International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

Explainable Artificial Intelligence for Journal Entry Anomaly Detection and Continuous Financial Auditing

Dr.R.Sugumar

Professor, Department of Computer Science & Engineering, SIMATS Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, India

ABSTRACT: The financial audit is proving to be holding its own in the sense of necessity to have intelligent mechanisms which not only enable to identify aberrations in the journal entries but also provide a clear and understandable evidence on the basis of audit decision. In this paper, an Explainable Artificial Intelligence (XAI) architecture of Journal Entry Anomaly Detection and Continuous Financial auditing is presented, an architecture merging data preprocessing, feature engineering, anomaly detection, explainability, risk assessment and continuous audit monitoring into one architecture. The framework analyzes properties of transactions such as time of posting, relationship between the account and the user, amount of transaction, user, document and historical online accounting trends to identify suspicious journal entries. Models used to detect anomalies are created to produce their own risk score and explainability mechanisms are used to interpret the factors behind each of the flagged transactions. The proposed framework also has control based on accounting rules and continuous monitoring which helps in the facilitation of early identification of the potentially suspicious financial activities. The given features, risk types and description summaries of high-priority transactions are displayed in an interactive audit layer, allowing the auditor to examine the anomaly scores. The framework evaluation is interested in the efficiency of detection, consistency of the explanations, reduction of false-positive and efficiency of audit response. The framework will promote transparency to the audit, accountability, and ongoing financial control and reduce the use of largely-manual transaction screening, with this methodology which combines automated anomaly detection with easily-understandable evidence.

KEYWORDS: Explainable Artificial Intelligence, Journal Entry Anomaly Detection, Continuous Auditing, Financial Fraud Detection, Risk Assessment, Interpretable Machine Learning

I. INTRODUCTION

The wave of digitization of accounting systems has turned fiscal transaction processing into regular, per-period, manually-inspected activities into highly automated, and constantly updated operations. The current enterprise resource planning (ERP) systems generate huge amounts of journal entries which include an array of account codes, transaction value, transaction date, user, attachment filings and department. Although financial reporting has its advantages, the automation of the reporting overly limits the scope of authority because of the sheer size and complexity of transactions, it is not particularly practical to conduct any very detailed examination of the same manually. Consequently, companies require effective analytical systems that have the capabilities of identifying fraudulent journal entries, and those that require further audit. Machine learning has come up as a significant solution to this need since it can recognize intricate associations and tendency patterns that might not be sufficiently recognized by the traditional accounting guidelines.

Financial fraud and accounting abnormalities tend to be subtle and involving the organization and its transactions. The common traditional audit procedures are based on pre-determined rules, sampling, threshold-based testing, as well as experience of the auditor. These techniques are not as efficient as they are currently important, but they produce considerable alert counts in large volumes of financial data and are not so efficient as detecting new patterns. Financial fraud detection via machine learning has thus been a growing focus of research. The metacategorization models have demonstrated the potential of applying a combination of two or more predictive models in improvement of financial fraud pattern detection [1]. According to these strategies, the definition of financial anomalies is possible based on many, rather than a single, signal predictive models.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

Detection of accounting fraud has also been done using machine learning on data relating to publicly traded companies. Automated models can be used to analyze financial features with the aim of determining nonlinear relationships that are connected to potentially fraudulent reporting [2]. This innovation demonstrates how the traditional auditing can be complemented with the use of data-driven solutions. Firm-level detection of fraud and financial-statement analysis are however not always effective in detecting the journal entries themselves which cause or lead to an accounting anomaly. The practice of continuous financial auditing would be particularly interested in transaction level analysis, as the auditors may need to make decisions as to what kind of entries may be audited further.

The journal-entry level analysis implies a closer look on the identification of the financial risks. One way of scoring by individual entries according to their probable risk in an ERP environment, is demonstrated with the help of a machine learning-enhanced journal-entry risk-scoring framework, which was created during the financial-close process [3]. This type of risk scoring can be used to augment a customary audit procedure in which it is performed in a retrospective fashion in bulk to more transactional monitoring. A risk-oriented system should not deal with the journal entries in the same way assigning priorities to different levels and utilizing the priorities as a guide through which the auditors can focus on the transactions that have unusual features. This is especially true of continuous auditing in which the financial information can be analysed numerous times or just once in realtime as the transactions are generated.

