International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. **11** Special Issue **03** | **2026**

Anomatrix: Advanced Scrutiny in Financial Ledgers Using Hybrid Deep Learning and Ensemble-Based Anomaly Detection

Kedar Pravin Damale[1],Anand Haresh Karmarkar[2], Ashish Chandrashekhar Ghadigaonkar[3], Mandar Joshi[4]
[1,2,3] *B.E. Student, Department of Information Technology, Finolex Academy of Management and Technology, Maharashtra, India*
[4]*Assistant Professor, Department of Information Technology, Finolex Academy of Management and Technology, Maharashtra, India*

DOI: 10.5281/zenodo.20630911

ABSTRACT

This study has been undertaken to develop Anomatrix, an intelligent anomaly detection system for financial and accounting ledgers using a hybrid approach of deep learning and machine learning ensembles. The proposed system aims to detect both global anomalies (rare individual attributes) and local anomalies (rare combinations of attributes) in large-scale journal entries and general ledger data. To achieve this, the framework integrates a deep autoencoder for feature compression and representation learning, an LSTM network for temporal pattern modeling, and a Random Forest classifier for robust anomaly classification. Additionally, the system incorporates attribute probability–adjusted anomaly scoring to improve the detection of subtle irregularities and applies SMOTE/ADASYN oversampling techniques to handle highly imbalanced financial datasets. The outcome of this research supports automated audit assistance by providing accurate anomaly flagging and interpretable outputs for accountants and auditors, reducing manual workload and improving fraud detection efficiency in real-world financial environments.

Index Terms - Anomaly Detection, Financial Ledgers, Deep Autoencoder, LSTM, Random Forest, Ensemble Learning, Audit Automation, Fraud Detection, Imbalanced Data, SMOTE, ADASYN, Machine Learning, Deep Learning.

1. INTRODUCTION

For this study, secondary financial accounting data has been considered to design and validate an automated anomaly detection framework for financial ledgers. The proposed work focuses on identifying abnormal and suspicious patterns from large-scale datasets such as journal entries and general ledger transactions, which are widely used in banking, corporate finance, and enterprise accounting systems.

With the rapid growth of digital transactions, organizations generate massive volumes of financial records on a daily basis. Conventional auditing methods that rely on manual checking and fixed rule-based verification are time-consuming, prone to human error, and often fail to detect newly emerging fraud patterns. As a result, there is a strong requirement for an intelligent system that can analyze complex financial datasets and highlight unusual entries in a faster and more reliable manner.

Anomalies in financial ledgers may occur due to incorrect data entry, misclassification of accounts, unusual transaction behavior, or intentional fraudulent manipulation. These anomalies affect the credibility of financial reporting and can lead to serious financial and compliance risks. Therefore, this research proposes Anomatrix, a hybrid anomaly detection system that leverages both deep learning and machine learning ensemble techniques to improve detection accuracy on highly imbalanced and real-world financial data.

The analytical framework of the proposed system integrates a deep autoencoder for feature representation and reconstruction-based anomaly scoring, an LSTM model for capturing sequential and temporal transaction patterns, and a Random Forest classifier for robust anomaly classification. In addition, oversampling methods such as SMOTE and ADASYN are applied to address class imbalance and enhance the learning capability for rare anomaly instances. The overall aim is to support auditors and accountants by providing scalable anomaly detection with interpretable outputs, reducing manual workload and improving fraud screening efficiency in financial environments.

2. LITERATURE REVIEW

Detection of Anomalies in Large-Scale Accounting Data using Deep Autoencoder Networks (Schreyer et al., 2020) This work presents the use of deep autoencoder networks to detect anomalies in large-scale accounting

and journal entry datasets. The model learns compressed representations of financial records and identifies suspicious entries using reconstruction error. Experimental results show strong performance in capturing complex patterns in high-dimensional ledger data. However, the approach mainly depends on a single deep learning model and provides limited support for temporal behavior analysis and ensemble-based decision making. Anomatrix extends this concept by combining autoencoder-based feature learning with additional temporal and ensemble models for improved accuracy.

Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks (Benchaji et al., 2021)

This research proposes an LSTM-based fraud detection model to identify suspicious credit card transactions by learning sequential and time-dependent behavior. The results demonstrate that LSTM networks effectively capture transaction flow patterns and improve fraud prediction compared to traditional classifiers. Although effective, the model is focused on card transaction sequences and does not address ledger-specific anomaly scoring or global/local anomaly separation. Anomatrix adapts LSTM-based sequence learning for ledger transactions and integrates it with anomaly scoring to detect both rare and evolving financial anomalies.

Detecting Anomalies in Financial Data Using Machine Learning Algorithms (Bakumenko & Elragal, 2022**)**

This study evaluates multiple machine learning algorithms for anomaly detection in financial datasets and highlights the effectiveness of ensemble models in improving detection stability. The work shows that Random Forest and other classifiers can perform well in handling noisy financial data. However, the system lacks deep feature extraction capability and struggles with highly imbalanced anomaly distributions. Anomatrix improves this by using deep autoencoders for representation learning and applying oversampling techniques like SMOTE/ADASYN to handle imbalance before classification.

