iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: https://doi.org/10.22214/ijraset.2026.85529

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue X Oct 2026- Available at www.ijraset.com

ORION: An Organizational Risk Intelligence Platform with Rule-Based Scoring and Isolation Forest Anomaly Detection for Multi-Department Risk Monitoring

Mangai K[1], Deepak M[2], Gokul Raj C[3], Chandra Mouli N[4]
Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

Abstract: ***Organizations monitor financial, human-resource, IT, operational and customer risks in separate spreadsheets and tools, so a risk in one department is reported in a different format and at a different time from a risk in another, and unusual transactions are found late. This paper presents ORION, an organizational risk intelligence platform that brings the five departments into one web application. Records are imported through a form or a bulk file, validated and cleaned, and stored in a unified database. A rule engine adds the weights of triggered conditions, such as a high amount, unusual timing or a suspicious merchant or location, into a risk score from 0 to 100 that is classified as Low, Medium, High or Critical and gives the reasons for a flag. An Isolation Forest model gives a second, unsupervised anomaly score for the same transaction. Department dashboards show key indicators, a severity index, trends and live alerts, and an audit view lets a reviewer approve, flag or block. Access is controlled by role and department with bcrypt-hashed passwords and signed tokens. The platform is built with React, Node.js, Express and MongoDB. The architecture, algorithms and prototype are described, and a reproducible evaluation plan is given.***

Keywords: ***Organizational Risk Intelligence, Risk Scoring, Anomaly Detection, Isolation Forest, Enterprise Risk Management, Department Dashboards, Role-Based Access Control.***

I. INTRODUCTION

Every organization faces risk in several places at once: an unusual payment in finance, a duplicate payroll entry in human resources, an unpatched device in IT, a supplier delay in operations and a churning account in customer relationship management (CRM). In many organizations each department tracks its own risk in its own spreadsheet or tool. The formats differ, the reports arrive at different times, and nobody sees the risk of the whole organization on one screen. A suspicious transaction is therefore often noticed only when an auditor reads the ledger.

Each part of this problem has been addressed, but only by a separate solution. Risk management frameworks describe how risks should be identified, assessed and treated [1], [2], but they are guidance and not software. Anomaly and fraud detection research provides statistical and machine learning detectors [3]–[6], but a detector alone gives a number and not a monitored, access-controlled process with alerts and recommended actions. A manager who needs all of these must combine separate tools whose data are not shared.

This paper presents ORION, a unified *organizational risk intelligence platform* in which one database and one dashboard serve Finance, Human Resources, IT, Operations and CRM. A *rule engine* gives each transaction a score from 0 to 100 with stated reasons, an *Isolation Forest* model [6] gives an independent anomaly score, and *role- and department-based access control* ensures that every user sees only the departments assigned to them. Alerts, recommendations and audit actions turn the scores into decisions.

II. LITERATURE SURVEY

1) Committee of Sponsoring Organizations of the Treadway Commission (COSO), “Enterprise Risk Management — Integrating with Strategy and Performance” (2017). The framework explains how risk management can be integrated into strategic planning and performance, by identifying risks, evaluating their impact and aligning the response with objectives. It supports systematic decision-making, but it is guidance that an organization must turn into its own tools and procedures. [1]

©IJRASET: All Rights are Reserved

2) International Organization for Standardization, "ISO 31000:2018 Risk Management — Guidelines". The standard gives principles and guidelines for identifying, analysing, evaluating and treating risk in organizations of any size, with continual monitoring. It is general, and an organization must customise it to its operations and resources. [2]

3) V. Chandola, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey", ACM Computing Surveys (2009). The survey reviews statistical, machine learning and other techniques for finding patterns that differ from normal behaviour in many domains. It is the foundation for detecting unusual transactions, but the choice of technique depends on how normal behaviour is defined in each application. [3]

4) R. J. Bolton and D. J. Hand, "Statistical Fraud Detection: A Review", Statistical Science (2002). The review examines statistical tools for detecting fraud and unusual transaction patterns and the need to separate legitimate from suspicious behaviour. It notes that changing fraud patterns and scarce labelled data limit accuracy, and it presents no monitoring platform. [4]

