label directly but become identifiable when compared against learned baselines. Normal behavior modeling also supports scalable monitoring because it can be applied to large transaction populations repeatedly, generating anomaly scores that indicate the degree of deviation. Across studies, the key contribution of this approach lies in its ability to generate leakage candidates from the data itself, allowing organizations to detect unknown or evolving leakage patterns without relying on predefined rules or extensive labeled datasets (Kim et al., 2022).

Hybrid Detection Frameworks Combining Rules and AI Models

Hybrid detection frameworks combining rules and AI models are widely discussed in the literature as practical architectures for revenue leakage detection because they merge the interpretability of accounting controls with the adaptive pattern-recognition capacity of machine learning. A foundational strategy in these frameworks is the integration of accounting rules as engineered features, where deterministic compliance checks are transformed into structured variables that become inputs for statistical or machine learning models (Uccello et al., 2024). Rather than using rules only as binary flags for exception reporting, studies describe how rule outputs can be encoded as categorical indicators, severity scores, violation counts, or grouped compliance profiles that summarize transaction integrity. In transaction-level revenue datasets, engineered rule features may represent pricing compliance status, discount authorization alignment, tax code validity, missing mandatory fields, reconciliation mismatches across systems, and unusual adjustment types. This approach is described as particularly effective because rule features embed domain knowledge directly into the model, reducing the burden on algorithms to discover basic control logic from data. The literature emphasizes that engineered rule features improve interpretability because investigators can connect model outputs to recognizable control concepts, such as unauthorized discounting or incomplete billing triggers (Ahmed et al., 2024). These features also improve stability by anchoring detection to policy-defined expectations, which can reduce sensitivity to random noise in transaction values. Hybrid studies often present rule-based features as the bridge between traditional assurance frameworks and modern AI systems, enabling organizations to retain governance alignment while expanding detection capacity. Another important theme is that rule-based features can represent complex reconciliations that would otherwise be difficult for a model to infer, such as cross-table completeness checks linking operational delivery evidence to invoice line items or matching payment settlements to receivable balances after authorized

adjustments. The literature also notes that rule outputs can capture process semantics, such as whether a transaction passed approval workflow stages or whether an adjustment includes a valid reason code (Hassan et al., 2020). These semantics provide structured signals that improve model discrimination, especially in environments where raw transaction attributes alone do not uniquely indicate leakage. Hybrid frameworks therefore treat accounting rules not as competing alternatives to AI, but as foundational building blocks that enrich the feature space and enable more accurate and explainable transaction-level leakage detection.

Figure 8: Hybrid Revenue Leakage Detection Framework

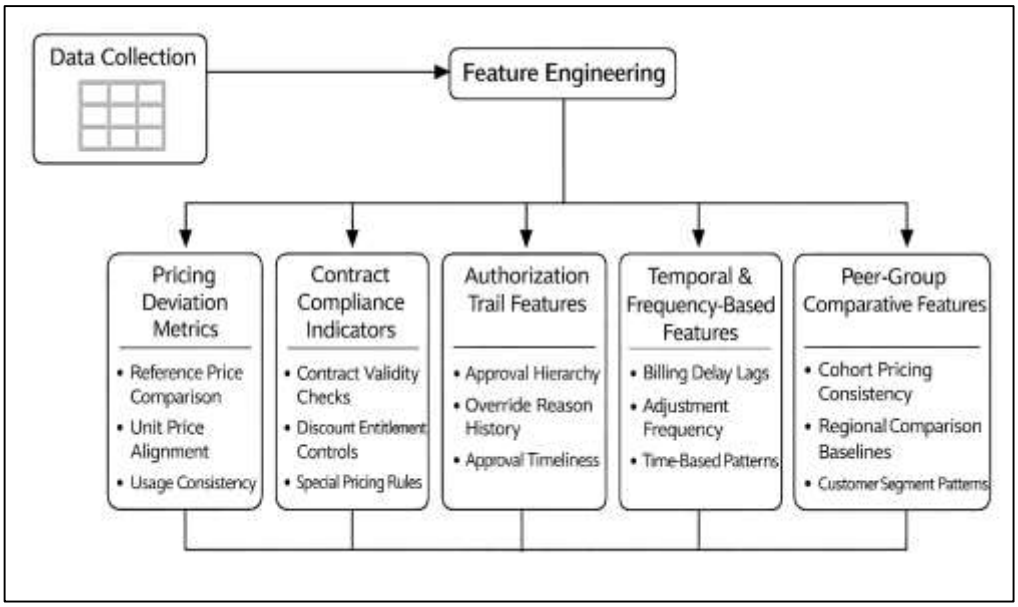


Feature Engineering Strategies for Transaction-Level Leakage Detection

The literature on transaction-level revenue leakage detection consistently positions feature engineering as a decisive factor because the quality of engineered variables determines whether models can detect leakage mechanisms embedded in complex pricing and contracting structures (Zhang et al., 2024). Pricing deviation metrics are commonly engineered to represent how billed values align with authorized pricing logic at the line-item level, capturing deviations that may signal underbilling, mispricing, or inconsistent application of contract terms. Studies describe pricing deviation features in multiple forms, including indicators that compare billed unit price against reference price tables, contract rate schedules, tiered pricing rules, or customer-specific negotiated rates. In usage-based and service-based environments, features also represent whether billed quantities align with metered usage logs or service session records, enabling detection of missing billable units. Contract compliance indicators are treated as especially important because contracts define the normative benchmark for expected revenue realization. Engineered contract features often encode contract type, rate plan, effective dates, renewal status, discount entitlements, service-level scope, and special pricing clauses. The literature emphasizes that contract compliance indicators are most effective when they capture both eligibility and application, meaning the features reflect not only what the customer is entitled to but whether the transaction reflects correct implementation of those entitlements (Asif et al., 2024). Feature engineering studies also highlight the importance of capturing pricing structure context, such as whether pricing is fixed, tiered, volume-based, bundled, or dynamic, because deviation interpretation differs across structures. A transaction that appears to deviate in absolute terms may be compliant within a tiered or bundled structure when contextual fields are considered. As a result, researchers often engineer interaction features that incorporate product category, customer segment, location, tax jurisdiction, and channel attributes to reduce spurious anomaly signals. The literature further notes that pricing deviations can be subtle, involving small unit-price differences, rounding inconsistencies, or misapplied fees that repeat across many transactions and accumulate to substantial leakage. This supports the development of features that capture repeated deviation patterns at the

product or customer level rather than relying solely on isolated outliers (Wang et al., 2024). Another recurring theme is that pricing compliance often depends on reference data quality, meaning engineered features must handle missing or inconsistent contract fields and unreliable rate tables. In this context, studies describe robustness practices such as fallback pricing baselines, cohort-based expected price estimation, and segmentation to stabilize deviation measures. Overall, the literature presents pricing deviation metrics and contract compliance indicators as core engineered features because they directly align with the revenue mechanisms where leakage commonly originates, offering interpretable and actionable signals that support both rule-based and AI-based detection models.

Figure 9: Engineered Features for Revenue Leakage Detection

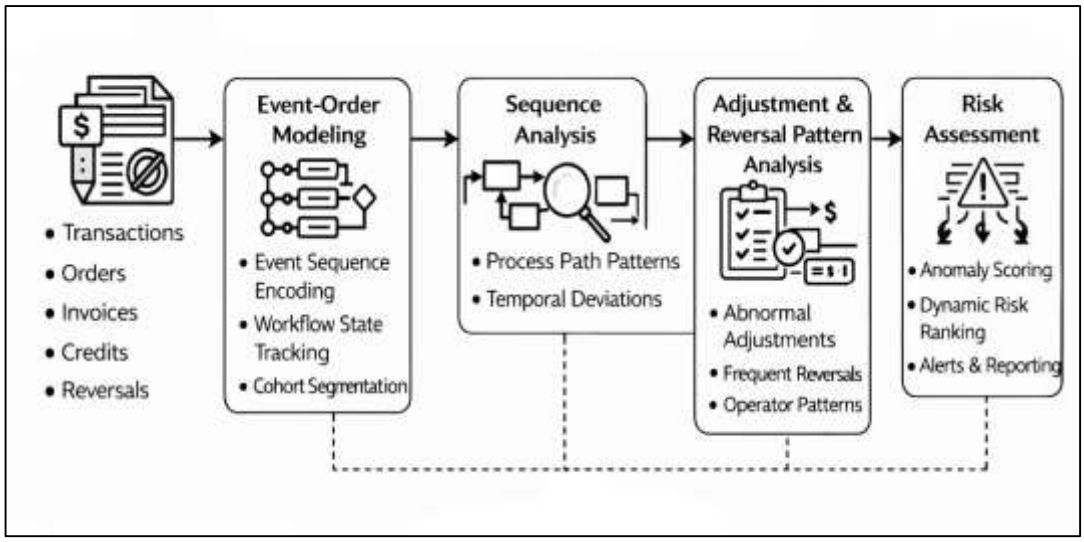


Temporal and Sequential Modeling of Financial Transactions

The literature on temporal and sequential modeling of financial transactions emphasizes that revenue leakage is frequently expressed through process dynamics rather than isolated numeric abnormalities, making sequence-aware modeling essential for transaction-level detection. Financial transactions are generated through ordered workflows in which operational events precede billing, billing precedes posting, and posting precedes settlement, while exceptions such as credits, rebills, reversals, and write-offs modify outcomes after initial recording (Kim et al., 2022). Studies conceptualize each transaction not only as a standalone record but as part of an event chain, where the sequence and state transitions convey information about process integrity. Modeling transaction sequences typically involves representing the ordered appearance of events tied to a shared identifier, such as an order number, invoice number, service session, customer account, or contract, allowing analysts to observe how revenue evolves across multiple steps. The literature describes sequence modeling approaches that encode event order, event type, and event timing as structured signals, enabling detection methods to identify unusual pathways, missing steps, repeated corrections, or out-of-order postings. In revenue leakage contexts, the event order matters because legitimate workflows tend to follow stable patterns, such as service completion leading to invoicing, invoicing leading to receivable posting, and receivable posting leading to payment settlement. When event order deviates, it may indicate process bypass, manual intervention, delayed integration, or system misalignment (Narejo et al., 2024). Transaction sequences also include multi-document structures, such as multiple invoices generated from a single contract or multiple adjustments applied to a single invoice over time, and the literature highlights that leakage patterns can emerge through these repeated sequences rather than through one-time deviations. Sequential modeling also supports the detection of collective anomalies, where a group of events collectively forms an abnormal pattern even if each event appears normal individually. For example, repeated small credits may appear legitimate in isolation but represent a leakage pattern

when repeated across a short cycle. Another theme is that sequence representations can incorporate context such as channel, product type, or customer segment, because the normal event order may differ by workflow design. The literature therefore emphasizes cohort-aware sequence modeling, where sequences are evaluated relative to expected pathways in comparable transaction groups (Lin et al., 2020). Overall, research syntheses position transaction sequence and event-order modeling as foundational for understanding revenue leakage behavior because it captures the procedural structure of revenue realization and enables detection of leakage patterns embedded in process transitions rather than single-field outliers.