An Intelligent Fraud Detection Model based on Deep Learning Ensembles (Zioviris et al., 2022)

This paper introduces an intelligent fraud detection framework using deep learning ensembles to enhance accuracy and reduce false positives. The ensemble strategy improves robustness compared to single-model detection systems and supports better generalization on complex fraud patterns. However, the work does not specifically emphasize interpretable anomaly scoring for audit support. Anomatrix builds on this by combining deep learning ensembles with probability-adjusted anomaly scoring and interpretable outputs to assist auditors in decision-making and investigation.

Table: Comparative Analysis

Feature	Schreyer et al. (2020) Deep Autoencoder	Benchaji et al. (2021) LSTM Fraud Detection	Bakumenko & Elragal (2022) ML Algorithms	Zioviris et al. (2022) Deep Learning Ensembles	Proposed System (Anomatrix)
Domain	Accounting / Journal Entries	CreditCard Transactions	Financial Datasets (general)	Fraud Detection (general)	Financial Ledgers / Journal Entries / Audit
Approach	Deep Autoencoder (reconstruction error)	LSTM sequential learning	ML classifiers (RF, etc.)	Ensemble Deep Learning	Hybrid: Autoencoder + LSTM + Random Forest
Anomaly type focus	Mostly global/point anomalies	Temporal/sequence fraud patterns	Pattern-based anomalies	Complex fraud patterns	Global + Local anomalies
Temporal Modeling	Not included	Yes	Limited	Partial	Yes (LSTM for sequences)
Feature Learning	Strong (latent representation)	Moderate	Low (manual features)	Strong	Strong (Autoencoder latent space)
Handling Imbalanced Data	Limited	Limited	Limited	Partial	Yes (SMOTE / ADASYN)
Interpretability for Auditors	Low–Moderate	Low	Moderate	Moderate	High (score + classification support)
Scalability	High	Moderate	High	High	High (scalable hybrid pipeline)
Output Type	Anomaly score	Fraud prediction	Classification	Fraud prediction	Anomaly score + fraud Decision + audit support

3. PROPOSED SYSTEM

Problem Statement

Even now, plenty of companies stick to old-school ways when checking their accounting logs - hand reviews paired with rigid rules. Such methods fail to grow alongside rising data loads, stumble when scams shift shape, yet somehow stay in place. Without smart scoring for odd behavior, red flags often slip through. Audits drag on, numbers waver between versions, trust in reports fades. Clarity takes a hit every time.

Nowadays financial setups produce huge amounts of complex data, unbalanced and dense, where odd cases pop up infrequently yet matter deeply. Standard approaches typically miss broad outliers - unusual single traits - as well as narrow ones - strange mixes of features - slowing down auditors and number keepers hunting risky entries. For this reason, a smart tool is necessary: one that runs on its own, handles growth smoothly, shows clear reasoning, lifts precision, cuts hand-driven tasks, and backs live checks when reviewing money records.

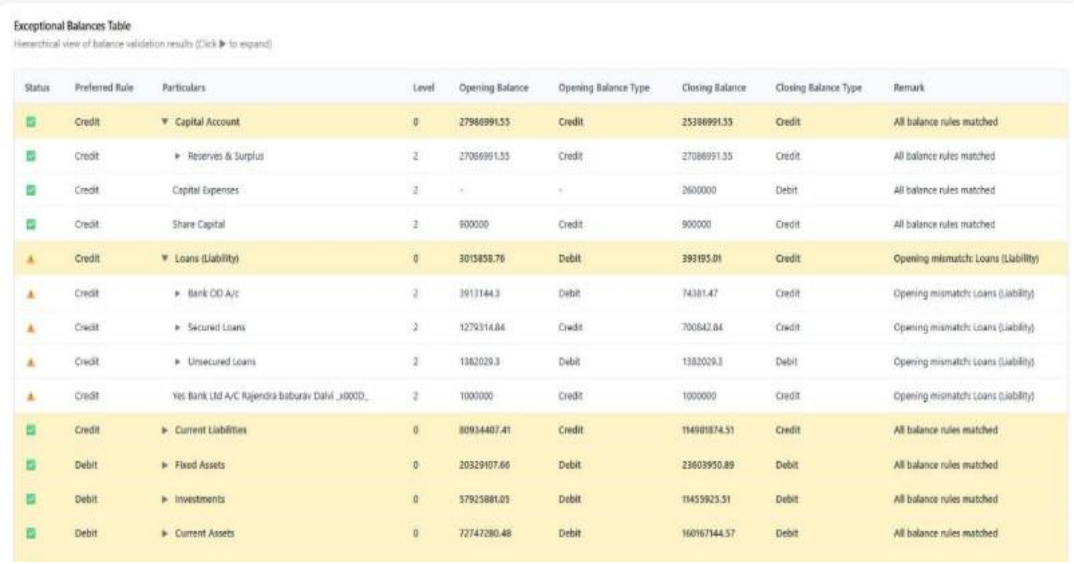
Proposed Solution

Module 1: Trial Balance Golden Rule Check

Here comes a check on every number entered into the books. When files arrive, they get scanned for how debits and credits line up. Matching pairs matter most because imbalance raises red flags right away. Through step by step math, left side sums meet right side tallies. Only when these amounts agree does the record pass inspection. Accuracy lives in that equality - nothing more, nothing less.

Sometimes, the system spots odd entries - like when one account shows both a debit and a credit at once - and flags them as possible errors. When checking amounts, it makes sure numbers aren't negative and fit how each type of account usually works. Take assets: they tend to sit on the debit side under normal conditions. Liabilities and revenue? Those belong more naturally on the credit side most times.