5) E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen and X. Sun, "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature", Decision Support Systems (2011). The review classifies data mining techniques used in financial fraud detection. It shows that data analysis can reveal suspicious financial activity, but results depend on data quality, features and the changing nature of fraud, and the work is not a deployed system. [5]

6) F. T. Liu, K. M. Ting and Z.-H. Zhou, "Isolation Forest", IEEE ICDM (2008). Isolation Forest detects anomalies by isolating observations with random partitions, so anomalies are isolated in fewer splits than normal records. It is fast and needs no labels, which suits transaction records, but its parameters and the characteristics of the data affect the result. [6]

7) T. Saito and M. Rehmsmeier, "The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets", PLOS ONE (2015). The study shows that precision and recall describe a classifier more informatively than the ROC curve when positive cases are rare. This applies to risk detection, where critical events are much rarer than normal activity, and it guides the evaluation plan of this paper. [7]

8) National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", NIST AI 100-1 (2023). The framework organises the management of AI risk into Govern, Map, Measure and Manage and stresses trustworthy, transparent and accountable AI. It offers principles for a responsible risk intelligence platform, which an organization must adapt to its own setting. [8]

9) L. Akoglu, H. Tong and D. Koutra, "Graph Based Anomaly Detection and Description: A Survey", Data Mining and Knowledge Discovery (2015). The survey reviews methods that detect unusual structures and relationships in connected data, such as suspicious groups of accounts. These methods could extend the platform, but they need complex data preparation and computing resources for large, changing networks. [9]

10) I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions", SN Computer Science (2021). The paper reviews machine learning algorithms and their applications in classification, prediction and pattern recognition. It is a general foundation for analytical methods in a risk platform, but reliable use depends on suitable data, model selection and evaluation. [10]

11) M. Jones, J. Bradley and N. Sakimura, "JSON Web Token (JWT)", RFC 7519 (2015). The specification defines a compact, URL-safe way to represent claims between two parties, signed so that they can be verified. It is the basis of the signed tokens that carry a user's role and department in ORION, but it does not define what access rules a system should apply. [11]

12) N. Provos and D. Mazières, "A Future-Adaptable Password Scheme", USENIX Annual Technical Conference (1999). The bcrypt scheme hashes passwords with an adjustable cost, so that the hashing can be made slower as computers become faster. It protects stored passwords, but a hashed password is only one part of securing a platform. [12]

III. RESEARCH GAP

The surveyed works each provide guidance, a detector or a security mechanism, as summarised in Table I. The following gaps remain.

A. Guidance without a Working Platform

Frameworks and standards [1], [2], [8] describe what to do with risk but do not provide a tool that collects the data of several departments and scores them in the same way.

B. Detectors without a Monitored Process

Anomaly and fraud detection studies [3]–[6], [9] produce scores or flags. They do not describe the surrounding process of department dashboards, alerts, recommended actions and audit decisions on which an organization acts.

C. Scores without Reasons

A single machine learning score is hard for an auditor to accept. A rule that states why a record was flagged, shown beside an independent anomaly score, is easier to review, and the evaluation must account for the rarity of critical events [7].

D. Access Not Tied to Department

Risk data of Finance, HR and IT are sensitive in different ways. A platform for several departments must limit each user to the departments assigned to them, which the surveyed detection works do not address.

TABLE I.
CAPABILITIES OF RELATED WORK AND ORION (YES = PROVIDED; PART. = PARTIALLY OR AS GUIDANCE; – = NOT DESCRIBED)

Work	Multi-department monitoring	Risk score and levels	Anomaly detection	Alerts and recommendations	Dashboard	Role and department access
[1], [2]	Part.	Part.	–	–	–	–
[3], [6], [9]	–	–	Yes	–	–	–
[4], [5]	–	–	Yes	Part.	–	–
[8]	Part.	Part.	–	–	–	Part.
[10]	–	–	Part.	–	–	–
[11], [12]	–	–	–	–	–	Part.
ORION	Yes	Yes	Yes	Yes	Yes	Yes

IV. PROBLEM STATEMENT

Organizations lack a unified, low-cost platform that (i) imports and cleans the data of Finance, HR, IT, Operations and CRM, (ii) gives each transaction a score from 0 to 100 with reasons and an independent anomaly check, (iii) shows department indicators, alerts and recommended actions on one dashboard, and (iv) lets each user see only the departments and functions assigned to them.