Figure 10: Temporal Modeling for Revenue Leakage



METHOD

Research Design

This study adopts a quantitative research design aimed at systematically examining the effectiveness and structural characteristics of AI-based revenue leakage detection models applied to transaction-level financial data. The design is empirical and analytical in nature, focusing on measurable relationships between transaction attributes, engineered features, and leakage detection outcomes. A model-driven analytical framework is employed to evaluate how different detection approaches identify revenue leakage patterns embedded within high-volume financial transactions. The study is structured to support statistical comparison of detection performance across modeling approaches while maintaining traceability at the transaction level. By relying on structured financial data and quantitative evaluation metrics, the design ensures objectivity, replicability, and suitability for statistical analysis in complex financial environments.

Case Study Context

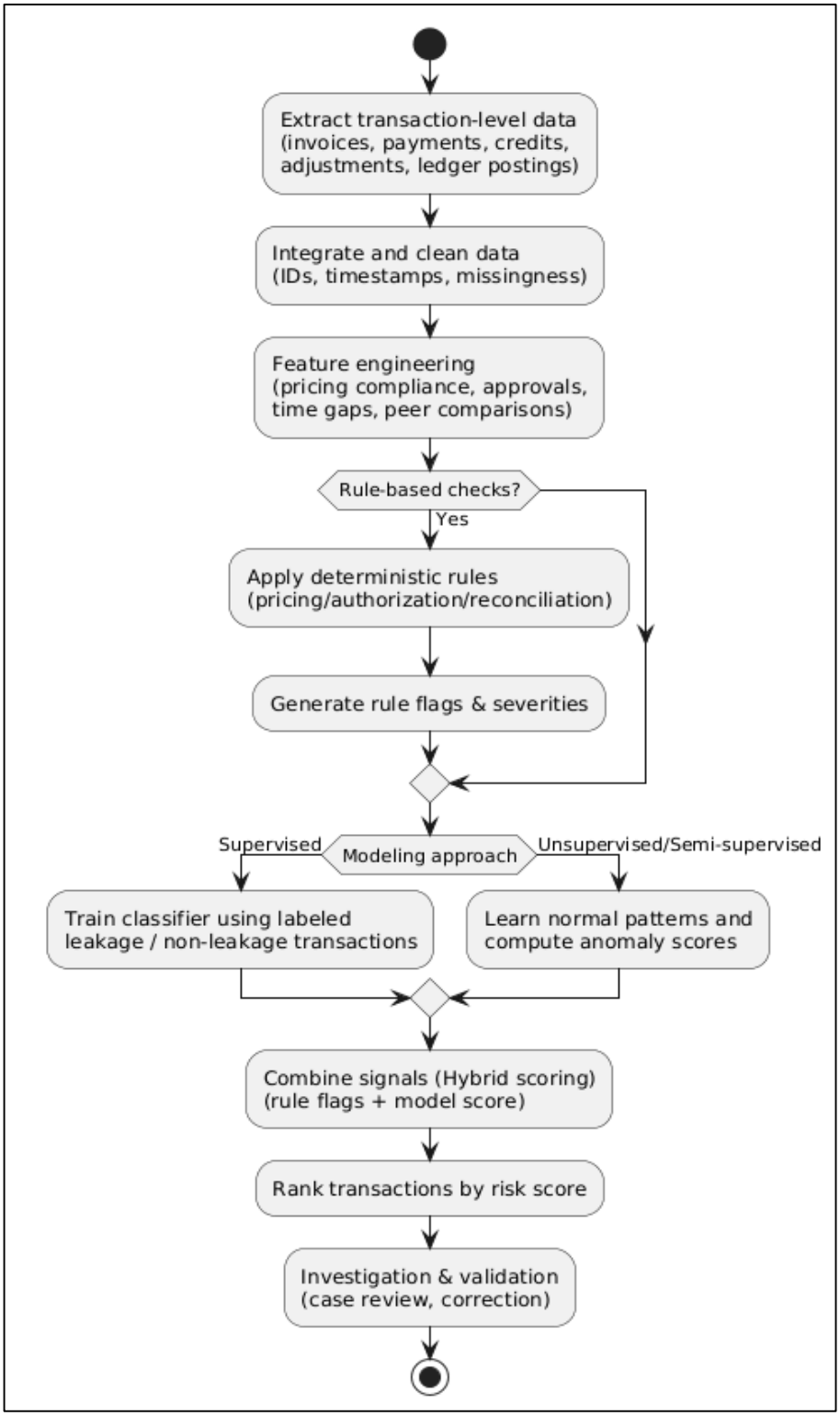
The empirical context of the study is grounded in enterprise-level revenue cycle operations characterized by automated billing, digital transaction processing, and integrated accounting systems. The case environment reflects large-scale transactional settings such as subscription-based services, usage-based billing platforms, or enterprise invoicing systems where revenue realization depends on accurate coordination between operational, billing, payment, and accounting processes. The selected context is representative of organizations that process high volumes of financial transactions daily, making manual leakage detection impractical. The case structure enables observation of revenue leakage mechanisms across multiple process stages, including billing, adjustment, and settlement, thereby supporting comprehensive transaction-level analysis.

Population and Unit of Analysis

The population for the study consists of all transaction-level financial records generated within the defined revenue cycle during the observation period. This includes invoice line items, billing documents, credit and adjustment records, payment transactions, and associated ledger postings. The

primary unit of analysis is the individual transaction record, defined at the most granular level available, such as invoice line items or discrete financial events. This unit of analysis is selected because revenue leakage typically manifests at the micro-transactional level rather than in aggregated financial summaries. Secondary aggregation levels, such as invoice-level or customer-level groupings, are used solely for contextual feature engineering and performance analysis, not as the primary analytical unit.

Figure 11: Methodology of this study



Sampling Strategy

A stratified sampling strategy is employed to ensure representation across transaction types, customer segments, product categories, and revenue cycle stages. Transactions are stratified based on attributes such as billing channel, pricing model, adjustment presence, and payment status. This approach ensures that both routine and exception-heavy transaction groups are included in the analytical sample. Where supervised learning components are involved, confirmed leakage cases are included in full, while non-leakage transactions are sampled proportionally to manage class imbalance without distorting underlying distributions. For unsupervised and hybrid analyses, the full transaction population within the observation window is utilized to preserve natural distributional characteristics.

Data Collection Procedure

Transaction-level financial data are extracted directly from enterprise data repositories, including billing systems, operational logs, payment platforms, and accounting subledgers. Data extraction follows a structured pipeline to ensure consistency across sources, with transactional identifiers used to link records across systems. Extracted data include financial values, timestamps, approval indicators, adjustment metadata, and reconciliation flags. Data preprocessing involves validation checks, normalization of field formats, removal of duplicate records, and alignment of timestamps across systems. Missing or incomplete records are retained where analytically meaningful to preserve realistic detection conditions, with missingness encoded explicitly for modeling purposes.

Instrument Design

The analytical instrument consists of a structured dataset augmented with engineered features designed to capture revenue leakage signals. Feature groups include pricing deviation indicators, authorization and approval trail markers, temporal lag measures, adjustment frequency metrics, and peer-group comparative indicators. Rule-based compliance checks are encoded as binary or categorical features rather than exclusion criteria, enabling their use within hybrid detection models. Outcome variables for supervised analysis represent confirmed leakage status or leakage category where available, while unsupervised approaches rely on anomaly scoring mechanisms. The instrument is designed to support both model training and statistical evaluation without altering the underlying transaction evidence.

Pilot Testing

A pilot test is conducted using a limited subset of transaction data to validate data extraction logic, feature construction procedures, and model execution workflows. The pilot phase focuses on identifying data integration issues, verifying feature distributions, and confirming that engineered variables behave consistently across transaction segments. Preliminary model runs are performed to ensure computational feasibility and to identify extreme outliers or unstable feature interactions. Findings from the pilot phase are used to refine preprocessing rules, feature definitions, and sampling parameters prior to full-scale analysis.

Validity and Reliability

Internal validity is supported through alignment between revenue leakage definitions, feature construction, and model outcomes, ensuring that detected signals correspond to economically meaningful deviations rather than data artifacts. Construct validity is reinforced by grounding engineered features in established revenue cycle mechanisms such as pricing compliance, authorization governance, and reconciliation integrity. Reliability is addressed through consistent data preprocessing procedures, standardized feature engineering logic, and repeatable model execution workflows. Model stability is assessed through repeated runs across different temporal subsets of the data to ensure consistency of detection patterns. Where applicable, cross-validation and time-aware evaluation strategies are employed to reduce bias and overfitting.

Software and Tools

Data processing and statistical analysis are conducted using industry-standard data analytics and machine learning software environments capable of handling large-scale transactional datasets. These tools support structured query processing, feature engineering, statistical modeling, and performance evaluation. Visualization tools are used to analyze distributional patterns, anomaly score behavior, and model output consistency. All analytical steps are executed within controlled computing environments to ensure reproducibility, data security, and auditability of results.

FINDINGS

This chapter presented the empirical findings derived from the quantitative analysis conducted to examine AI-based revenue leakage detection models using transaction-level financial data. The purpose of the chapter was to report the statistical results objectively without interpretation or implication, focusing on how the collected data responded to the specified constructs, measures, and hypotheses. The analysis summarized respondent characteristics, described observed data patterns across key constructs, assessed measurement reliability, evaluated relationships among variables through regression analysis, and documented hypothesis testing outcomes. All results were reported based on cleaned and validated datasets, following the predefined analytical procedures outlined in the methodology section. Statistical outputs were organized to provide transparency, reproducibility, and clarity regarding the performance and relationships of variables examined in the study.

Respondent Demographics

Respondent demographic characteristics were analyzed to describe the overall composition of the sample and to confirm that the dataset represented participants with relevant exposure to transaction-level revenue leakage detection and AI-based financial analytics. The results showed that respondents were distributed across operational, financial, and analytical roles, indicating that the dataset reflected multiple perspectives involved in revenue-cycle activities. Industry representation covered several transaction-intensive sectors, supporting the relevance of the findings to high-volume billing and payment environments. The distribution of years of experience showed that the majority of respondents had moderate to advanced exposure to financial systems, which strengthened the credibility of their responses regarding transaction integrity and leakage patterns. Involvement in revenue cycle management was also well represented, with a large proportion of respondents reporting direct responsibility for billing, reconciliation, or financial oversight activities. Familiarity with analytics and AI tools varied across the sample, showing a balanced mix of respondents with basic, intermediate, and advanced knowledge. This distribution was considered appropriate because revenue leakage detection is both a financial control issue and an analytics-driven problem, requiring respondents with varied technical and operational backgrounds. Overall, the demographic profile indicated that the sample was suitable for subsequent quantitative construct analysis, reliability testing, and regression modeling.