Machine learning has also been seen to be effective in detection of accounting misstatements. Driven-by-data models are able to find trends that are dependent on financial reporting anomalies and can be used to effectively supplement the normal audit process [4]. But, a critical issue comes in when the predictions given by such state-of-the-art machine learning models lack an explainable cause behind the benchmarked predictions. In a financial auditing setting, it may not be enough to declare an entry in a journal as being anomalous. The auditors usually require the supporting evidence to tell them the nature of the transactions which occasioned the high risk and why a higher weight should be extra ordinary to the transaction. In turn, interpretability and transparency are positive forces of feasible AI-assisted auditing. The studies on financial fraud detection have also shown that it was important to analyze the accounting information of various organizational and reporting settings. Research using the financial statements data revealed that machine learning has potential to detect the pattern related to fraudulent reporting in the listed businesses [5]. These results endorse the more generalizability of smart analytical methods to financial-risk detection. These are however aggregated in a financial statement and the evidence of transactions is detailed in journal entries. Consequently, a journal-entry-specific model could benefit the audit investigation process, providing more actionable-related information which can be traced down to one transaction due to identified risks.

The increased use of automated financial analysis, therefore, poses a need of an integrated system that incorporates anomaly detection, explainability, and risk scoring, and continuous audit tracking. This framework ought to decompose the feature attributes of journal-entries, known deviations to normal accounting behavior, quantifying the risk of anomaly and providing comprehensible explanations to the observed anomalies. The goal is to provide a smart decision-support system that will help them prioritize potentially valuable transactions and audit the evidence of each alert instead of replacing auditors.

In this paper, the suggested Explainable Artificial Intelligence and Journal Entry Anomaly Detection and Continuous Financial Auditing are proposed. The framework includes transaction preprocesses, feature engineering, detection of anomalies which is done by the machine using the scoring of risk, explainable feature, validation by the accounting and real-time monitoring. Transactional, temporal, account-level and behavioral characteristics of journal entries are used to transform them into analytical representations. Detection models show when something unusual goes on and explainability mechanisms, show what goes into the individual scores of anomaly. The ensuing information on risks can be then transformed to an auditor based monitoring layer to prioritize and probe the transactions.

The proposed solution will take a transitional step between the automated detection of anomalies and actual audit interpretation. With predictive analytics, and transparent explanations, the framework can assist a shift to more frequent and less retrospective transaction analysis to more risk-oriented financial auditing. The framework assessment of it revolves around the effectiveness of detection, consistency of its explanation and the risk prioritization along with the effective utility of the generated audit evidence. The overall goal is to make available a clear and scalable analytical framework of how potentially anomalous journal entries can be found and how timely, evidence based, and financial audit processes can be facilitated.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

II. RELATED WORK

More recent work added to using machine learning as a means of detecting financial fraud, predicting accounting misstatements, lessening anomalies in transactions, and explaining decision support has resulted in a heightened interest in this area. All these developments underlie the use of automated anomaly detection with transparent financial auditing. However, the existing studies differ greatly in the degree of their data granularity, perceivable purposes, the degree to which they can be interpreted and to which extent they can be integrated with ongoing auditing processes.

The early research conducted has demonstrated machine learning as a viable approach as far as detecting advanced financial fraud trends are concerned. A meta-learning architecture showed how factorizing multiple learning strategies could help them to better detect financial fraud than just using a single classifier [6]. As this investigation has revealed, there is a need to take advantage of variability of the predictive models in situations where financial frauds are of a heterogeneous nature. Similarly, this is observed when balance sheets of Chinese listed-companies that applied machine learning were analysed, information in financial reporting could be used to determine fraud and non-fraud behaviours [5]. These studies determined the possibility of automated analysis methods in detecting financial irregularities but focused mostly on the indicators at the organizational or financial-statement level (as opposed to individual journal entries).

Future research turned its focus on misstatement detection and accounting specific anomaly detection. The machine learning methods were devised to recognize accounting fraud in the prevalence of publicly traded companies based on financial and organizational features [2]. These methods showed that the presence of nonlinear links between accounting variables are useful signupers of the possibility of fraudulent reporting. The use of machine learning to detect accounting misstatements was also researched, with results indicating the predictive capabilities of models to audit-related financial statements [4]. Even these contributions can be easily adapted to automated auditing since they demonstrate how machine learning can complement the traditional rule-based processes. Nevertheless, they largely focus on the financial statements or firm-levels of observation, however journal-entry analysis deals with the transaction level analysis of posting behavior, posting amounts, posting account and timing and the nature of users.

Operating on the journal-entry anomaly-detection problem, a machine-learning-based financial-close-risk-score in SAP S/4HANA provides a closer relationship [3]. The framework concentrates on risk scores that can be given to journal entries in the financial-close process showing that transaction-level analytics can be used to detect journal entries that need additional risk audit. This point of view can be very pertinent to continuous auditing since risk scoring will allow auditors to focus on suspicious transactions instead of proceeding to review the entire population of transactions manually. However, one can impose risk scoring at the transaction level with explainability mechanisms and provide these explanations as to why this or that journal entry has been scored as abnormal.