When something breaks the rules, the transaction gets marked as suspicious. Right away, this check points auditors toward mistakes in the books while keeping numbers aligned with accepted accounting methods.


Exceptional Balances Table

Hierarchical view of balance validation results (Click ▶ to expand)

Status	Preferred Rule	Particulars	Level	Opening Balance	Opening Balance Type	Closing Balance	Closing Balance Type	Remark
✓	Credit	▼ Capital Account	0	27986991.55	Credit	25386991.55	Credit	All balance rules matched
✓	Credit	▶ Reserves & Surplus	2	27086991.55	Credit	27086991.55	Credit	All balance rules matched
✓	Credit	Capital Expenses	2	-	-	2600000	Debit	All balance rules matched
✓	Credit	Share Capital	2	900000	Credit	900000	Credit	All balance rules matched
⚠	Credit	▼ Loans (Liability)	0	3015858.76	Debit	393195.01	Credit	Opening mismatch: Loans (Liability)
⚠	Credit	▶ Bank OD A/c	2	3913144.3	Debit	74381.47	Credit	Opening mismatch: Loans (Liability)
⚠	Credit	▶ Secured Loans	2	1279314.84	Credit	700842.84	Credit	Opening mismatch: Loans (Liability)
⚠	Credit	▶ Unsecured Loans	2	1382029.3	Debit	1382029.3	Debit	Opening mismatch: Loans (Liability)
⚠	Credit	Yes Bank Ltd A/C Rajendra baburav Dalvi ...i0003...	2	1000000	Credit	1000000	Credit	Opening mismatch: Loans (Liability)
✓	Credit	▶ Current Liabilities	0	80934407.41	Credit	114981874.51	Credit	All balance rules matched
✓	Debit	▶ Fixed Assets	0	20329107.66	Debit	23603950.89	Debit	All balance rules matched
✓	Debit	▶ Investments	0	5792588.03	Debit	11455925.51	Debit	All balance rules matched
✓	Debit	▶ Current Assets	0	72747280.48	Debit	160167144.57	Debit	All balance rules matched

Fig -1.1: Trial Balance Analysis Result Screen

Module 2: Opening and Closing Balance Check

This module keeps financial records steady from one period to the next. Because accuracy matters, it checks if the starting amount links properly with debits, credits, and the ending total. What counts here is a clear logic connecting each piece. Without that link, numbers might seem right but fail deeper review. So instead of just adding up entries, it examines how they relate over time.

The system applies the accounting equation:

$$\text{Opening Balance} + \text{Debit} - \text{Credit} = \text{Closing Balance}$$

A gap shows up when the computed ending amount misses alignment with the recorded one - the software tags that instantly. Missing starting figures? Spotted too. Sudden jumps or drops in value - say, over half a grand in growth - get highlighted without delay.

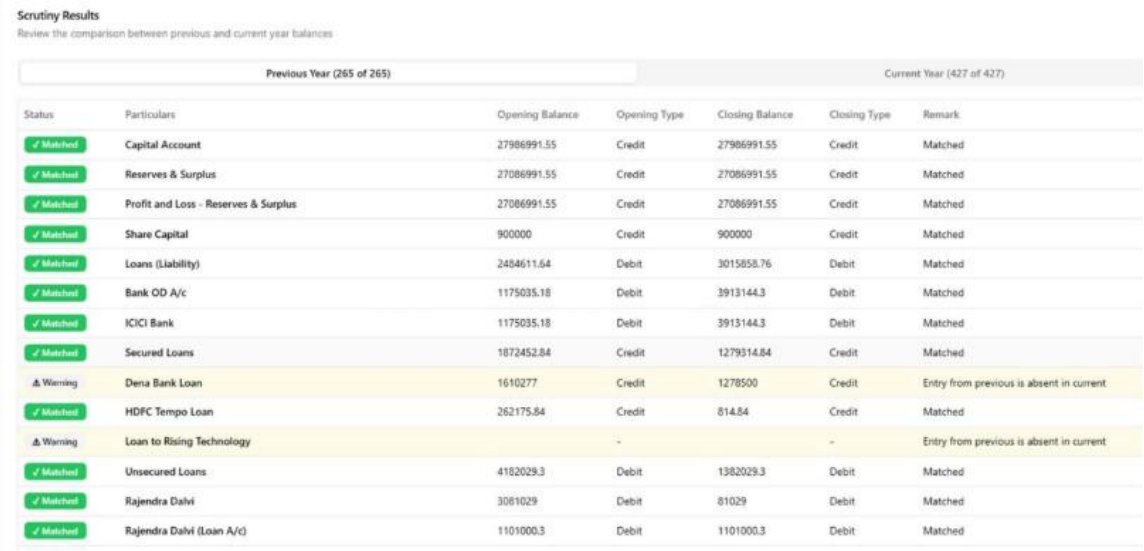
Unexpectedly spotting negative amounts in asset records, the module flags potential mistakes or odd activity. When such cases pop up, automatic checks kick in - keeping numbers aligned across reports. This way, anyone reviewing past entries can spot mismatches without delay.