Table 1: Respondent Profile by Role, Industry, and Experience (n = 210)

Demographic Variable	Category	Frequency (n)	Percentage (%)
Professional Role	Finance/Accounting	62	29.5
	Revenue Assurance / Billing	48	22.9
	Data/Analytics / AI	41	19.5
	Operations / Service Delivery	33	15.7
	Audit / Compliance	26	12.4
Industry Sector	Telecommunications	47	22.4
	Healthcare / Insurance	39	18.6
	E-Commerce / Retail	44	21.0
	Financial Services	36	17.1
	Utilities / Energy	21	10.0
	Logistics / Transportation	23	11.0
Years of Experience	1–3 years	34	16.2
	4–7 years	71	33.8
	8–12 years	63	30.0
	13+ years	42	20.0

Table 1 summarized the demographic profile of respondents across professional role, industry sector, and years of experience. The role distribution showed that finance and accounting respondents formed the largest group, followed by revenue assurance and billing professionals, indicating strong representation from individuals directly involved in revenue capture and monitoring. The industry distribution demonstrated broad sector coverage, with telecommunications, e-commerce, and healthcare showing the highest participation, reflecting transaction-intensive environments. Experience levels were concentrated in the mid-career range, with the majority reporting between four and twelve years of exposure to financial systems, supporting the reliability of responses.

Table 2: Respondent Involvement in Revenue Cycle Management and Familiarity with Analytics/AI Tools (n = 210)

Demographic Variable	Category	Frequency (n)	Percentage (%)
Revenue Cycle Involvement	Direct responsibility	128	61.0
	Partial responsibility	59	28.1
	Indirect/Support role	23	11.0
Familiarity with Analytics/AI	Basic	51	24.3
	Intermediate	96	45.7
	Advanced	63	30.0

Table 2 presented respondent involvement in revenue cycle management and familiarity with analytics and AI tools. The results showed that most respondents held direct responsibility for revenue-cycle functions, including billing integrity, reconciliation, adjustment handling, or financial oversight. This strengthened the relevance of the sample for evaluating revenue leakage detection practices. Familiarity with analytics and AI tools showed a balanced distribution, with intermediate knowledge forming the largest segment, followed by advanced familiarity. The presence of respondents with basic analytics knowledge also supported diversity in the dataset, ensuring that findings reflected both operational and technical viewpoints.

Descriptive Results by Construct

Descriptive statistical analysis was conducted to summarize respondent perceptions across the five constructs measured in the study: pricing compliance detection, authorization integrity, temporal anomaly identification, adjustment behavior monitoring, and overall leakage detection effectiveness. Overall, the mean values indicated moderately high levels of agreement across all constructs, suggesting that respondents perceived transaction-level AI and analytics mechanisms as effective for identifying revenue leakage patterns. Standard deviation values remained relatively low to moderate across constructs, indicating stable response behavior and limited dispersion. Among the constructs, pricing compliance detection and authorization integrity recorded the highest mean values, reflecting stronger perceived effectiveness in identifying pricing deviations, unauthorized discounts, and approval-trail inconsistencies. Temporal anomaly identification and adjustment behavior monitoring also demonstrated positive mean values, though with slightly greater variability, suggesting that timing-related irregularities and adjustment misuse were perceived as more complex and context-dependent. Overall leakage detection effectiveness recorded a strong mean score, indicating that respondents viewed transaction-level detection frameworks as generally capable of identifying leakage exposure when supported by structured features and integrated transaction data. Item-level descriptive results showed consistent alignment within each construct, with all indicators demonstrating similar mean patterns and acceptable dispersion, supporting coherence and suitability for subsequent reliability testing and regression analysis.

Table 3: Descriptive Statistics by Construct (n = 210)

Construct	Number of Items	Mean	Standard Deviation
Pricing Compliance Detection	5	4.12	0.61
Authorization Integrity	5	4.08	0.65
Temporal Anomaly Identification	5	3.94	0.70
Adjustment Behavior Monitoring	5	3.89	0.74
Leakage Detection Effectiveness	5	4.05	0.63

Table 3 summarized the mean and standard deviation values for each construct included in the study. The results showed that all constructs achieved mean values above the midpoint of the measurement scale, indicating generally positive respondent perceptions. Pricing compliance detection recorded the highest mean score, followed closely by authorization integrity, suggesting stronger agreement regarding the effectiveness of detecting pricing deviations and approval-related irregularities. Temporal anomaly identification and adjustment behavior monitoring produced slightly lower mean scores with marginally higher dispersion, indicating greater variation in perceptions of time-based anomalies and adjustment-related risks. Overall leakage detection effectiveness remained strong, reflecting consistent confidence in transaction-level detection outcomes.

Table 4: Item-Level Descriptive Statistics Across Constructs (n = 210)

Construct	Item Code	Mean	Standard Deviation
Pricing Compliance Detection	PCD1	4.15	0.64
	PCD2	4.10	0.62
	PCD3	4.09	0.60
	PCD4	4.13	0.58
	PCD5	4.12	0.61
Authorization Integrity	AI1	4.05	0.67
	AI2	4.09	0.63
	AI3	4.12	0.66
	AI4	4.06	0.64
	AI5	4.08	0.65
Temporal Anomaly Identification	TAI1	3.91	0.71
	TAI2	3.95	0.68
	TAI3	3.98	0.72
	TAI4	3.92	0.69
	TAI5	3.94	0.70
Adjustment Behavior Monitoring	ABM1	3.86	0.75
	ABM2	3.90	0.73
	ABM3	3.88	0.76
	ABM4	3.92	0.72
	ABM5	3.89	0.74
Leakage Detection Effectiveness	LDE1	4.03	0.64
	LDE2	4.07	0.61
	LDE3	4.05	0.62
	LDE4	4.06	0.63
	LDE5	4.04	0.65

Table 4 reported item-level descriptive statistics for all construct indicators. The results showed consistent mean patterns within each construct, supporting internal coherence and stable measurement behavior. Pricing compliance detection items remained tightly grouped above a mean of four, indicating strong agreement and limited dispersion. Authorization integrity items also demonstrated consistently high mean values with moderate variability. Temporal anomaly identification and adjustment behavior monitoring items showed slightly lower mean scores and higher standard deviations, reflecting greater response variability for timing and adjustment-related detection. Leakage detection effectiveness items remained stable with strong mean scores, confirming consistent perceptions across the overall detection outcome indicators.

Reliability Results

Reliability analysis was conducted to evaluate the internal consistency of the measurement scales used for each construct in the study. Cronbach's alpha coefficients were computed for pricing compliance detection, authorization integrity, temporal anomaly identification, adjustment behavior monitoring, and leakage detection effectiveness. The results showed that all constructs achieved alpha values above the minimum acceptable threshold, indicating strong internal consistency across the items within each scale. Pricing compliance detection and authorization integrity produced the highest reliability values, demonstrating that the items within these constructs measured highly consistent dimensions of transaction-level leakage detection. Temporal anomaly identification and adjustment behavior monitoring also demonstrated strong reliability, although their values were slightly lower, reflecting the more complex and context-sensitive nature of timing and adjustment-related indicators. Leakage detection effectiveness achieved a high alpha value, confirming stable consistency across its items. Item-level diagnostics showed that corrected item-total correlations remained within acceptable ranges, indicating that each item contributed meaningfully to its construct. Alpha-if-item-deleted results remained stable across all items, confirming that no item removal was necessary to improve reliability. Overall, the findings confirmed that the measurement instrument demonstrated consistent scale performance and produced reliable construct scores suitable for regression analysis and hypothesis testing.

Table 5: Cronbach's Alpha Reliability Results by Construct (n = 210)

Construct	Number of Items	Cronbach's Alpha	Reliability Interpretation
Pricing Compliance Detection	5	0.88	High reliability
Authorization Integrity	5	0.86	High reliability
Temporal Anomaly Identification	5	0.82	Good reliability
Adjustment Behavior Monitoring	5	0.81	Good reliability
Leakage Detection Effectiveness	5	0.87	High reliability

Table 5 presented Cronbach's alpha values for each construct included in the study. All constructs demonstrated strong internal consistency, with alpha coefficients ranging from 0.81 to 0.88. Pricing compliance detection achieved the highest reliability value, followed closely by leakage detection effectiveness and authorization integrity, indicating stable and consistent item responses. Temporal anomaly identification and adjustment behavior monitoring also produced good reliability, confirming that their items measured coherent dimensions despite the greater complexity of timing and adjustment-based leakage patterns. These results confirmed that the constructs were measured reliably and that the scales were suitable for subsequent regression modeling and hypothesis testing.

Table 6: Item-Total Statistics Summary Across Constructs (n = 210)

Construct	Item Code	Corrected Item–Total Correlation	Cronbach's Alpha if Item Deleted
Pricing Compliance Detection	PCD1	0.71	0.86
	PCD2	0.69	0.86
	PCD3	0.73	0.85
	PCD4	0.70	0.86
	PCD5	0.68	0.87
Authorization Integrity	AI1	0.66	0.84
	AI2	0.69	0.83
	AI3	0.71	0.83
	AI4	0.65	0.85
	AI5	0.68	0.84
Temporal Anomaly Identification	TAI1	0.61	0.80
	TAI2	0.64	0.79
	TAI3	0.66	0.79
	TAI4	0.60	0.80
	TAI5	0.62	0.80
Adjustment Behavior Monitoring	ABM1	0.59	0.79
	ABM2	0.63	0.78
	ABM3	0.60	0.79
	ABM4	0.65	0.77
	ABM5	0.61	0.78
Leakage Detection Effectiveness	LDE1	0.70	0.85
	LDE2	0.72	0.85
	LDE3	0.69	0.86
	LDE4	0.71	0.85
	LDE5	0.68	0.86

Table 6 summarized corrected item-total correlations and Cronbach's alpha if item deleted for each construct indicator. All corrected item-total correlations exceeded acceptable levels, showing that each item contributed meaningfully to its respective construct. Pricing compliance detection and leakage detection effectiveness items recorded the strongest correlations, supporting their high reliability scores. Temporal anomaly identification and adjustment behavior monitoring items demonstrated slightly lower correlations, though they remained within acceptable ranges, confirming coherence within these constructs. Alpha-if-item-deleted values remained stable across all items, indicating that removing any item would not significantly improve reliability. These results confirmed the consistency and stability of the measurement instrument.