The increasing use of complicated machine learning models has also led to the heightening of relevance of explainable artificial intelligence (XAI). A structured perception of XAI indicated that the black-box predictive systems had to be made explainable to its users, by any way of providing meaningful explanations of how the system arrived at decisions [8]. Explanations are particularly important in the field of financial auditing since prior to an auditor examines or escalates a transaction, an auditor must have the capability to comprehend and use explanatory evidence. A more abstract analysis on the subject of the explanation in artificial intelligence also noted how the explanations have to be invoked to match human mental abilities in their attribution of causes, choices and also unexpected implications rather than an exposure of model internals [9]. These principles provide a strong foundation on which auditor friendly explanations of journal-entry anomalies detected can be built.

Specialized kinds of explainability methods exist as well that have been investigated in financial modelling. A Shapley-Lorenz-based XAI suggested a framework to understand the contribution of features and model outputs in an easier to understand way [7]. Transformation These contribution-based models can be applicable in identifying financial anomalies as auditors can know the most contributing characteristics of transactions to the high risk score. Other areas that have been enquired in explainable machine learning include credit risk management, where interpretable predictive models have been found helpful in augmenting decision making in financial environments that are heavily regulated [11]. The vision of credit risk is quite different in contrast to journal-entry auditing, yet the emphasis on conspicuous assessment of risk is evidently associated with the financial audit applications.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

Explainability as something to be applied practically and as involving a human factor has also found studies conducted. Explainable machine learning at deployed state addressed the issues that revolve around how explanations can be transformed into meaningful information to real-world users [12]. This is critical to ongoing financial auditing since an explanation should not just be provided to accompany an anomaly score but should serve to guide auditors to gain insight as to the underlying risk factors and whether further investigation should be proceeded with. Equally, a study on the impact of explainable AI on users information processing revealed that explanations have the capability of moderating the way user interpret and process the information generated by AI [10]. This again support use of explanation interfaces which will be grounded on the requirement of the human decision-makers rather than the interpretation of interpretability as an entirely technical property.

XAI has also been utilized in the field of financial decision-making. An example of explainable AI has been applied to crypto-asset allocation, in which very complex financial models are solved, using explainable information about the decisions made by the model [14]. Despite the fact that the area where the application is carried out is not auditing, the research justifies the general need to have transparency in case AI systems are applied under financial sensitive scenarios. The studies, in sum, indicate that explainability can be utilized to make machine learning more useful by reducing the gulf between explainable evidence and predictive output.

Another important research direction is also related to ensemble learning. The contributions of diversity in learners and the classifier-combination schemes have been investigated in regards to heterogeneous classifier groups [13]. Ensemble techniques can be used on information held in financial anomalies because suspicious transactions may bear numerous patterns of behavior, which cannot be detected by a single, algorithm. Combining information provided by various sources of predictors was also shown to add value to the combination of expert predictions in the previous studies [15]. Although forecasting is not an and anomaly detection, it is based on the principle of integrating complementary predictive signals, which can guide multi-model financial risk assessment.

Altogether, the literature shows that machine learning-based financial fraud detection has made significant strides towards transaction-level risk scoring and explainable financial decision support. Nonetheless, unified implementation on the use of transaction-level journal-entry anomaly detection, elucidable risk evaluation, accounting, and ongoing audit is lacking. The focus in existing literature is on either the individual problem of choosing either fraud-detection, misstatement-detecting, journal-entry risk scoring, explainability or the ensemble learning. The suggested framework fills this gap by using a combination of anomaly detection and interpretable feature-level explanations, risk prioritization, accounting-rule validation and continuous monitoring. Not only would this integration enable auditors to recognize potential anomalous journal entries through automation but it would also present them with understandable evidence to aid in timely and transparent audit investigation.

III. INTELLIGENT AUDIT INTELLIGENCE AND EXPLAINABLE JOURNAL-RISK FRAMEWORK

The proposed model will include machine learning, explainable artificial intelligence (XAI), account control and a constant monitoring of the proposed abnormal journal entries. The architecture is designed to be consumed as an intelligent auditing support layer over top of typical accounting or ERP systems. The framework is not limited to the application of predefined rules or periodically sampled situations but can continuously examine the nature of journal-entry, score anomaly risks, explain why the risks are serious and highlight prioritized evidence to auditors. There are seven interconnected steps presented in the general model: the acquisition of journal entries, data preparation, preparation of behavioral features, anomaly detection, explainable score of risk, audit validation, and the further monitoring.