Module 3: GST Reconciliation (Purchase and Sales)

One way it works is by matching up what was bought and sold against the GST reports, just to stay within tax laws. Checking each GSTIN happens before anything else, making sure every number fits official formats. Invoice info comes under review next, where dates, amounts, and parties involved get cross-checked carefully. Tax figures go through a second look, comparing how much should be paid versus what actually shows on record. The whole point becomes clear only after everything lines up without mismatches or gaps. What ends up mattering most is whether all entries reflect real transactions under current regulations. Accuracy here doesn't come from guesses but from step-by-step verification of every detail tied to taxes.

With each entry, it confirms the invoice total matches taxable value along with GST parts. Valid GST percentages - like 0%, 5%, 12%, 18%, or 28% - are cross-checked automatically. Instead of assumptions, clear logic prevents mixing IGST with paired CGST and SGST entries.

Each transaction gets sorted by type - like company trades, customer sales, or overseas deals - not through manual work but system logic. When a sale to an individual crosses a set amount, it draws attention for closer review. Instead of skipping oddities, the tool spots them: wrong billing details, tax numbers off track, gaps that might break rules. With routine checks handled digitally, businesses see problems earlier, often before they grow. What slips past human eyes tends to show up here, quietly logged for follow-up.

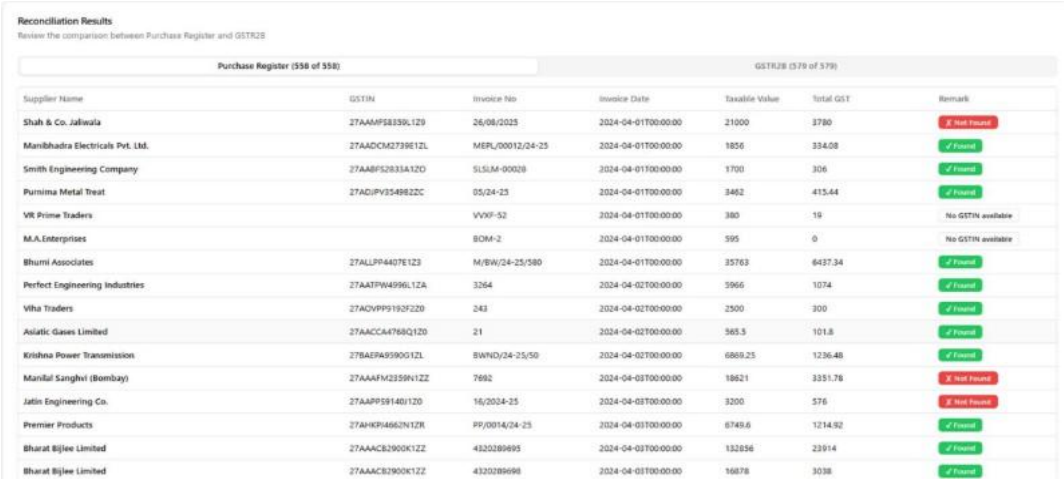


Scrutiny Results

Review the comparison between previous and current year balances

	Previous Year (265 of 265)			Current Year (427 of 427)		
Status	Particulars	Opening Balance	Opening Type	Closing Balance	Closing Type	Remark
✓ Matched	Capital Account	27986991.55	Credit	27986991.55	Credit	Matched
✓ Matched	Reserves & Surplus	27086991.55	Credit	27086991.55	Credit	Matched
✓ Matched	Profit and Loss - Reserves & Surplus	27086991.55	Credit	27086991.55	Credit	Matched
✓ Matched	Share Capital	900000	Credit	900000	Credit	Matched
✓ Matched	Loans (Liability)	2484611.64	Debit	3015858.76	Debit	Matched
✓ Matched	Bank OD A/c	1175035.18	Debit	3913144.3	Debit	Matched
✓ Matched	ICICI Bank	1175035.18	Debit	3913144.3	Debit	Matched
✓ Matched	Secured Loans	1872452.84	Credit	1279314.84	Credit	Matched
⚠ Warning	Dena Bank Loan	1610277	Credit	1278500	Credit	Entry from previous is absent in current
✓ Matched	HDFC Tempo Loan	262175.84	Credit	814.84	Credit	Matched
⚠ Warning	Loan to Rising Technology		-		-	Entry from previous is absent in current
✓ Matched	Unsecured Loans	4182029.3	Debit	1382029.3	Debit	Matched
✓ Matched	Rajendra Dalvi	3081029	Debit	81029	Debit	Matched
✓ Matched	Rajendra Dalvi (Loan A/c)	1101000.3	Debit	1101000.3	Debit	Matched