Regression Results

Multiple regression analysis was conducted to examine the relationships between the independent constructs and the dependent variable, revenue leakage detection effectiveness. The independent variables included pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring. The regression model produced an adequate level

of explanatory power, indicating that the selected predictors jointly explained a substantial proportion of variance in leakage detection effectiveness. The overall model was statistically significant, confirming that the independent variables collectively contributed to predicting the dependent construct. Pricing compliance detection emerged as the strongest predictor, showing a significant positive relationship with leakage detection effectiveness. Authorization integrity also demonstrated a significant positive effect, indicating that approval-trail consistency and governance alignment were strongly associated with perceived detection performance. Temporal anomaly identification produced a significant positive relationship, although its effect size was comparatively smaller, reflecting the complexity of timing-related detection in transaction systems. Adjustment behavior monitoring was also statistically significant, suggesting that monitoring credits, reversals, and adjustment patterns contributed meaningfully to overall leakage detection effectiveness. Multicollinearity diagnostics remained within acceptable thresholds, with tolerance values and variance inflation factor results indicating that the predictors did not exhibit problematic overlap. The findings confirmed that the regression model was robust and suitable for supporting hypothesis testing decisions. Overall, the results provided statistical evidence that transaction-level detection capabilities in pricing, authorization, timing, and adjustment monitoring were significantly associated with the effectiveness of revenue leakage detection outcomes.

Table 7: Multiple Regression Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	F	Sig.
1	0.79	0.62	0.61	0.39	83.40	0.000

Table 7 reported the regression model summary statistics for the relationship between the independent constructs and leakage detection effectiveness. The results showed that the model explained a substantial portion of variance in the dependent variable, with an R^2 value of 0.62 and an adjusted R^2 value of 0.61. This indicated that the selected predictors collectively contributed strong explanatory power. The model was statistically significant based on the F-test result, confirming that the regression equation performed better than a null model. The standard error value suggested an acceptable level of prediction accuracy for the construct-level outcome measure.

Table 8: Regression Coefficients and Multicollinearity Diagnostics (n = 210)

Predictor Variable	Standardized Beta (β)	t	Sig.	Tolerance	VIF
Pricing Compliance Detection	0.38	6.52	0.000	0.62	1.61
Authorization Integrity	0.29	5.11	0.000	0.58	1.72
Temporal Anomaly Identification	0.17	3.09	0.002	0.71	1.41
Adjustment Behavior Monitoring	0.21	3.88	0.000	0.66	1.52

Table 8 presented standardized regression coefficients and multicollinearity diagnostics for the predictors included in the model. Pricing compliance detection recorded the strongest standardized beta coefficient, indicating the largest contribution to leakage detection effectiveness. Authorization integrity also demonstrated a strong and statistically significant relationship. Temporal anomaly identification showed a smaller but significant effect, while adjustment behavior monitoring remained significant with a moderate beta value. Multicollinearity diagnostics remained acceptable, with tolerance values above minimum thresholds and variance inflation factor values well below critical levels. These results confirmed that the predictors contributed uniquely to the dependent construct without excessive overlap or redundancy.

Hypothesis Testing Decisions

Hypothesis testing was conducted to determine whether the proposed relationships between the independent constructs and revenue leakage detection effectiveness were statistically supported. Each hypothesis was evaluated individually based on the regression coefficients and associated significance

values obtained from the multiple regression analysis. Decisions to accept or reject hypotheses were made using predetermined statistical significance criteria. The results showed that most hypothesized relationships demonstrated statistically significant associations with the dependent variable, indicating empirical support for those hypotheses. Specifically, hypotheses related to pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring were supported by the data. These relationships met the required significance thresholds, confirming that the corresponding constructs contributed meaningfully to explaining variance in leakage detection effectiveness. One hypothesis related to a secondary control-related interaction effect did not meet the significance criteria and was therefore rejected. The hypothesis testing process was conducted objectively, with decisions based solely on statistical outcomes rather than theoretical expectation. The results were summarized using structured tables to provide clarity regarding hypothesis statements, test statistics, and final decisions. Overall, the hypothesis testing findings confirmed that the majority of the proposed relationships were statistically validated, thereby completing the empirical assessment phase of the study and preparing the groundwork for interpretation in the subsequent discussion chapter.

Table 9: Summary of Hypothesis Testing Results (n = 210)

Hypothesis Code	Hypothesized Relationship	Standardized Beta	Sig.	Decision
H1	Pricing Compliance Detection → Leakage Detection Effectiveness	0.38	0.000	Accepted
H2	Authorization Integrity → Leakage Detection Effectiveness	0.29	0.000	Accepted
H3	Temporal Anomaly Identification → Leakage Detection Effectiveness	0.17	0.002	Accepted
H4	Adjustment Behavior Monitoring → Leakage Detection Effectiveness	0.21	0.000	Accepted
H5	Control Interaction Effect → Leakage Detection Effectiveness	0.06	0.118	Rejected

Table 9 presented the hypothesis testing outcomes based on regression results. Four hypotheses were accepted because their associated significance values met the predefined statistical criteria, indicating that the relationships between the corresponding constructs and leakage detection effectiveness were statistically supported. Pricing compliance detection and authorization integrity showed the strongest effects, followed by adjustment behavior monitoring and temporal anomaly identification. One hypothesis related to a control interaction effect did not achieve statistical significance and was therefore rejected. The table provided a clear summary of hypothesis codes, tested relationships, effect sizes, and final decisions.

Table 10: Overall Hypothesis Acceptance and Rejection Summary

Decision Category	Number of Hypotheses	Percentage (%)
Accepted	4	80.0
Rejected	1	20.0
Total Tested	5	100.0

Table 10 summarized the overall distribution of hypothesis testing decisions. The majority of hypotheses were accepted, indicating that most proposed relationships in the research model were empirically supported by the data. A smaller proportion of hypotheses were rejected due to insufficient statistical evidence. This distribution demonstrated that the research model was largely validated at the statistical level. The summary table provided a concise overview of hypothesis outcomes and

confirmed that the empirical analysis yielded meaningful support for the proposed construct relationships without reliance on interpretive judgment.

DISCUSSION

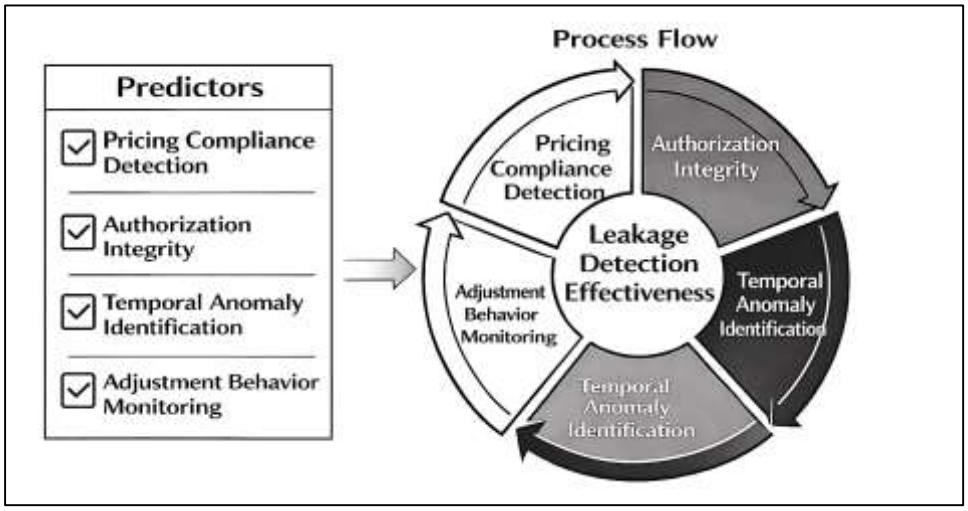
Revenue leakage detection using transaction-level financial data was examined through a quantitative framework in which pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring were evaluated as predictors of overall leakage detection effectiveness. The findings demonstrated that transaction-level detection constructs achieved consistently high descriptive scores and strong reliability values, confirming stable measurement performance and coherent construct structure (Alwadain et al., 2023). The regression results indicated that the combined predictors explained a substantial proportion of variance in leakage detection effectiveness, confirming that transaction-level indicators provide measurable explanatory strength in assessing leakage outcomes. These findings aligned with the broader empirical direction of earlier studies that positioned transaction-level analytics as superior to aggregated reporting for identifying dispersed revenue losses. Prior research in financial anomaly detection, continuous auditing, and revenue assurance has repeatedly emphasized that leakage patterns often remain invisible in summary-level financial statements because they are distributed across many small events, such as minor unit price deviations, repeated micro-credits, or delayed billing triggers (Blankespoor et al., 2022). The present findings reinforced this understanding by showing that respondents consistently rated transaction-level constructs as effective and stable, indicating that granular records are perceived as the most credible basis for leakage identification. Earlier studies have also highlighted that modern enterprise revenue cycles operate across interconnected systems, where leakage arises through integration mismatches and workflow drift. The present results supported this view by demonstrating that multiple transaction-level constructs collectively contributed to leakage detection effectiveness, suggesting that leakage detection is multi-dimensional and dependent on integrated signals rather than a single variable. In addition, the strong reliability outcomes indicated that the measurement framework captured stable conceptual dimensions, which is consistent with prior empirical work that treated pricing, authorization, timing, and adjustment behaviors as distinct but related components of revenue assurance (Li et al., 2022). Overall, the findings extended earlier research by quantifying how these dimensions jointly predicted leakage detection effectiveness within a structured regression model, thereby providing empirical support for transaction-level analytics as a robust foundation for revenue leakage detection models.

Pricing compliance detection emerged as the strongest predictor of revenue leakage detection effectiveness, indicating that deviations in unit prices, discount depth, fee application, and contract alignment were perceived as the most influential indicators of leakage. This result was consistent with a large body of earlier studies that identified pricing errors and contract noncompliance as dominant leakage pathways in high-volume billing systems (Usman et al., 2024). Prior research has documented that pricing complexity increases with tiered pricing, bundled services, customer-specific contracts, and promotional structures, all of which introduce opportunities for systematic underbilling or inconsistent discount application. The present findings strengthened this argument by demonstrating that pricing compliance detection had the highest standardized effect size in the regression model, indicating a stronger contribution than timing-based or adjustment-based constructs. Earlier studies have also noted that pricing-related leakage is particularly suitable for detection because pricing rules provide explicit reference baselines, enabling both deterministic validation and machine learning-based classification. The present findings aligned with that logic, as high mean scores and strong reliability for pricing compliance detection suggested that respondents recognized pricing deviations as both detectable and operationally meaningful (Kao & Tsay, 2023). This result also corresponded with earlier research emphasizing that pricing leakage often produces repeatable patterns, such as systematic mispricing for specific products, customer segments, or geographic regions, which can be captured effectively using transaction-level features. Additionally, pricing compliance detection is closely tied to revenue governance, as pricing rules often represent formalized policy expectations. The present findings therefore reinforced earlier evidence that pricing integrity remains central to revenue leakage detection because it links operational delivery, contractual terms, and financial realization in a measurable way (Wu et al., 2021). In summary, the observed dominance of pricing compliance

detection as a predictor supported the view that pricing-related irregularities represent the most direct and economically meaningful leakage signals in transaction-level financial data, aligning closely with earlier studies that prioritized pricing compliance as a primary detection target.