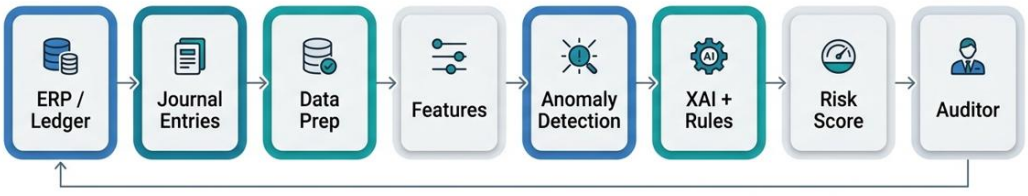


Figure 1- Explainable Journal-Entry Audit Framework

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

3.1 Journal-Entry Acquisition and Audit Data Layer

The first layer collects journal-entry data, ERP, accounting, and financial-close systems and general-ledger systems. A journal record might consist of the transaction amount, debit account, credit account, date of entry, the document type, company code, a cost center, currency, user identifier, the approval details, document reference and description of entry. Contextual information (where it is available) like historical posting behavior, account frequency, reversal signs and posting-period characteristics can be included as well.

The data acquisition layer constructs usual form of heterogeneous accounts of analysis. Each transaction gets a unique identifier to help trace the original accounting record of an analysis. Such a traceability is significant to audit since an anomaly spotted by the framework is finally to be traced to the accounting document and evidence.

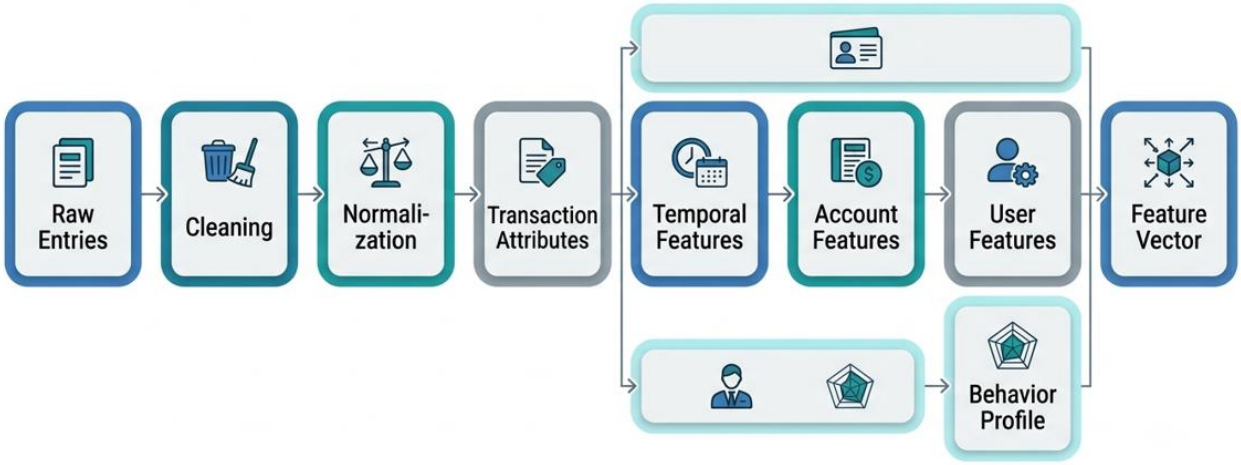


Figure 2- Journal-Entry Data Processing and Behavioral Feature Pipeline

3.2 Data Preparation and Quality Assurance

Raw accounting data often has missing data, redundant records, lack of uniform forms and shapes, nominal variables, and extremely skewed financial amounts. The preprocessing module therefore manages to validate data, identify duplicates, handle missing values, categorize values, normalization of numerical values as and where necessary and consistency check of debit and credit data.

In extreme transaction values, particular attention should be paid to them because they could be both effective high-value business transactions and even accounting practices. The framework does not automatically reject such observations, rather, it just stores them but leaves it to the layer of anomaly detection to determine the risk towards them. Time also gets normalized so as to enable comparisons across accounting periods.

Derived indicators are also generated during the preprocessing step which consist of, transaction frequency, amount deviation, posting-period deviation, unusual-hour indicator, reversal frequency, account-user association. These transformations help convert the unstructured records of accounting into the form of structured features of analysis and maintain its audit ability.

3.3 Behavioral and Contextual Feature Engineering

The analytical center of the suggested framework is comprised of the feature-engineering layer. The framework does not evaluate a journal entry in terms of the significance of the monetary value but rather in terms of different dimensions to reach out to the behavior of a transaction.