Fig -1.2: Opening and Closing Balance Validation Screen



Reconciliation Results

Review the comparison between Purchase Register and GSTR2B

	Purchase Register (558 of 558)				GSTR2B (579 of 579)	
Supplier Name	GSTIN	Invoice No	Invoice Date	Taxable Value	Total GST	Remark
Shah & Co. Jaliwala	27AAMFS8139L1Z9	26/08/2025	2024-04-01T00:00:00	21000	3780	✗ Not Found
Manibhadra Electricals Pvt. Ltd.	27AADCM2739E1ZL	MEPL/00012/24-25	2024-04-01T00:00:00	1856	334.08	✓ Found
Smith Engineering Company	27AABFS2833A1ZO	SLSLM-00028	2024-04-01T00:00:00	1700	306	✓ Found
Purnima Metal Treat	27ADJPV3549B2ZC	05/24-25	2024-04-01T00:00:00	3462	415.44	✓ Found
VR Prime Traders		VVKF-52	2024-04-01T00:00:00	380	19	No GSTIN available
M.A.Enterprises		BOM-2	2024-04-01T00:00:00	595	0	No GSTIN available
Bhumi Associates	27ALLPP4407E1Z3	M/BW/24-25/580	2024-04-01T00:00:00	35763	6437.34	✓ Found
Perfect Engineering Industries	27AATPW4996L1ZA	3264	2024-04-02T00:00:00	5966	1074	✓ Found
Viha Traders	27AOVPP9192F2Z0	243	2024-04-02T00:00:00	2500	300	✓ Found
Asiatic Gases Limited	27AACCA4768Q1Z0	21	2024-04-02T00:00:00	565.5	101.8	✓ Found
Krishna Power Transmission	27BAEPA9590G1ZL	BWND/24-25/50	2024-04-02T00:00:00	6869.25	1236.48	✓ Found
Manilal Sanghvi (Bombay)	27AAAFM2259N1ZZ	7692	2024-04-03T00:00:00	18621	3351.78	✗ Not Found
Jatin Engineering Co.	27AAPFS9140J1Z0	16/2024-25	2024-04-03T00:00:00	3200	576	✗ Not Found
Premier Products	27AHKPI4662N1ZR	PP/0014/24-25	2024-04-03T00:00:00	6749.6	1214.92	✓ Found
Bharat Bijlee Limited	27AAACB2900K1ZZ	4320289895	2024-04-03T00:00:00	132856	23914	✓ Found
Bharat Bijlee Limited	27AAACB2900K1ZZ	4320289698	2024-04-03T00:00:00	16878	3038	✓ Found

Fig -1.3: Purchase Register Reconciliation Output

Module 4: User Management, Audit and Reporting

Who gets in, who sees what - handled here. Permissions shift by job role, locking down tools to those approved. Every move stays visible, logged for review later. Reports pull straight from activity trails. Access lives on rules, not guesses. System clarity builds step by step, no shortcuts.

Profile progress gets measured through various details filled out, adding up to a total score shown as percent. Once that number goes past eighty roughly, it counts as done. Admins handle worker IDs carefully, making sure each one stays different. Skipping duplicates keeps records clean, managed step by step without overlap.

Every move a person makes inside the system gets saved with exact time stamps, locked in unchangeable records. Happens every time someone adds a file, spots an irregularity, tries logging in, or adjusts settings. Security checks and rule tracking get easier because each event is sorted by how serious it is. Logs stay fixed after entry, never altered, forming a steady trail of what occurred when.

Dashboards take shape when audit logs meet alerts, forming clear summaries you can save or share. Reviewing odd transactions becomes easier once admins flip through these organized snapshots of what happened. Compliance stays on track because each report lays out activity in a way that makes sense later. Figuring out who did what gets simpler when everything shows up sorted by time and type. Files ready for export keep teams aligned without extra steps or guesswork. Seeing patterns in behavior happens naturally after enough details line up just right. Regulators ask fewer questions if records appear consistent and built with care. Moments of confusion fade when every entry traces back to a known source. System checks continue quietly while reports pull together the pieces behind the scenes. Alerts find their place beside log entries, turning noise into something worth reading.

Module 5: PDF Document Processing and Text Extraction

Handling uploaded documents falls to this component, pulling out written details from PDFs so they can move on to later steps. Invoices, reports, or account summaries often arrive as PDFs inside audit and money tracking setups. So reading those messy PDF pages needs to happen without manual help, turning loose layouts

into clean lines of text ready for inspection. Without such a tool, moving paper-like files into digital understanding would slow everything down too much.

Built on Flask, this tool creates a lean backend that manages document transfers and service calls. A person may add single or several PDFs by way of an online form. After submission, each file gets checked then saved safely into a preset folder on the machine. To block harmful inputs, names of incoming files are cleaned with trusted techniques before storage.

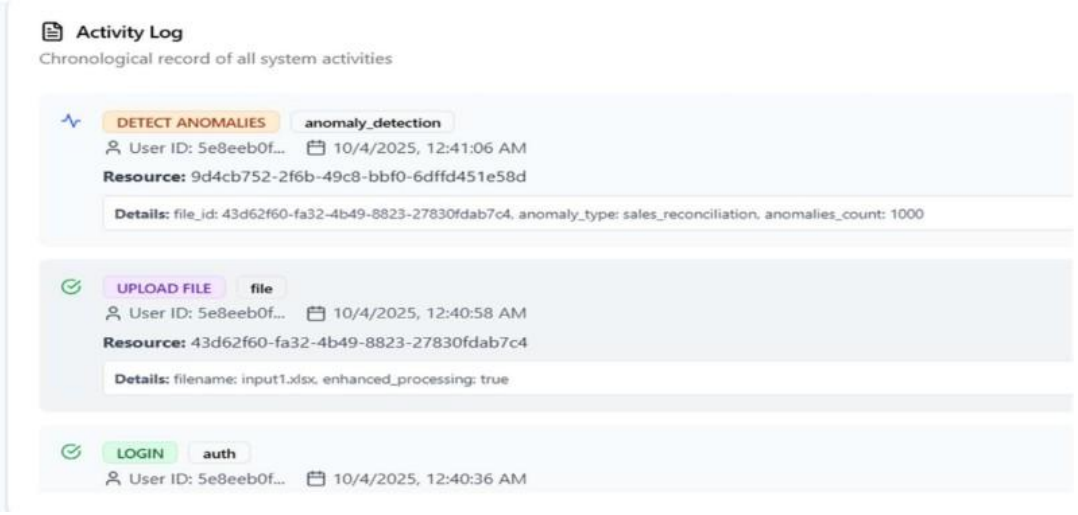


Fig -1.4: User Management and Audit Logs Screen

Page after page, the tool pulls out words using PyPDF when someone uploads a PDF file. As it moves forward, every piece of readable text gets pulled from each sheet. What comes out joins together into one clean block of writing. Each chunk carries the original filename so you know where it came from. Marking everything keeps things clear and linked back correctly.