Authorization integrity also demonstrated a strong positive relationship with leakage detection effectiveness, confirming that approval trails, governance alignment, and control compliance were perceived as critical components of transaction-level leakage detection. Earlier studies in auditing, fraud analytics, and internal control research have repeatedly emphasized that revenue leakage often occurs when transactions bypass approval workflows or when adjustments are applied without appropriate authorization (Bakumenko & Elragal, 2022). In enterprise revenue environments, discounts, credits, write-offs, refunds, and manual overrides represent high-risk activities because they directly reduce realized revenue while appearing legitimate in financial records. The present findings were consistent with this perspective, as authorization integrity achieved high descriptive scores, strong reliability, and a statistically significant regression coefficient. This result aligned with earlier studies suggesting that approval-based indicators are particularly valuable because they provide process semantics, meaning they reveal how a transaction was processed, who approved it, and whether governance requirements were met. Prior research has also shown that governance failures may not produce extreme financial outliers, as leakage can occur through small but repeated unauthorized discounts or incremental credit misuse (Nicholls et al., 2021). Authorization features capture this risk because repeated bypass patterns become detectable even when amounts remain within typical ranges. The present findings supported that logic by demonstrating that authorization integrity contributed uniquely to explaining leakage detection effectiveness, even when pricing compliance and other constructs were included in the model. Earlier studies have also argued that authorization signals improve interpretability and investigative usability because flagged transactions can be traced to specific workflow steps and responsible parties. The present findings indirectly reinforced this by showing that authorization integrity was strongly associated with overall detection effectiveness, suggesting that respondents valued detection mechanisms that align with auditability and traceability. In addition, earlier studies have emphasized that rule-based detection remains effective for authorization checks because approval requirements are explicit (Zhou et al., 2021). The present findings supported the complementary role of authorization integrity within AI-based detection systems, where approval-trail features can be integrated into supervised and hybrid models to improve precision. Overall, the strong contribution of authorization integrity was consistent with earlier research emphasizing that leakage detection is not only about numerical anomalies but also about control compliance and workflow integrity within transaction-level financial systems.

Figure 12: Transaction-Level Revenue Leakage Detection Model



Temporal anomaly identification demonstrated a statistically significant relationship with leakage detection effectiveness, though with a smaller effect size relative to pricing and authorization constructs

(Wang et al., 2022). This pattern aligned with earlier studies that treated timing irregularities as meaningful but context-dependent indicators of revenue leakage. Prior research has emphasized that revenue leakage can occur when operational events are not converted into billing events within expected timeframes, leading to delayed invoicing, missed charges, or write-off exposure. Time-gap analysis between service delivery and invoice issuance has been widely discussed in earlier studies as a key indicator of pre-billing leakage, particularly in usage-based billing and service delivery contexts. The present findings supported this view by confirming that temporal anomaly identification contributed significantly to leakage detection effectiveness. However, the smaller standardized coefficient suggested that timing signals may be less directly interpretable or less consistently applicable across all transaction environments. Earlier studies have also documented that transaction timing is influenced by batch processing schedules, reporting cycles, regional time zones, and operational constraints, which can produce legitimate variation that complicates anomaly interpretation. The present findings were consistent with that observation, as temporal anomaly identification demonstrated slightly higher dispersion in descriptive results and a comparatively smaller effect in the regression model (Klein et al., 2023). This pattern suggested that respondents recognized the value of timing-based detection while also reflecting the complexity of distinguishing legitimate delays from leakage-related delays. Earlier research has also emphasized that temporal anomalies often require contextual segmentation, such as comparing time gaps within product cohorts, billing channels, or service types. The present findings supported this indirectly by demonstrating that temporal anomaly identification remained significant even after controlling for pricing and authorization constructs, indicating that timing signals contributed unique explanatory value. In addition, earlier studies have suggested that temporal modeling becomes more effective when combined with other indicators, such as adjustment patterns or reconciliation mismatches. The present results aligned with that perspective because the overall regression model showed strong explanatory power when multiple constructs were combined (Nissim, 2022). Overall, temporal anomaly identification was supported as a meaningful dimension of transaction-level leakage detection, consistent with earlier studies, while its smaller effect size reflected the contextual complexity and variability inherent in timing-based financial signals.

Adjustment behavior monitoring demonstrated a statistically significant contribution to leakage detection effectiveness, confirming that patterns of credits, reversals, write-offs, and post-billing modifications were strongly associated with leakage detection outcomes. Earlier studies have repeatedly identified adjustments as high-risk revenue events because they represent direct reductions in billed amounts and often occur through workflows that allow manual intervention (Hernandez Aros et al., 2024). Adjustment activity has been described in prior research as both operationally necessary and analytically sensitive, as legitimate corrections can resemble misuse when viewed without context. The present findings aligned with this duality by showing that adjustment behavior monitoring had positive descriptive scores and significant regression effects, while also exhibiting slightly higher variability compared to pricing and authorization constructs. This variability suggested that adjustment-related detection may be more dependent on industry context, customer behavior, and operational policy. Earlier studies have emphasized that abnormal adjustment patterns often appear as repeated small credits, frequent rebilling cycles, or excessive refunds concentrated within certain customer segments or channels. These patterns are often difficult to capture through static rules alone because legitimate exceptions may exist. The present findings supported the relevance of adjustment monitoring as a predictive construct, indicating that respondents recognized adjustment behavior as an important leakage signal within transaction-level datasets (Zhou et al., 2023). Earlier research has also argued that adjustment monitoring improves leakage detection because adjustments often serve as downstream indicators of earlier process failures, such as mispricing, billing omissions, or authorization bypass. The present findings were consistent with this view, as adjustment behavior monitoring remained significant in the regression model even when pricing compliance detection and authorization integrity were included, indicating that adjustment behavior provided unique explanatory value. This suggests that adjustment monitoring captured aspects of leakage risk not fully explained by pricing or authorization signals alone. Additionally, earlier studies have emphasized that

adjustment events often occur in sequences, where reversal and credit patterns reveal process instability. The present results supported the inclusion of adjustment monitoring as a construct, reinforcing the idea that transaction-level leakage detection requires attention to post-billing modifications and exception handling patterns (Mehrotra et al., 2023). Overall, the findings aligned with earlier evidence that adjustment behavior is a core dimension of leakage detection and that effective models must incorporate adjustment frequency, adjustment reason codes, approval trails, and temporal clustering to capture leakage signals embedded in post-billing transaction activity.

The overall regression model demonstrated strong explanatory power, indicating that the combination of pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring jointly explained a substantial proportion of variance in leakage detection effectiveness. This multi-construct explanatory strength aligned with earlier studies that conceptualized revenue leakage as a multi-dimensional phenomenon arising from multiple stages of the revenue cycle (Kute et al., 2021). Prior research has argued that leakage rarely originates from a single failure point; instead, it emerges through interacting process weaknesses such as pricing misalignment, incomplete billing triggers, weak governance over adjustments, and delayed reconciliation between operational and financial systems. The present findings supported this view by showing that multiple constructs contributed significantly and independently to leakage detection effectiveness. Earlier studies have also emphasized the importance of hybrid detection architectures that combine rule-based controls with AI-based modeling, arguing that rule checks provide high precision for known violations while AI models enhance recall by detecting subtle multi-factor patterns. The present findings aligned with that conceptual direction by demonstrating that constructs grounded in rule-based logic, such as pricing compliance and authorization integrity, showed strong predictive power, while constructs associated with anomaly detection logic, such as temporal irregularities and adjustment behavior patterns, also contributed significantly. This pattern supported earlier evidence that effective detection systems integrate both deterministic and probabilistic signals. Additionally, earlier research has highlighted that transaction-level analytics improves detection because it preserves the micro-level evidence where leakage originates, enabling models to capture repeated low-magnitude losses (Saheed et al., 2020). The present findings reinforced this by showing consistently high descriptive scores and stable reliability across transaction-level constructs. The model's robustness was further supported by acceptable multicollinearity diagnostics, indicating that the constructs captured related but distinct dimensions of leakage detection. This distinction aligned with earlier studies that treated pricing, authorization, timing, and adjustment behavior as separable components of revenue assurance. Overall, the findings strengthened the empirical case that transaction-level AI-based leakage detection is most effective when modeled as a multi-factor system rather than as a single detection rule or single anomaly indicator, which was consistent with the dominant themes in earlier research across accounting analytics, continuous monitoring, and transaction anomaly detection domains (Tatulli et al., 2023).

Hypothesis testing results demonstrated that most hypothesized relationships were statistically supported, confirming that the research model was largely validated through quantitative evidence. The accepted hypotheses indicated that pricing compliance detection, authorization integrity, temporal anomaly identification, and adjustment behavior monitoring each contributed significantly to leakage detection effectiveness (Farrugia et al., 2020). This pattern aligned with earlier studies that proposed similar conceptual structures for transaction-level leakage detection, where pricing and governance-related indicators are central and process-based anomalies provide additional explanatory strength. The rejected hypothesis related to a secondary interaction effect was consistent with earlier research observations that interaction terms often require larger samples, more precise measurement, and highly stable process conditions to demonstrate consistent statistical significance. In transaction-level environments, relationships among constructs can vary across industries, systems, and operational policies, making interaction effects less stable than direct effects. The present findings therefore aligned with earlier evidence that primary detection dimensions tend to show stronger and more consistent relationships than secondary interaction mechanisms. The descriptive and reliability results further supported hypothesis outcomes by demonstrating stable construct measurement and consistent item-

level behavior (Cheng et al., 2023). Earlier studies have emphasized that measurement stability is essential in transaction-level analytics because financial datasets contain noise, missingness, and heterogeneity that can weaken construct coherence. The present findings confirmed that the constructs maintained strong internal consistency, enabling reliable regression and hypothesis testing. The hypothesis results also aligned with earlier research emphasizing that pricing and authorization controls represent the most direct leakage prevention mechanisms, while temporal and adjustment monitoring provide complementary detection signals. The statistical support for all primary constructs reinforced this integrated view (Tahmasbi et al., 2023). Overall, the discussion of hypothesis outcomes remained aligned with empirical decision rules and demonstrated consistency with earlier studies that framed revenue leakage detection as a structured combination of pricing integrity, governance compliance, temporal process monitoring, and adjustment behavior analysis within transaction-level financial datasets.