Among features based on amount, there are transaction value, relative deviation on historic account amounts, logarithmic transaction magnitude and deviation of typical user-level transaction values. Temporal features consist of posting hour, day-of-week, month end activity, period end concentration and unusual posting hours. The account-

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

related features comprise debit-credit mixes, frequency of account, anomalous account associations, and typical past account operation.

User properties define how the users are associated with the accounts, how often transactions are done, unfamiliar user account association and deviation of user profile posting. Document characteristics may also include document type, reversal, reference availability, description characteristics and duplicate like characteristics. All these features enable the framework to detect the anomalies in the context that might otherwise have been overlooked by merely relying on amount-based rules.

Behaviors are based on transactions. The normal accounting behavior of the involved users, accounts, periods, as well as type of transactions, is considered as the basis. The journal entries, which have been made up to date, can then be compared to this baseline in order to detect deviations.

3.4 Hybrid Anomaly Detection Engine

The proposed anomaly-detection layer will have a hybrid analysis which will consist of machine learning and accounting controls. Anomaly detection, which is unsupervised or semi-supervised is especially needed in cases where assured fraud labels are few. The normal patterns of transaction can be learnt by the models, with an assignment of higher scores of anomalies related to the observations that hold significant differences in comparison to the transaction patterns.

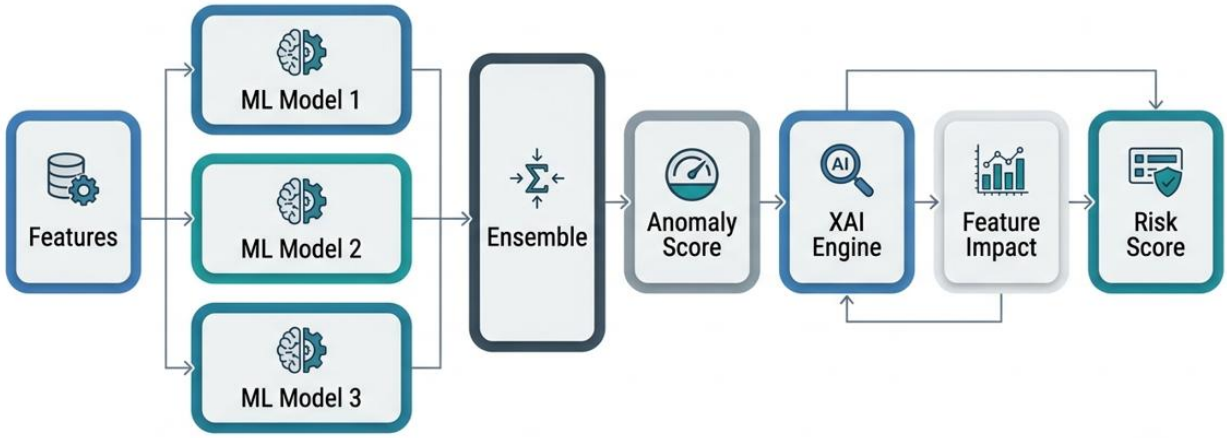


Figure 3- Hybrid Anomaly Detection and Explainable Risk Scoring Architecture

Various detection methods could be included to detect various types of irregularity. Examples here are isolation-based methods to identify observations that are structurally abnormal, clustering methods to identify abnormalities in the existing transaction groups and density-based approaches that intends to identify observations that are minimal in dense areas. Complementary models may be combined in order to obtain outputs through ensemble detection.

The model scores obtained are normalised to one anomaly score. Higher the score, the more incongruent are certain transactions with what has been learned about transactional behavior; it is not necessarily that there is fraud or accounting malpractice. This difference is crucial since even sound exceptional transactions might seem to be anomalous.

3.5 Explainable Risk Scoring Layer

One of the main advances of the framework is the incorporation of XAI and anomaly detection. The explainability module transforms the model outputs into evidence which may be interpreted and accessed by an auditor. The feature-attribution methods can be trusted to determine which characteristics provided the best contribution to the risk score in the journal entry of one person.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

Take the case of an entry (high value) on the measure of anomaly, because an extreme valueuser account relation, a very large amount, uploading, not according to the pattern the user uploads generally, or an outliers debitcredit balance. The framework does not just give a numeric score but it gives explanation profile which is the major driving factors.

Other trends in the population of transactions might also be established in case of international accountings. To illustrate, the framework can show that abnormal period-end posts or superior account matching is often the cause of high anomaly scores. Local explanations deal with single transactions and global explanations facilitate the planning and analysis of global audit and control.