When something goes wrong, the system knows how to respond. Missing files trigger clear warnings instead of failing silently. Wrong formats get flagged right away through built-in checks. Problems during processing lead to specific feedback messages. After everything runs smoothly, the collected text flows back. It arrives structured as JSON data. That format connects easily with tools that analyze records. Auditing systems pick it up without extra steps. Even anomaly detectors use it directly when scanning for irregularities.

This tool turns PDFs into readable text so machines can process them. Because of that, it helps analyze documents without manual work. It fits into the bigger system aiming to make audits more precise. With clearer data, spotting odd patterns in finances becomes easier. Efficiency rises when repetitive steps run on their own. Accuracy improves as human errors drop during review tasks.

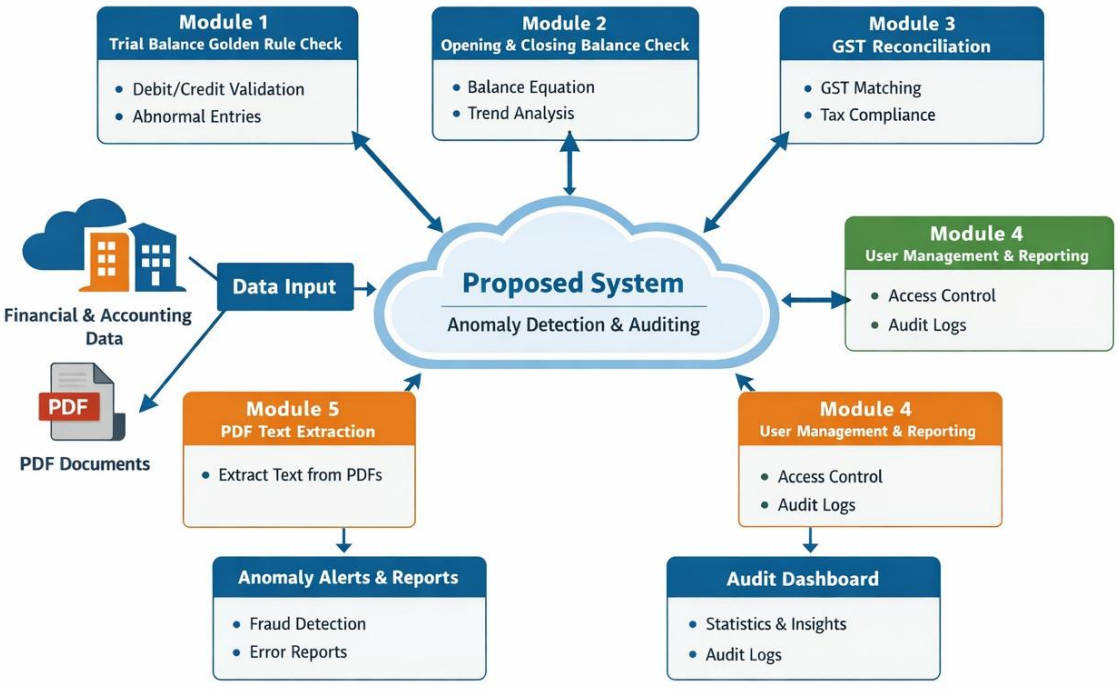


Fig -2: Proposed System

4. SYSTEM ARCHITECTURE

Built to grow as needed, the **Anomatrix** setup works like separate pieces that fit together, spotting odd patterns in money records. Instead of one rigid structure, it combines an up-to-date website front end alongside protected server operations, smart learning tools, plus organized data saving spots - making audits happen without constant manual checks.

1. **User Interface Layer**

A space where auditors, staff, and admins engage directly with the system opens through a live web portal. Built on React powered by Vite and styled with Tailwind CSS, the display loads swiftly while adapting smoothly to different screen sizes. Interaction happens here - ledgers get uploaded, findings from checks appear instantly, reports become visible, gaps in finances show up as they happen. Smooth navigation supports constant oversight without delays or cluttered visuals getting in the way.

Depending on user roles, dashboard views change automatically. Admins see tools suited to management tasks while staff get only what they need. Access levels decide who sees what without mixing features meant for others.

2. **API Gateway and Authentication Layer**

Out there, the setup runs on **RESTful APIs** so the front end talks smoothly with back end parts. Instead of handling requests directly, an API gateway steps in - checking who logs in, managing files sent up, pulling needed info, plus setting limits on what users can reach. **To keep things locked down, it uses JSON Web Tokens; these confirm who someone really is while keeping their session safe behind the scenes**.

Not just any user gets into every part of the system - access depends on assigned roles. Because of this setup, people see only what they're allowed to, nothing more. Security goes up when entry points are locked behind job-specific permissions. Sensitive financial details stay protected under these limits. Each role acts like a key, opening certain doors while leaving others sealed.