V. OBJECTIVES

1) To import records through a form and a bulk file and to validate, clean and store them in a unified database.
2) To score each transaction from 0 to 100 with a weighted rule engine and to classify it as Low, Medium, High or Critical, with the reasons for a flag.
3) To add an Isolation Forest anomaly score as an independent check on the same transaction.
4) To present indicators, a severity index, trends and alerts for Finance, HR, IT, Operations and CRM.
5) To let a reviewer approve, flag or block a transaction and to record the status.
6) To restrict access by role and department, and to define a reproducible evaluation.

VI. METHODOLOGY

A. System Architecture

ORION has five layers, as shown in Fig. 1. Records from the five departments enter an import and preprocessing layer that validates, cleans and transforms them and stores them in a unified MongoDB database. A risk engine built in Node.js and Express.js scores and classifies each record. A React dashboard layer shows alerts, recommendations, department dashboards and audit actions. A security layer applies to every request: passwords are checked against bcrypt hashes, a signed token carries the role and department, and each API route is limited to the departments allowed to use it.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

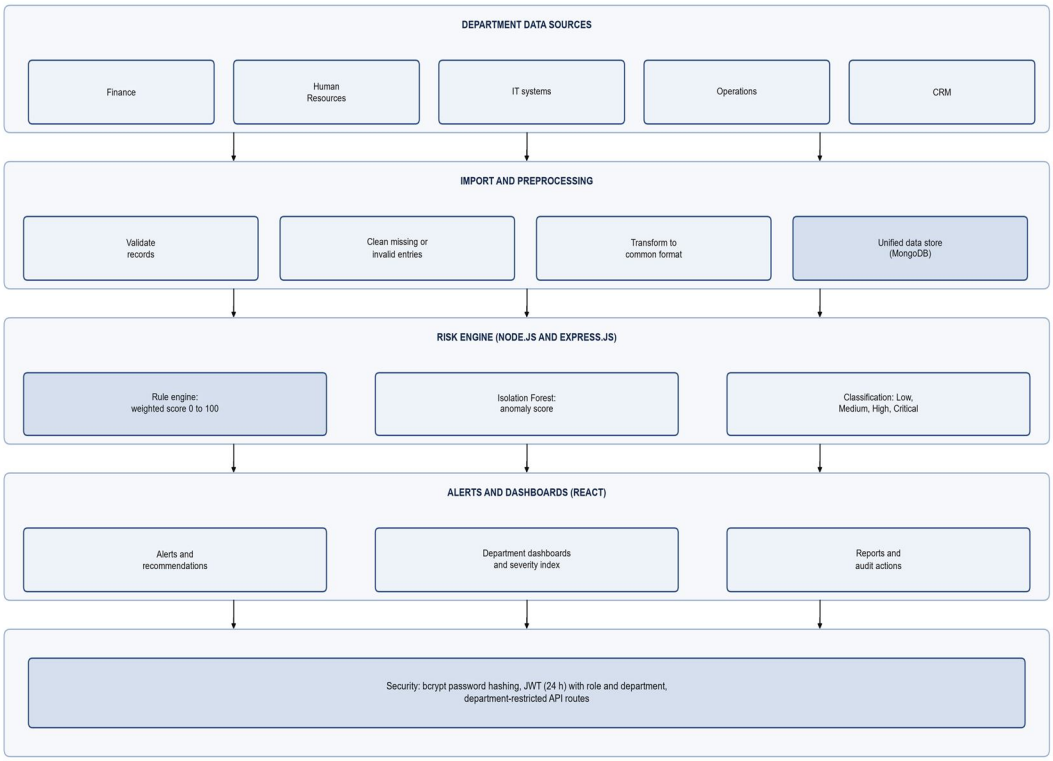


Fig. 1. Architecture of ORION: department data sources, preprocessing, risk engine, alerts and dashboards, and the security layer.