3.6 Accounting Rule and Audit Validation Layer

Deterministic rules of accounting supplement machine-learned results. This mixed method allows the reliance to be on neither statistical models nor pre-specified controls. The rules include some that are duplicate-entry checks, unusual reversal pattern, and threshold violation, segregating of duty indicators, unsupported posting properties and period-end control conditions.

The validation layer checks machine-learning warnings with the outcome of accounting controls. In both mechanisms, it is possible to put an additional focus on transactions, although only those transactions mentioned by the machine learning can be modeled as potential patterns of abnormal behavior that should be discussed by a professional. This combination assists in covering more without compromising on a normal set of accounting-control practices.

The framework further segregates the transactions as risky, moderate, high and critical transactions child to organizational thresholds which are configurable. Risk categories would be in terms of priorities with the auditors rather than judgemental pronunciation on fraud.

3.7 Continuous Audit Monitoring and Auditor Interface

The last layer converts the outputs of the analytics to form a continuous monitoring environment. While new journal entries can be periodically or continuously processed as they become available. Each of the two transactions is allocated an anomaly score, an overview of the explanation, a control-validation result and an audit-priority.



Figure 4- Continuous Financial Audit Monitoring and Auditor Decision Loop

The amount of flagged transactions, risk distribution, new patterns of anomalies, top-ranking features, user-account relationship, and temporal concentrations can be regarded as data that can be visualized in an auditor dashboard. It is also possible to further define the single transactions to be able to see a profile of their explanation and accounting attributes. A document of audit trail of detection outcome, status of review, auditor remarks and resolutions given can also be supported by an interface.

The framework can be further improved, using a feedback mechanism. Auditor checked legitimate anomalies, common business and checked irregularities may be fed into a further model refinement. This builds a closed premise of analysis

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

wherein transaction information is used to offer risk indicators, human interpretation is used to authenticate, audit findings are used to evidence, and periodic system re-tuning is used.

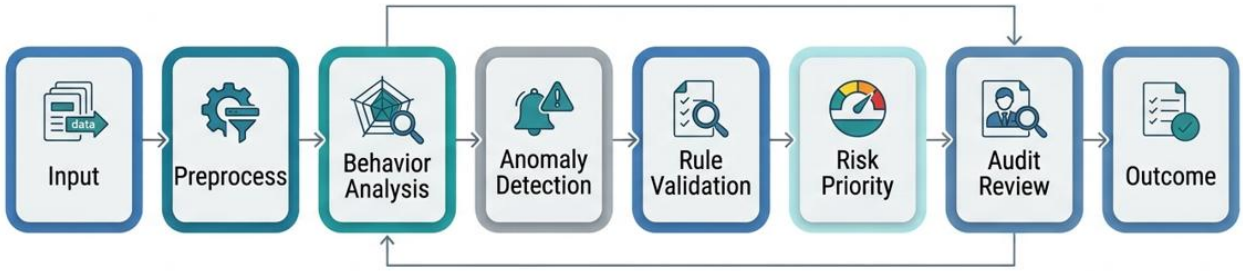


Figure 5- End-to-End Explainable Journal-Entry Risk Analysis Workflow

IV. AUDIT-CENTRIC FRAMEWORK VALIDATION AND EXPLAINABILITY ASSESSMENT

The suggested framework is evaluated in several aspects to reveal the effectiveness of the framework in detecting abnormal journal entries, producing interpretable risk data, and aiding ongoing financial audit. The rating entails the detection performance, risk-ranking capabilities, the quality of the explanations, the false-alerts and efficiency in the support of audit. Rather than playing anomaly detection as a one-shot classification fashion, the framework-based analysis considers the whole analytical process of the transaction processing in the face of the interpretation of the auditor.

4.1 Anomaly Detection Effectiveness

The first dimension is an indicator of the framework performance in isolating abnormal journal entries and accounting transactions as a normal accounting operations. In a case where the labelled transactioned data is accessible, one can use standard measures (precision, recall, F1-score, accuracy and area under the receiver operating characteristic curve (AUC-ROC)). Looking to better inform highly imbalanced financial data, precision-recall analysis and AUC-PR are as well helpful to supply more information to an anomalous transactions as a small proportion of the total population of journal-entries.

The analysis also finds out whether the hybrid detection architecture is able to capture various anomaly patterns. The behavioral and deterministic detection mechanism complementary significance is determined by comparing the machine-learning scores and accounting-rule alerts.

4.2 Risk-Scoring and Prioritization

The second dimension will check how well the journal entries with respect to their relative risk of anomaly can be ranked by the framework. Risk categories of transactions are aggregated based on normalized scores of anomaly and accounting-control indicators, which may be configured. The precision/K, Recall/K and even top-risk transaction coverage can be used to identify the effectiveness of the framework in mitigating the corresponding anomalies to the highest-priority group.