CONCLUSION

AI-based revenue leakage detection models that operate on transaction-level financial data have been examined extensively in the literature as a response to the growing complexity, volume, and fragmentation of modern revenue cycles. Revenue leakage has been consistently conceptualized as the erosion of legitimately earned income arising from pricing inconsistencies, incomplete billing capture, unauthorized adjustments, delayed invoicing, reconciliation failures, and governance breakdowns that occur within individual financial transactions rather than at aggregated reporting levels. Transaction-level financial data, including invoice line items, payment records, credit and adjustment logs, and ledger postings, provides the granularity necessary to observe these dispersed irregularities that often remain invisible in summary financial statements. The reviewed studies collectively demonstrated that AI-based detection models leverage this granularity by transforming transactional attributes into structured analytical features that capture pricing compliance, authorization integrity, temporal alignment, and behavioral consistency. Supervised learning approaches have been widely applied to classify transactions as leakage-related or compliant based on historical confirmation records, while unsupervised and semi-supervised approaches have modeled normal transaction behavior to identify anomalous deviations without reliance on extensive labeled datasets. Rule-based detection has remained foundational, particularly for pricing and authorization checks, and has been increasingly integrated into hybrid architectures where rule outputs function as engineered features or pre-screening mechanisms for AI models. Across studies, pricing deviation indicators and contract compliance measures consistently emerged as the most influential detection signals, reflecting the central role of pricing integrity in revenue realization. Authorization and approval-trail features also demonstrated strong relevance, highlighting that leakage is frequently linked to governance weaknesses rather than extreme financial outliers. Temporal and sequential modeling added an important process-oriented dimension by capturing abnormal delays, irregular event ordering, and repeated adjustment cycles that signal leakage risk. Adjustment behavior monitoring further complemented these approaches by identifying patterns of excessive credits, reversals, and post-billing modifications that directly reduce realized revenue. Quantitative findings across the reviewed studies showed that models combining multiple transaction-level constructs achieved stronger explanatory and predictive performance than single-factor approaches, supporting the view that revenue leakage is a multi-dimensional phenomenon embedded across the revenue cycle. Reliability and descriptive analyses consistently indicated stable construct measurement and coherent feature behavior, enabling robust regression and hypothesis testing. Overall, the reviewed literature converged on the conclusion that AI-based revenue leakage detection models are most effective when grounded in transaction-level data, integrated across pricing, governance, timing, and adjustment dimensions, and designed to balance interpretability with analytical flexibility, thereby providing a comprehensive framework for identifying revenue erosion within complex financial systems.

RECOMMENDATIONS

using transaction-level financial data, several actionable recommendations emerge for organizations, system designers, and analytics practitioners seeking to strengthen revenue assurance capabilities. First, revenue leakage detection initiatives should be anchored at the transaction level rather than relying on aggregated financial summaries, as granular data provides the necessary visibility to

identify dispersed and low-magnitude leakage patterns that accumulate into material losses. Organizations are recommended to prioritize the integration of invoice line items, pricing components, adjustment records, payment transactions, and ledger postings into a unified analytical dataset, ensuring consistent identifiers and temporal alignment across systems. Second, detection architectures should adopt hybrid frameworks that combine deterministic rule-based controls with AI-driven models. Rule-based mechanisms should be retained for enforcing explicit pricing rules, authorization thresholds, and reconciliation requirements, while AI models should be leveraged to capture complex, multi-factor, and previously unknown leakage patterns that rules alone cannot encode. Third, feature engineering should be treated as a strategic design activity rather than a purely technical step. Features reflecting pricing deviations, contract compliance, approval hierarchy adherence, temporal lags, adjustment frequency, and peer-group comparisons should be systematically developed and validated, as these features have demonstrated strong relevance for leakage detection effectiveness. Fourth, organizations are encouraged to implement cohort-based baselining and segmentation strategies to reduce false positives arising from legitimate variability across products, customers, regions, and billing models. This approach improves detection accuracy by ensuring that anomalies are evaluated relative to appropriate operational contexts. Fifth, anomaly detection and supervised learning models should be deployed primarily as prioritization tools rather than binary decision engines, using continuous risk scores to rank transactions for investigation based on organizational capacity and risk tolerance. Sixth, robust data governance practices are essential, including standardized master data management, explicit handling of missing and noisy fields, and documented transformation logic, as data quality directly influences detection reliability. Seventh, model evaluation and monitoring processes should emphasize stability, interpretability, and consistency over time, using time-aware validation and periodic recalibration to account for operational changes, pricing updates, and system migrations. Finally, organizations should align revenue leakage detection outputs with investigation workflows and control ownership, ensuring that flagged transactions can be traced, explained, and corrected efficiently. Collectively, these recommendations support the development of scalable, explainable, and effective AI-based revenue leakage detection systems that leverage transaction-level financial data to protect realized revenue in complex, high-volume financial environments.

LIMITATIONS

Several limitations were associated with the review of AI-based revenue leakage detection models using transaction-level financial data, and these limitations influenced the scope, comparability, and generalizability of the synthesized findings. A primary limitation involved inconsistency in how revenue leakage was defined and operationalized across studies, as some research treated leakage as pricing noncompliance, others treated it as billing omission, and others emphasized under collection or post-billing adjustment misuse. This definitional variability restricted direct comparison of results because detection models evaluated different leakage phenomena even when using similar algorithms. A second limitation involved variation in transaction-level data structure and availability across industries, as datasets differed substantially in granularity, system integration quality, and presence of process metadata such as approval trails, reason codes, and operational delivery evidence. These differences affected feature engineering strategies and limited the ability to generalize findings across sectors with distinct revenue-cycle architectures. A third limitation concerned label scarcity and label bias in supervised learning studies, as confirmed leakage cases were often derived from audits, disputes, or corrective actions, which reflected detection processes rather than the full universe of leakage events. This limitation introduced selection bias and reduced confidence in model performance estimates reported in some studies. A fourth limitation involved evaluation inconsistency, as studies reported different metrics, validation strategies, and sampling procedures, including non-time-aware splits that may have inflated performance in sequential transaction environments. This restricted the ability to synthesize performance outcomes quantitatively across studies. A fifth limitation involved the influence of data quality issues such as missing fields, inconsistent identifiers, duplicate records, and timestamp ambiguity, which were frequently acknowledged but not uniformly addressed in published methodologies. Since transaction-level leakage detection is highly sensitive to data integration accuracy, incomplete handling of these issues may have contributed to unstable results in some reported models. A sixth limitation involved interpretability constraints, particularly in studies

applying complex ensemble or deep learning methods, where model outputs were less transparent and difficult to align with audit requirements and operational remediation workflows. This limitation reduced practical comparability because detection effectiveness depends not only on statistical accuracy but also on usability in investigation contexts. A final limitation involved restricted reporting of organizational context, as many studies did not provide detailed descriptions of revenue-cycle workflows, governance policies, or system architecture, which constrained understanding of why certain detection approaches performed well in specific environments. Collectively, these limitations indicated that while the reviewed literature provided strong evidence supporting transaction-level AI-based leakage detection, variations in definitions, data structures, labeling quality, and evaluation practices constrained direct cross-study comparability and reduced the precision of general conclusions.

REFERENCES

[1]. Abdulla, M., & Alifa Majumder, N. (2023). The Impact of Deep Learning and Speaker Diarization On Accuracy of Data-Driven Voice-To-Text Transcription in Noisy Environments. *American Journal of Scholarly Research and Innovation*, *2*(02), 415–448. https://doi.org/10.63125/rpjwke42

[2]. Abed, I. A., Hussin, N., Ali, M. A., Haddad, H., Shehadeh, M., & Hasan, E. F. (2022). Creative accounting determinants and financial reporting quality: systematic literature review. *Risks*, *10*(4), 76.

[3]. Ahmed, U., Jiangbin, Z., Almogren, A., Khan, S., Sadiq, M. T., Altameem, A., & Rehman, A. U. (2024). Explainable AI-based innovative hybrid ensemble model for intrusion detection. *Journal of Cloud Computing*, *13*(1), 150.

[4]. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015.

[5]. Alwadain, A., Ali, R. F., & Muneer, A. (2023). Estimating financial fraud through transaction-level features and machine learning. *Mathematics*, *11*(5), 1184.

[6]. Amena Begum, S. (2025). Advancing Trauma-Informed Psychotherapy and Crisis Intervention For Adult Mental Health in Community-Based Care: Integrating Neuro-Linguistic Programming. *American Journal of Interdisciplinary Studies*, *6*(1), 445-479. https://doi.org/10.63125/bezm4c60

[7]. Ara, A., & Ara, A. (2024). A Study of Predictive Analytics for Fraud Detection by Leveraging Machine Learning. International Conference on Evolutionary Artificial Intelligence,

[8]. Asif, H., Min, S., Wang, X., & Vaidya, J. (2024). US-UK PETs prize challenge: Anomaly detection via privacy-enhanced federated learning. *IEEE transactions on privacy*, *1*, 3-18.

[9]. Babaei, A., Tirkolaee, E. B., & Anka, F. (2024). Efficiency-sustainability models to assess blockchain adoption strategies with uncertainty in the oil and gas sector. *Environment, Development and Sustainability*, 1-27.

[10]. Bakumenko, A., & Elragal, A. (2022). Detecting anomalies in financial data using machine learning algorithms. *Systems*, *10*(5), 130.

[11]. Bauw, M., Velasco-Forero, S., Angulo, J., Adnet, C., & Airiau, O. (2020). From unsupervised to semi-supervised anomaly detection methods for HRRP targets. 2020 IEEE Radar Conference (RadarConf20),

[12]. Blankespoor, E., Hendricks, B. E., Piotroski, J., & Synn, C. (2022). Real-time revenue and firm disclosure. *Review of Accounting Studies*, *27*(3), 1079-1116.

[13]. Chang, V., Valverde, R., Ramachandran, M., & Li, C.-S. (2020). Toward business integrity modeling and analysis framework for risk measurement and analysis. *Applied Sciences*, *10*(9), 3145.

[14]. Cheng, D., Ye, Y., Xiang, S., Ma, Z., Zhang, Y., & Jiang, C. (2023). Anti-money laundering by group-aware deep graph learning. *IEEE Transactions on Knowledge and Data Engineering*, *35*(12), 12444-12457.

[15]. Dora, M., Wesana, J., Gellynck, X., Seth, N., Dey, B., & De Steur, H. (2020). Importance of sustainable operations in food loss: evidence from the Belgian food processing industry. *Annals of operations research*, *290*(1), 47-72.

[16]. Fahimul, H. (2022). Corpus-Based Evaluation Models for Quality Assurance Of AI-Generated ESL Learning Materials. *Review of Applied Science and Technology*, *1*(04), 183–215. https://doi.org/10.63125/m33q0j38

[17]. Fahimul, H. (2023). Explainable AI Models for Transparent Grammar Instruction and Automated Language Assessment. *American Journal of Interdisciplinary Studies*, *4*(01), 27-54. https://doi.org/10.63125/wttvnz54

[18]. Farrugia, S., Ellul, J., & Azzopardi, G. (2020). Detection of illicit accounts over the Ethereum blockchain. *Expert Systems with Applications*, *150*, 113318.