3. **Backend Processing Layer**

Running behind everything, the backend uses **FastAPI** to manage heavy data loads quickly through async operations. At its heart, this part drives the whole system's workload.

It manages multiple services such as:

Data preprocessing and validation File conversion and processing

Execution of anomaly detection algorithms User management and **audit** logging

Communication with databases and storage systems

Each part of the backend works on its own, yet fits into the whole system through a flexible structure.

4. **Data Processing and Machine Learning Layer**

Inside the system, raw numbers get shaped into clearer forms before anyone studies them. Files added by users turn into organized layouts that machines can work through. **Tools like Pandas and NumPy handle steps that clean and arrange the information ahead of deeper review**.

Out of the analyzed data, strange trends begin to surface through pattern detection. Because algorithms sort through numbers, odd shifts in finance show up more clearly. Unusual activity often stands out when systems compare past behavior with current results. When balances do not line up, alerts rise without delay. Suspicious sequences trigger review thanks to trained models noticing small deviations first. Fraud signs emerge quietly - then grow hard to ignore.

By learning patterns, these systems handle audits faster, cutting down hands-on work. Accuracy gets a boost too, since spotting oddities becomes more reliable through their analysis.

5. **Storage Layer**

Storage happens through blobs alongside MongoDB, handling varied data without slowing down.

Efficient management comes from pairing these two methods instead of relying on just one.

- Uploaded ledgers and spreadsheets like .xlsx go into **Blob Storage** for safekeeping. Files stay protected once they land there. Security kicks in the moment data arrives. Spreadsheets do not sit exposed. Protection wraps around each document right away. Safety stays active as long as files remain. Data rests secure through every step after upload.
- Apart from traditional setups, **MongoDB** handles data like user profiles, cleaned-up transaction entries, flagged irregularities, along with tracking history. Stored differently, it manages these using flexible formats instead of fixed rows. Information flows into it naturally, fitting varied shapes without rigid schemes. Each piece rests inside without needing predefined columns. User facts sit alongside system checks, linked through dynamic grouping. Processed numbers appear next to alerts raised during scans. Logs follow every move, saved just in time. Structure bends here, adapting per need rather than rule.

A mix of storage types helps the system manage organized data alongside messy, freeform information without slowing down. Still, speed stays strong even as demands shift.

6. Control and Monitoring Layer

Administrators find their workspace here, inside the control layer, where dashboards guide oversight. Monitoring tools show what users are doing across the system. Oversight unfolds through activity logs instead of guesswork. Anomaly alerts appear clearly, helping spot irregularities without delay. Management becomes visible, moment by moment, line by line.

Every move users make gets captured alongside system activities, time-stamped without exception. Because of this tracking, who did what and when stays clear. Oversight becomes possible, rules are followed, responsibility is traceable. Moments after an event, it's already stored for review. What happens inside doesn't stay hidden - timing included.

7. Output and Reporting Layer

A screen shows what the system found, using charts and summaries people can look at. When something seems off with a transaction, a notice pops up automatically. Odd numbers in money records get marked clearly so they stand out. Files that contain full details are ready to save whenever someone needs them for checking later.

Possibility of fraud, mistakes in numbers, or rule breaches shows up fast through these results. Professionals checking finances get alerts without delay when something seems off.

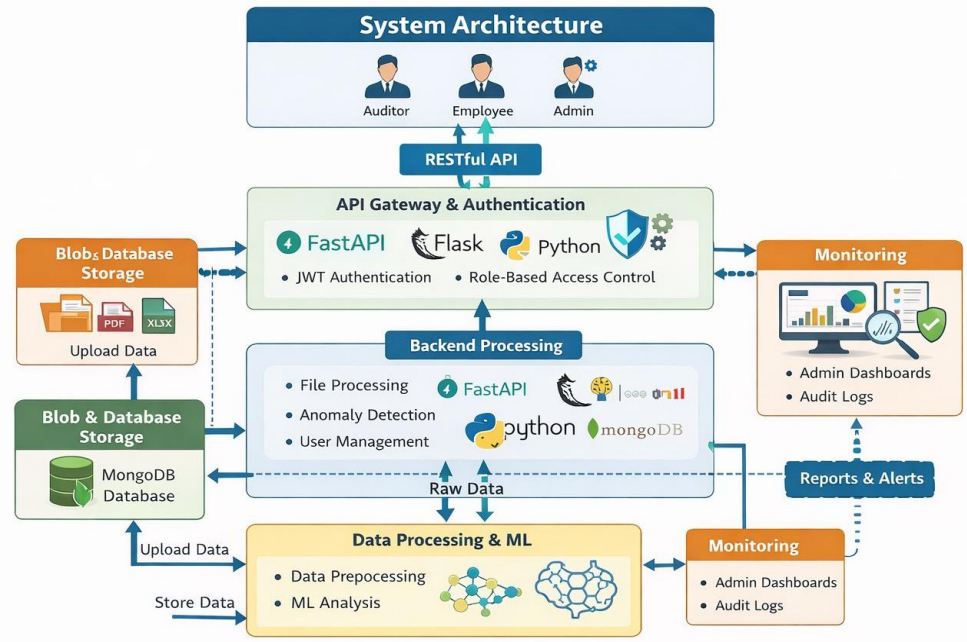


Fig -3: System Architecture

5. CHALLENGES

Even with big steps forward in using artificial intelligence to catch fraud and spot oddities, problems still get in the way when applying these tools in actual finance and bookkeeping settings. A key issue found in past studies comes down to how tangled and varied financial record data can be. Entries in accounting logs carry many traits at once - some numbers, some labels - and reflect unique ways each company operates, so one model often fails to work well across separate systems or industries.