This measurement is especially critical to continuous auditing since auditors might lack adequate resources to investigate all the transactions at the same time. Effective prioritization facilitates the audit team targeting the initial audit review efforts on those transactions which contain a combination of increased behavioral signal and control-related signal.

4.3 Explainability Quality

The explainability layer is evaluated based on the extent of the generated explainability to mirror on the factors that result in anaberration score. Individual transaction explanations occur at a local level, and general explanations are carried out regarding general risk driving features of the whole population of transactions.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

Important properties include consistency, relevancy of features and interpretability and consistency of the explanation. The meaningful characteristics should be established in an explanation and could be the atypical amount of transactions, atypical account combinations and unexpected times of posting or atypical useraccount relationships. Having a sameness in the explanation of similar transactions can lead to increase in the confidence of the auditor on the analysis process.

4.4 False-Alert and Robustness Analysis

There is inherent legitimacy of exceptional transactions in financial systems. Therefore, an anomalous transaction should not necessarily be construed to mean a fraudulent transaction. The framework thus assesses its false-positive rate, false-negative rate, as well as its alert concentration with respect to various types of transactions.

The robustness of the models can similarly be analyzed in terms of accounting period, amount of transactions, user groups to which the model is used, types of accounts and end period activities. The effects of changes in sensitivity can be determined by performing a sensitivity analysis based on varying the values of the anomaly thresholds to determine the effects on the coverage and the number of transactions to check the alert.

4.5 Continuous Audit Support

The last evaluation dimension looks at the usefulness of the framework in the continuous audit activities. Relevant indicators that are listed include 1) alert processing time; 2) coverage of transaction; auditor review effort; 3) availability of explanations; and 4) completeness of audit-trail. The amount of transactions that are automatically analyzed and the proportion of the number of transactions not to be limited by reviews provided by a manual can be contrasted with the structure and the traditional periodic or rule-based screening.

Among the assessment goals is to determine whether the framework would transform the enormous masses of items of trade into manageable and understandable audit priorities. The collection of anomaly scores, summaries of explanations and accounting-control results and historical information on the behavior of the evidence leaves the auditors with a layer of pieces that they may develop upon in subsequent studies.

The framework assessment is comprehensive and the issues are that it is possible to identify anomalous journal entries or even better, it is possible to rank these detections, detailing, validating them and even continuously overseeing them. This measurement that is multidimensional creates a multidimensional ground on the issue of determining the practical utility of explainable AI in the context of on-top-of-the-financial-audit scenario at the transaction level.

V. EXPLAINABLE AUDIT INTELLIGENCE: DISCUSSION AND INSIGHTS

The proposed framework demonstrates how the explainable artificial intelligence could change the conventional financial auditing of periodic transactions verification to an environment of on-going risk-conscious monitoring. The combination of journal-entry anomaly detection and interpretable risk scoring, account controls, and auditor feedbacks is its primary contribution. The importance of this type of integration is that unusual determination of transactions is not sufficient evidence to arrive at an audit decision. The explanation layer is a contextual information which brings light into the nature of the characteristics that make a high score in the anomaly scale, and which can allow an auditor to explore the transactions based on comprehensible analytic findings.

Transaction-level is also rich in granularity as compared to measures that base their main interest of consideration on financial-statement-level measures. Such features as transaction value, post date, account relationship, user activity, history of reversal and trend analysis can be used jointly to detect any irregularities, which can be difficult to detect about individual accounting policies. In the meantime, suspicious actions cannot be considered as always indicative of fraud because legitimate business cases might also leave statistically uncharacteristic journal metre. Human review thus is an obligatory part of the stipulated architecture.

Another useful aspect is the hybridism of machine learning, as it was employed concomitant to accounting rules. The machine learning will be capable of identifying the behavioral patterns that have not been identified by other methods, as opposed to deterministic controls, which can be exploited in seizing the familiar accounting circumstances. Their sets of applications may be potentially beneficial when it comes to improving the coverage of transactions since such a way will no longer depend on either of the discussed strategies. Explainability can further improve this mixture since it allows the auditors to understand why a machine-learning system has determined a high risk to a particular entry.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

The framework also encourages the continuous monitoring in that new transactions generated can be allowed flow through the analytical pipeline without the need to be audited periodically. The prioritization of risks that are analyzed can help an auditor to concentrate in their attention depending on the level of transactions that will help them in revising the model on periodic basis, feedback analysis of audited cases can help in updating the model. Nonetheless, in the practical application one should focus on the choice of thresholds, data-quality, data protection, monitoring of the model and governance processes. The quality of the generated explanations should also be discovered periodically to ensure that the generated explanations stand and have some meaning.