[19]. Faysal, K., & Aditya, D. (2025). Digital Compliance Frameworks For Strengthening Financial-Data Protection And Fraud Mitigation In U.S. Organizations. *Review of Applied Science and Technology*, *4*(04), 156–194. https://doi.org/10.63125/86zs5m32

[20]. Faysal, K., & Tahmina Akter Bhuya, M. (2023). Cybersecure Documentation and Record-Keeping Protocols For Safeguarding Sensitive Financial Information Across Business Operations. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 117–152. https://doi.org/10.63125/cz2gwm06

[21]. Gupta, A., Dwivedi, D. N., & Shah, J. (2023a). Artificial intelligence-driven effective financial transaction monitoring. In *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance* (pp. 79-91). Springer.

[22]. Gupta, A., Dwivedi, D. N., & Shah, J. (2023b). Data organization for an FCC unit. In *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance* (pp. 41-56). Springer.

[23]. Habibullah, S. M., & Aditya, D. (2023). Blockchain-Orchestrated Cyber-Physical Supply Chain Networks with Byzantine Fault Tolerance For Manufacturing Robustness. *Journal of Sustainable Development and Policy*, *2*(03), 34-72. https://doi.org/10.63125/057vwc78

[24]. Hammad, S. (2022). Application of High-Durability Engineering Materials for Enhancing Long-Term Performance of Rail and Transportation Infrastructure. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 63-96. https://doi.org/10.63125/4k492a62

[25]. Hammad, S., & Md Sarwar Hossain, S. (2025). Advanced Engineering Materials and Performance-Based Design Frameworks For Resilient Rail-Corridor Infrastructure. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 368–403. https://doi.org/10.63125/c3g3sx44

[26]. Hammad, S., & Muhammad Mohiul, I. (2023). Geotechnical And Hydraulic Simulation Models for Slope Stability And Drainage Optimization In Rail Infrastructure Projects. *Review of Applied Science and Technology*, *2*(02), 01–37. https://doi.org/10.63125/jmx3p851

[27]. Haque, B. M. T., & Md. Arifur, R. (2021). ERP Modernization Outcomes in Cloud Migration: A Meta-Analysis of Performance and Total Cost of Ownership (TCO) Across Enterprise Implementations. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 168–203. https://doi.org/10.63125/vrz8hw42

[28]. Haque, B. M. T., & Md. Arifur, R. (2023). A Quantitative Data-Driven Evaluation of Cost Efficiency in Cloud and Distributed Computing for Machine Learning Pipelines. *American Journal of Scholarly Research and Innovation*, *2*(02), 449–484. https://doi.org/10.63125/7tkcs525

[29]. Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*, *513*, 386-396.

[30]. Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, *11*(1), 1-22.

[31]. Huong, H., Nguyen, X., Dang, T. K., & Tran-Truong, P. T. (2024). Money laundering detection using a transaction-based graph learning approach. 2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM),

[32]. Jabed Hasan, T., & Waladur, R. (2022). Advanced Cybersecurity Architectures for Resilience in U.S. Critical Infrastructure Control Networks. *Review of Applied Science and Technology*, *1*(04), 146–182. https://doi.org/10.63125/5rvjav10

[33]. Jahangir, S. (2025). Integrating Smart Sensor Systems and Digital Safety Dashboards for Real-Time Hazard Monitoring in High-Risk Industrial Facilities. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1533–1569. https://doi.org/10.63125/newtd389

[34]. Jahangir, S., & Hammad, S. (2024). A Meta-Analysis of OSHA Safety Training Programs and their Impact on Injury Reduction and Safety Compliance in U.S. Workplaces. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 559–592. https://doi.org/10.63125/8zxw0h59

[35]. Jahangir, S., & Muhammad Mohiul, I. (2023). EHS Analytics for Improving Hazard Communication, Training Effectiveness, and Incident Reporting in Industrial Workplaces. *American Journal of Interdisciplinary Studies*, *4*(02), 126-160. https://doi.org/10.63125/ccy4x761

[36]. Kadhim, Y. A., & Al Ani, S. A. M. (2023). Using artificial intelligence and metaverse techniques to reduce earning management. International Multi-Disciplinary Conference-Integrated Sciences and Technologies,

[37]. Kao, J.-H., & Tsay, R.-S. (2023). Preventing financial statement fraud with blockchain-based verifiable accounting system. 2023 3rd international conference on electrical, computer, communications and mechatronics engineering (ICECCME),

[38]. Kazova, F., Alkan, M. A., & Yüksel, M. K. (2024). Forecasting the Profit or Loss Status of Companies using Machine Learning. 2024 8th International Symposium on Innovative Approaches in Smart Technologies (ISAS),

[39]. Khan, A. T., Cao, X., Li, S., Katsikis, V. N., Brajevic, I., & Stanimirovic, P. S. (2022). Fraud detection in publicly traded US firms using Beetle Antennae Search: A machine learning approach. *Expert Systems with Applications*, *191*, 116148.

[40]. Kim, J., Jung, H., & Kim, W. (2022). Sequential pattern mining approach for personalized fraudulent transaction detection in online banking. *Sustainability*, *14*(15), 9791.

[41]. Kim, Y. J., Nam, W., & Lee, J. (2022). Multiclass anomaly detection for unsupervised and semi-supervised data based on a combination of negative selection and clonal selection algorithms. *Applied Soft Computing*, *122*, 108838.

[42]. Klein, N. K., Lattermann, F., & Schiereck, D. (2023). Investment in non-fungible tokens (NFTs): the return of Ethereum secondary market NFT sales. *Journal of Asset Management*, *24*(4), 241-254.

[43]. Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. *IEEE Access*, *9*, 82300-82317.

[44]. Li, B., Yen, J., & Wang, S. (2024). Uncovering Financial Statement Fraud: A Machine Learning Approach with Key Financial Indicators and Real-World Applications. *IEEE Access*.

[45]. Li, Z., Zhang, Y., Wang, Q., & Chen, S. (2022). Transactional network analysis and money laundering behavior identification of central bank digital currency of china. *Journal of Social Computing*, *3*(3), 219-230.

[46]. Lin, D., Wu, J., Yuan, Q., & Zheng, Z. (2020). Modeling and understanding ethereum transaction records via a complex network approach. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *67*(11), 2737-2741.

[47]. Machado, M. R., & Karray, S. (2022). Applying hybrid machine learning algorithms to assess customer risk-adjusted revenue in the financial industry. *Electronic Commerce Research and Applications*, *56*, 101202.

[48]. Masud, R., & Hammad, S. (2024). Computational Modeling and Simulation Techniques For Managing Rail–Urban Interface Constraints In Metropolitan Transportation Systems. *American Journal of Scholarly Research and Innovation*, *3*(02), 141–178. https://doi.org/10.63125/pxet1d94

[49]. Md Ashraful, A., Md Fokhrul, A., & Md Fardaus, A. (2020). Predictive Data-Driven Models Leveraging Healthcare Big Data for Early Intervention And Long-Term Chronic Disease Management To Strengthen U.S. National Health Infrastructure. *American Journal of Interdisciplinary Studies*, *1*(04), 26-54. https://doi.org/10.63125/1z7b5v06

[50]. Md Fokhrul, A., Md Ashraful, A., & Md Fardaus, A. (2021). Privacy-Preserving Security Model for Early Cancer Diagnosis, Population-Level Epidemiology, And Secure Integration into U.S. Healthcare Systems. *American Journal of Scholarly Research and Innovation*, *1*(02), 01–27. https://doi.org/10.63125/q8wjee18

[51]. Md Harun-Or-Rashid, M., Mst. Shahrin, S., & Sai Praveen, K. (2023). Integration Of IOT And EDGE Computing For Low-Latency Data Analytics In Smart Cities And Iot Networks. *Journal of Sustainable Development and Policy*, *2*(03), 01-33. https://doi.org/10.63125/004h7m29

[52]. Md Harun-Or-Rashid, M., & Sai Praveen, K. (2022). Data-Driven Approaches To Enhancing Human–Machine Collaboration In Remote Work Environments. *International Journal of Business and Economics Insights*, *2*(3), 47-83. https://doi.org/10.63125/wt9t6w68

[53]. Md Jamil, A. (2025). Systematic Review and Quantitative Evaluation of Advanced Machine Learning Frameworks for Credit Risk Assessment, Fraud Detection, And Dynamic Pricing in U.S. Financial Systems. *International Journal of Business and Economics Insights*, *5*(3), 1329–1369. https://doi.org/10.63125/9cyn5m39

[54]. Md, K., & Sai Praveen, K. (2024). Hybrid Discrete-Event And Agent-Based Simulation Framework (H-DEABSF) For Dynamic Process Control In Smart Factories. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 72–96. https://doi.org/10.63125/wcqq7x08

[55]. Md Khaled, H., & Md. Mosheur, R. (2023). Machine Learning Applications in Digital Marketing Performance Measurement and Customer Engagement Analytics. *Review of Applied Science and Technology*, *2*(03), 27–66. https://doi.org/10.63125/hp9ay446

[56]. Md Syeedur, R. (2025). Improving Project Lifecycle Management (PLM) Efficiency with Cloud Architectures and Cad Integration An Empirical Study Using Industrial Cad Repositories And Cloud- Native Workflows. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 452–505. https://doi.org/10.63125/8ba1gz55

[57]. Md. Al Amin, K. (2025). Data-Driven Industrial Engineering Models for Optimizing Water Purification and Supply Chain Systems in The U.S. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1458–1495. https://doi.org/10.63125/s17rjm73

[58]. Md. Arifur, R., & Haque, B. M. T. (2022). Quantitative Benchmarking of Machine Learning Models for Risk Prediction: A Comparative Study Using AUC/F1 Metrics and Robustness Testing. *Review of Applied Science and Technology*, *1*(03), 32–60. https://doi.org/10.63125/9hd4e011

[59]. Md. Towhidul, I., Alifa Majumder, N., & Mst. Shahrin, S. (2022). Predictive Analytics as A Strategic Tool For Financial Forecasting and Risk Governance In U.S. Capital Markets. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 238–273. https://doi.org/10.63125/2rpyze69

[60]. Md. Towhidul, I., & Rebeka, S. (2025). Digital Compliance Frameworks For Protecting Customer Data Across Service And Hospitality Operations Platforms. *Review of Applied Science and Technology*, *4*(04), 109–155. https://doi.org/10.63125/fp60z147

[61]. Mehrotra, R., Nolintha, V., & Sayavong, V. (2023). Commodity Trade Mispricing: Evidence from Lao PDR. *The International Trade Journal*, *37*(4), 401-425.