One big problem? How uncommon strange cases are - plus how uneven the groups can be. Most money data holds just a few odd or wrong actions among many regular ones. That tilt pushes learning systems to favor common patterns, so they miss spotting outliers more often than not. Oddities might show up as rare single traits or unusual mixes of features, both tricky in their own way. Spotting them needs smarter scoring methods that adapt to these hidden shifts.

Hard to understand, hard to check - that's what happens when models hide their logic. Some tools get good results yet give no clear path through their thinking. People who review finances need reasons behind odd findings, scores they can follow, proof they can track down; most current methods fall short here.

When it comes to spotting odd patterns in data, handling growth becomes tricky. Even if a system works fine in tests, real-world ledgers keep changing fast - more records pile up by the minute. Running checks on live streams means everything must respond quickly, without lag. Getting data ready ahead of time helps, yet pulling out useful details still takes effort. How models are set up later affects how smoothly they run over time. Without smart design early on, using them widely just doesn't hold together.

Over time, keeping detection steady gets tough when fraud shifts shape. As tricks evolve, old models might miss fresh warning signs because they can't keep up. So relying only on fixed rules won't work well anymore since surprises happen often now. A mix of methods helps stay sharp - adapting faster while cutting down wrong

alarms across banking networks.

6. FUTURE DIRECTION

Not far off, work on smarter finance tracking might emphasize how well systems adjust, spot oddities correctly, their practical fit in daily operations. A shift toward blending deep data analysis with machine learning could open paths to forecast risks, signal fraud sooner, trigger automatic review cues. Spotting questionable deals ahead of time may let companies act faster, reduce harm to reports, and strengthen efforts against deception.

Watching data as it flows helps spot odd patterns right when they happen. Because systems react to events, alerts go out fast if something looks wrong. This way, accountants and auditors stay on the same page without delay. When updates appear instantly, teams respond faster than before. Seeing clear visuals of activity means choices get made quicker. Information moves smoothly, so everyone knows what is going on at each step.

One way ahead might involve building systems that grow easily, shaped in pieces that fit together as needs change. Instead of fixed designs, using cloud setups allows space to stretch when more work comes through. Containers help keep things running smoothly, even as demands shift over time. Performance stays steady, access remains protected, reliability holds firm - all without slowing down. How it expands matters just as much as what it does.

Finding ways to work across different devices keeps coming up as a clear need. When dashboards take less power to run, small teams can keep up without high-end gear. Tools that fit on phones help too - especially where the internet or training aren't strong. Simpler interfaces tend to spread faster when tech support is thin.

Frozen records might soon ride alongside blockchain, locking every step in stone. Clearer machine thinking could walk hand in hand with anomaly spotting, thanks to explainable AI. Trust grows when reasons tag along with alerts. Efficiency tags rise when systems stop guessing. Audit trails gain weight when nothing slips through time. Progress hides in how pieces link, not just what they do.

7. CONCLUSION

Not one method fixes every gap, though some try hard by using deep autoencoders to rebuild data points. Others lean on sequences predicting suspicious activity step by step. A few stick with older machine learning models sorting cases into clean buckets. Still, problems pop up when rare events drown in oceans of normal records. Understanding why a decision was made often stays unclear. Spotting oddities across entire systems while also catching tiny irregularities nearby? Rarely handled well. When scams shift shape over time, many tools lag behind instead of keeping pace. Real audits feel these shortcomings sharply.

Looking at what's missing, one thing stands out - a smart anomaly detector that runs on its own, grows with demand, learns patterns clearly. This study's findings set the stage for **Anomatrix**, built to fix current flaws by mixing several methods: **Deep Autoencoders** dig into features, LSTMs track time-driven shifts, **Random Forests** weigh decisions firmly. It also tackles skewed data using SMOTE or ADASYN, while scoring odd events more accurately through adjusted probabilities.

All things considered, this work pulls together recent advances along with real-world uses in spotting oddities within financial records, while also flagging key hurdles ahead. Results show **Anomatrix** fits well into today's audit and fraud-checking scenes - its strength lies in sharper precision, lighter human effort, fewer black-box moments during reviews.

8. REFERENCES

[1] G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "An Intelligent Fraud Detection Model based on Deep Learning Ensembles," 2022.

[2] A. Bakumenko and A. Elragal, "Detecting Anomalies in Financial Data Using Machine Learning Algorithms," *Systems*, vol. 10, no. 130, 2022.

[3] M. Schreyer, T. Sattarov, D. Borth, A. Dengel, and B. Reimer, "Detection of Anomalies in Large-Scale Accounting Data using Deep Autoencoder Networks," 2020.

[4] I. Benchaji, S. Douzi, and B. El Ouahidi, "Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks," *Journal of Advances in Information Technology*, vol. 12, no. 2, pp. 113–118, 2021.

[5] J. Chen, Y. Shen, and R. Ali, "Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network," in *Proc. IEEE IEMCON*, 2019.