Overall, the framework causes XAI to be an audit-support feature and not an independent audit decision-maker, which is a synthesis of the scalable analysis of transactions and the revelation of this analysis by evidence and professional judgment of the auditor.

VI. CONCLUSION

This paper outlined an explainable artificial intelligence system of journal-entry anomaly detection and continuous auditing of finances. The proposed new architecture is an amalgamation of journal-entry acquisition, data preparation, behavioral feature engineering, machine-learning-based anomaly-detection, explainable risk-scoring, accounting-rule validation, continuous-monitoring, and auditor feedback, into a single architecture. A significant disadvantage of such a traditional financial audit is that large volumes of transactions, and an increasingly complex accounting process, can make all manual reviews excruciating.

The framework subdivides the different dimensions about journal-entry behavior, including the sizes of transaction, time, relatedness of accounts, user activity, documental features and historical patterns of transactions. Machine learning models capture a given change in the behavior according to the current behavior rules and the risk-scoring layer translates changes into high-priority audit signals. The addition of XAI gives understandable insights into the traits that attributed to individual scores in anomalies. Consequently, the auditors are also able to examine the transactions which have been identified as unusual as well as the reasons which have caused them to be more risky.

The collaboration between the machine learning and accounting controls strengthens the framework again, namely, attaining a better data-driven method of finding anomalies and preventing them by having the reliable validation of rules. Periodic regressing of the newly-created journal entries will assist increase in systematic examination of the transaction instead of real-time and perilous audit. It is interesting to note that the anomaly scores are treated as such whereby they are treated as a professional judgment that awaits a conclusion that can be breaching of fraud or misuse of accounting.

The framework also gives a feedback control which gives opportunity to make observations by auditors and the outcome of resolving transactions can be observed to adjust the model in future. The future frameworks can be evaluated with numerous possible anomaly-detection algorithms, ensemble-based algorithm, explanation-based algorithm, and setting of thresholds as well as real-life ERP data. Additional research can also be conducted to investigate the consistency of the explanation, external organization generalization, capabilities of computation scaling and adoption to the new continuous-audit systems.

Overall, the proposed architecture presents us with a roadmap of systematic integration of machine learning, explainability, accounting controls, and active monitoring to enable transparent analysis of risks through journal entries. The framework offers the foundation of smart, responsible and ever backed financial auditing through maintaining human supervision and providing expandable and understandable informative proofs.

REFERENCES

[1] M. A. K. Achakzai *et al.*, “Using machine learning meta-classifiers to detect financial frauds,” *Finance Research Letters*, 2022.
[2] Y. Bao *et al.*, “Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach,” *Journal of Accounting Research*, 2020.
[3] R. R. Juvvadi, “Machine learning for anomaly detection in the financial close: A journal entry risk-scoring framework for SAP S/4HANA,” *International Journal of Communication Networks and Information Security*, vol. 14, no. 3, pp. 1684–1695, 2022.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 4, July- August 2024|

DOI:10.15680/IRJIE.2024.0804003

[4] J. Bertomeu *et al.*, "Using machine learning to detect misstatements," *Review of Accounting Studies*, 2021.
[5] Y. Wei *et al.*, "Detecting fraud in Chinese listed company balance sheets," *Pacific-Basin Finance Journal*, 2017.
[6] A. Abbasi *et al.*, "MetaFraud: A meta-learning framework for detecting financial fraud," *MIS Quarterly*, 2012.
[7] P. Giudici *et al.*, "Shapley-Lorenz eXplainable artificial intelligence," *Expert Systems with Applications*, 2021.
[8] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE Access*, 2018.
[9] T. Miller, "Explanation in artificial intelligence: Insights from the social sciences," *Artificial Intelligence*, 2019.
[10] K. Bauer *et al.*, "Expl(AI)ned: The impact of explainable artificial intelligence on users' information processing," *Information Systems Research*, 2023.
[11] N. Bussmann *et al.*, "Explainable machine learning in credit risk management," *Computational Economics*, 2021.
[12] U. Bhatt *et al.*, "Explainable machine learning in deployment," 2020.
[13] M. P. Sesmero *et al.*, "Impact of the learners diversity and combination method on the generation of heterogeneous classifier ensembles," *Applied Soft Computing*, 2021.
[14] G. Babaei *et al.*, "Explainable artificial intelligence for crypto asset allocation," *Finance Research Letters*, 2022.
[15] V. Genre *et al.*, "Combining expert forecasts: Can anything beat the simple average?" *International Journal of Forecasting*, 2013.