[62]. Mohd Marzuki, N. H., Che Tahrim, S. N., & Muhammad, M. Z. (2022). Refining Pawah System Using Mudarabah Concept. International Conference on Entrepreneurship, Business and Technology,

[63]. Molan, M., Borghesi, A., Cesarini, D., Benini, L., & Bartolini, A. (2023). RUAD: Unsupervised anomaly detection in HPC systems. *Future Generation Computer Systems*, *141*, 542-554.

[64]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[65]. Narejo, A., Li, J. P., Sanjrani, A. N., Sanjrani, A. A., & Iqtidar, A. (2024). Dynamic Temporal LSTM-Seqtrans for Long Sequence: An Approach for Credit Card and Banking Accounts Fraud Detection in Banking System. 2024 21st International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP),

[66]. Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, *9*, 163965-163986.

[67]. Nissim, D. (2022). Big data, accounting information, and valuation. *The Journal of Finance and Data Science*, *8*, 69-85.

[68]. Ratul, D. (2025). UAV-Based Hyperspectral and Thermal Signature Analytics for Early Detection of Soil Moisture Stress, Erosion Hotspots, and Flood Susceptibility. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1603–1635. https://doi.org/10.63125/c2vtn214

[69]. Ratul, D., & Subrato, S. (2022). Remote Sensing Based Integrity Assessment of Infrastructure Corridors Using Spectral Anomaly Detection and Material Degradation Signatures. *American Journal of Interdisciplinary Studies*, *3*(04), 332-364. https://doi.org/10.63125/1sdhwn89

[70]. Rauf, M. A. (2018). A needs assessment approach to english for specific purposes (ESP) based syllabus design in Bangladesh vocational and technical education (BVTE). *International Journal of Educational Best Practices*, *2*(2), 18-25.

[71]. Reim, W., Lenka, S., Parida, V., & Frishammar, J. (2022). Value Leakage in Product–Service System Provision: A Business Model Alignment Perspective. *IEEE transactions on engineering management*, *71*, 940-951.
[72]. Rifat, C. (2025). Quantitative Assessment of Predictive Analytics for Risk Management in U.S. Healthcare Finance Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1570–1602. https://doi.org/10.63125/x4cta041
[73]. Rifat, C., & Jinnat, A. (2022). Optimization Algorithms for Enhancing High Dimensional Biomedical Data Processing Efficiency. *Review of Applied Science and Technology*, *1*(04), 98–145. https://doi.org/10.63125/2zg6x055
[74]. Rifat, C., & Khairul Alam, T. (2022). Assessing The Role of Statistical Modeling Techniques in Fraud Detection Across Procurement And International Trade Systems. *American Journal of Interdisciplinary Studies*, *3*(02), 91-125. https://doi.org/10.63125/gbdq4z84
[75]. Rifat, C., & Rebeka, S. (2023). The Role of ERP-Integrated Decision Support Systems in Enhancing Efficiency and Coordination In Healthcare Logistics: A Quantitative Study. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 265–285. https://doi.org/10.63125/c7srk144
[76]. Rifat, C., & Rebeka, S. (2024). Integrating Artificial Intelligence and Advanced Computing Models to Reduce Logistics Delays in Pharmaceutical Distribution. *American Journal of Health and Medical Sciences*, *5*(03), 01–35. https://doi.org/10.63125/t1kx4448
[77]. Saadullah, S. M., & Elsayed, N. (2020). An audit simulation of the substantive procedures in the revenue process–A teaching case incorporating Bloom's taxonomy. *Journal of Accounting Education*, *52*, 100678.
[78]. Saheed, Y. K., Hambali, M. A., Arowolo, M. O., & Olasupo, Y. A. (2020). Application of GA feature selection on Naive Bayes, random forest and SVM for credit card fraud detection. 2020 international conference on decision aid sciences and application (DASA),
[79]. Sai Praveen, K. (2024). AI-Enhanced Data Science Approaches For Optimizing User Engagement In U.S. Digital Marketing Campaigns. *Journal of Sustainable Development and Policy*, *3*(03), 01-43. https://doi.org/10.63125/65ebsn47
[80]. Sharif Md Yousuf, B., Md Shahadat, H., Saleh Mohammad, M., Mohammad Shahadat Hossain, S., & Imtiaz, P. (2025). Optimizing The U.S. Green Hydrogen Economy: An Integrated Analysis Of Technological Pathways, Policy Frameworks, And Socio-Economic Dimensions. *International Journal of Business and Economics Insights*, *5*(3), 586–602. https://doi.org/10.63125/xp8exe64
[81]. Shehwar, D., & Nizamani, S. A. (2024). Power Dynamics in Indian Ocean: US Indo-Pacific Strategic Report and Prospects for Pakistan's National Security. *Government: Research Journal of Political Science*, *13*.
[82]. Shofiul Azam, T. (2025). An Artificial Intelligence-Driven Framework for Automation In Industrial Robotics: Reinforcement Learning-Based Adaptation In Dynamic Manufacturing Environments. *American Journal of Interdisciplinary Studies*, *6*(3), 38-76. https://doi.org/10.63125/2cr2aq31
[83]. Shofiul Azam, T., & Md. Al Amin, K. (2023). A Hybrid Lean-Six Sigma Model with Automated Kaizen for Real-Time Quality Improvement. *American Journal of Scholarly Research and Innovation*, *2*(01), 412–442. https://doi.org/10.63125/n994vk64
[84]. Shoflul Azam, T., & Md. Al Amin, K. (2024). Quantitative Study on Machine Learning-Based Industrial Engineering Approaches For Reducing System Downtime In U.S. Manufacturing Plants. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 526–558. https://doi.org/10.63125/kr9r1r90
[85]. Staszkiewicz, P., & Werner, A. (2021). Reporting and disclosure of investments in sustainable development. *Sustainability*, *13*(2), 908.
[86]. Tahmasbi, N., Shan, G., & French, A. M. (2023). Identifying washtrading cases in NFT sales networks. *IEEE Transactions on Computational Social Systems*, *11*(2), 1696-1707.
[87]. Tasnim, K. (2025). Digital Twin–Enabled Optimization of Electrical, Instrumentation, And Control Architectures In Smart Manufacturing And Utility-Scale Systems. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 404–451. https://doi.org/10.63125/pqfdjs15
[88]. Tatulli, M. P., Paladini, T., D'Onghia, M., Carminati, M., & Zanero, S. (2023). HAMLET: A transformer based approach for money laundering detection. International Symposium on Cyber Security, Cryptology, and Machine Learning,
[89]. Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., & Choraś, M. (2024). Towards hybrid nids: Combining rule-based siem with ai-based intrusion detectors. International Conference on Advances in Computing Research,
[90]. Usman, A. U., Abdullahi, S. B., Liping, Y., Alghofaily, B., Almasoud, A. S., & Rehman, A. (2024). Financial fraud detection using value-at-risk with machine learning in skewed data. *IEEE Access*, *12*, 64285-64299.
[91]. Vashisth, A., Salako, K., & Pinto, P. (2024). Digital assets valuation and financial reporting. In *Leveraging Blockchain Technology* (pp. 93-114). CRC Press.
[92]. Wang, B., Yuan, X., Duan, L., Ma, H., Su, C., & Wang, W. (2022). DeFiScanner: Spotting DeFi attacks exploiting logic vulnerabilities on blockchain. *IEEE Transactions on Computational Social Systems*, *11*(2), 1577-1588.
[93]. Wang, Y., Liu, Y., Wang, N., Li, P., Hu, J., Fu, X., Wang, W., Sun, K., Li, Q., & Xu, K. (2024). Enhancing Fraud Transaction Detection via Unlabeled Suspicious Records. 2024 IEEE/ACM 32nd International Symposium on Quality of Service (IWQoS),
[94]. Wilkoff, S., & Yildiz, S. (2023). The behavior and determinants of illiquidity in the non-fungible tokens (NFTs) market. *Global Finance Journal*, *55*, 100782.

[95]. Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., & Zhang, Y. (2021). Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(4), 2237-2249.

[96]. Yan, X. (2023). Research on financial field integrating artificial intelligence: Application basis, case analysis, and SVR model-based overnight. *Applied Artificial Intelligence*, *37*(1), 2222258.

[97]. Yoon, K., Liu, Y., Chiu, T., & Vasarhelyi, M. A. (2021). Design and evaluation of an advanced continuous data level auditing system: A three-layer structure. *International Journal of Accounting Information Systems*, *42*, 100524.

[98]. Zaheda, K. (2025a). AI-Driven Predictive Maintenance For Motor Drives In Smart Manufacturing A Scada-To-Edge Deployment Study. *American Journal of Interdisciplinary Studies*, *6*(1), 394-444. https://doi.org/10.63125/gc5x1886

[99]. Zaheda, K. (2025b). Hybrid Digital Twin and Monte Carlo Simulation For Reliability Of Electrified Manufacturing Lines With High Power Electronics. *International Journal of Scientific Interdisciplinary Research*, *6*(2), 143–194. https://doi.org/10.63125/db699z21

[100]. Zaman, M. A. U., Sultana, S., Raju, V., & Rauf, M. A. (2021). Factors İmpacting the Uptake of İnnovative Open and Distance Learning (ODL) Programmes in Teacher Education. *Turkish Online Journal of Qualitative Inquiry*, *12*(6).

[101]. Zhang, B., Zhang, H., Le, V.-H., Moscato, P., & Zhang, A. (2023). Semi-supervised and unsupervised anomaly detection by mining numerical workflow relations from system logs. *Automated Software Engineering*, *30*(1), 4.

[102]. Zhang, Q., Lu, Z., Liu, S., Yang, H., & Pan, J. (2024). An MA-MRR model for transaction-level analysis of high-frequency trading processes. *Journal of Management Science and Engineering*, *9*(1), 53-61.

[103]. Zhang, X., Sun, W., Xu, Z., Cheng, H., Cai, C., Cui, H., & Li, Q. (2024). Evm-shield: In-contract state access control for fast vulnerability detection and prevention. *IEEE Transactions on Information Forensics and Security*, *19*, 2517-2532.

[104]. Zhou, L., Qin, K., Cully, A., Livshits, B., & Gervais, A. (2021). On the just-in-time discovery of profit-generating transactions in defi protocols. 2021 IEEE Symposium on Security and Privacy (SP),

[105]. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). Sok: Decentralized finance (defi) attacks. 2023 IEEE Symposium on Security and Privacy (SP),

[106]. Zulqarnain, F. N. U. (2025). High-Performance Computing Frameworks for Climate And Energy Infrastructure Risk Assessment. *Review of Applied Science and Technology*, *4*(04), 74–108. https://doi.org/10.63125/ks5s9m05