B. Data Import and Preprocessing

A record can be entered through a registration form with the transaction identifier, account reference, amount in rupees, transaction type, merchant or receiver, location, payment method and an optional timestamp, or imported in bulk from XLSX, DOCX, CSV or TXT files that follow a template. On entry the record is checked for missing values, inconsistent values and invalid entries, cleaned according to the validation rules, converted to a common format and stored. The same structure is thus available to every later step and to every department.

C. Rule-Based Risk Scoring

The rule engine tests a transaction against the conditions of Table II. Each triggered condition *i* adds a configured weight w_i, and the score is limited to the range 0 to 100:

$$R = \min(\max(\Sigma\, w_i\, c_i, 0), 100), \quad c_i = 1 \text{ if condition } i \text{ is triggered, else } 0 \tag{1}$$

The score is classified into Low, Medium, High or Critical by configured limits, and the transaction is flagged when R reaches the lower limit τ_H of the High level. Every triggered condition adds a reason, such as “high transaction amount detected”, to the record, so that a reviewer sees why the score was given. The weights, limits and lists of risky merchants and locations are kept in a configuration file and not in the code.

TABLE II.
CONDITIONS OF THE RULE ENGINE

Condition	Triggered when
High amount	The amount exceeds the configured threshold (₹50,000 in the prototype)
Unusual timing	The hour of the transaction is in the configured late-night period
Suspicious merchant or location	The merchant name or the location matches a configured list of risky entries
Frequency (design)	The account makes an unusual number of transactions in a period
Deviation (design)	The amount differs strongly from the account’s historical amounts

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Isolation Forest Anomaly Check

An Isolation Forest [6] is trained on the stored transactions. It builds an ensemble of isolation trees, each on a random sub-sample of the records, and an anomalous record is isolated after fewer random splits than a normal one. The prototype uses 100 trees and a sub-sample size of 256, and refuses to train on fewer than five records. For a record x and a sample of size n, the anomaly score of [6] is

$$s(x, n) = 2^{-E[h(x)] / c(n)}, \quad c(n) = 2\,H(n-1) - 2\,(n-1)/n \tag{2}$$

where $E[h(x)]$ is the mean path length of x over the trees and $H(i)$ is the harmonic number, approximately $\ln i + 0.5772$. A score near 1 marks an anomaly. ORION reports this score on a 0 to 100 scale beside the rule-based score and does not merge the two, so a reviewer can see when the rules and the model disagree.

E. Department Dashboards, Alerts and Recommendations

Each department has its own dashboard with indicator cards, a severity index that counts open alerts as Critical, High, Medium and Low, a trend chart that can be viewed for today, this week or this month, and a list of live alerts. Alerts are raised when a score reaches a configured threshold, are ordered by severity, and carry a recommendation for the corrective action. A transaction can be opened in an audit view that shows its data, the rule reasons and the anomaly check, and a reviewer can approve it as legitimate, flag it as suspicious, block the account or download a report. Fig. 2 shows how a transaction is processed. The dashboard summary also reports the average risk score of the N stored transactions:

$$\text{Average risk score} = (1/N)\,\Sigma\, R_j \tag{3}$$

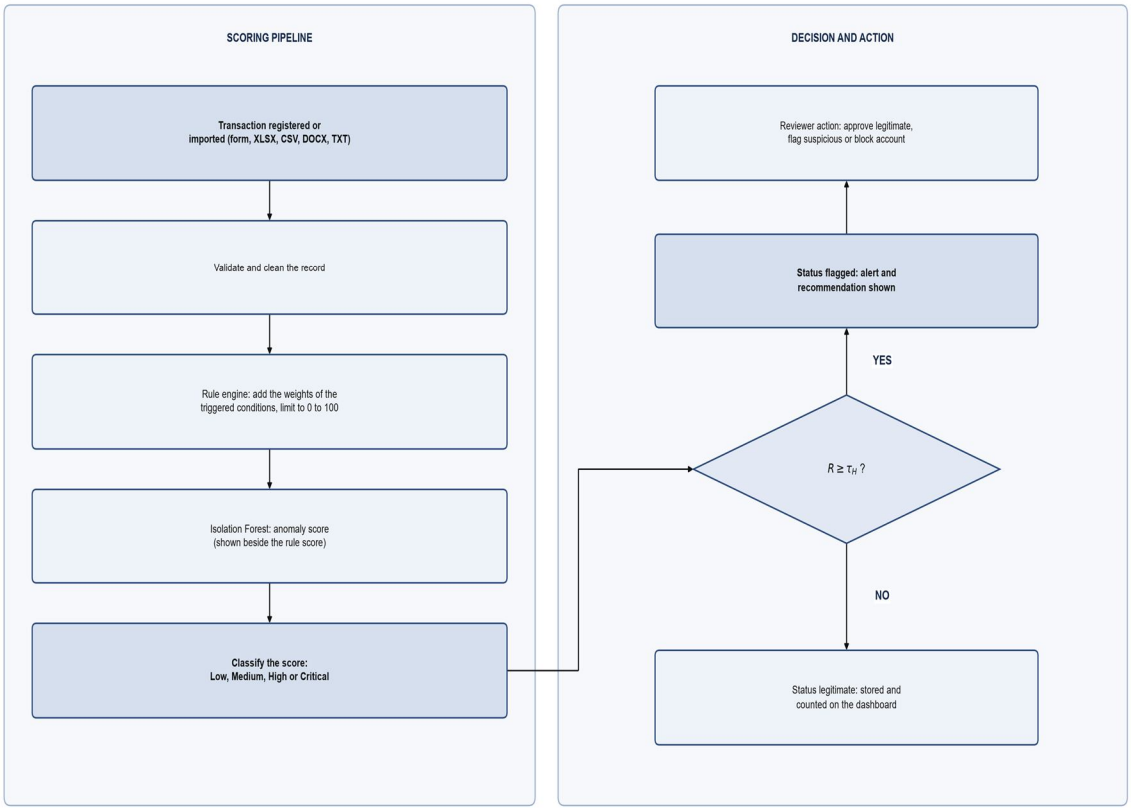


Fig. 2. Processing of a transaction: scoring pipeline (left) and decision and action (right).

F. Security and Access Control

Every user has a role and a department and may be deactivated by an administrator (Table III). At login the password is compared with its bcrypt hash [12], and an active user receives a signed JSON Web Token [11] that carries the user's identity, role and department and expires after 24 hours. Each API request passes an authentication check that verifies the token and the account status, and the route of a department additionally requires that the user belongs to that department, as listed in Table IV.

TABLE III.
ROLES AND DEPARTMENTS

Role	Department	Access
Admin	All	User accounts, roles and departmental permissions
Risk Manager	All	Risk information of all departments
Finance Analyst	Finance	Transactions and finance dashboard
HR Analyst	HR	HR risk dashboard
IT Analyst	IT	IT risk dashboard
Operations Analyst	Operations	Operations risk dashboard
CRM Analyst	CRM	CRM risk dashboard

TABLE IV.
API ROUTE GROUPS

Route	Access limited to	Purpose
/api/auth	Public	Login
/api/transactions	Finance	Register, import and analyse transactions
/api/dashboard	Finance	Summary of transactions and risk
/api/hr	HR	HR risk data
/api/it	IT	IT risk data
/api/operations	Operations	Operations risk data
/api/crm	CRM	CRM risk data
/api/health	Public	Server and database status

The data are stored in MongoDB through Mongoose in collections for users, transactions, vendors and invoices; a transaction carries its amount, time, merchant, location, risk score and status (legitimate, flagged or blocked). If the configured database cannot be reached, an in-memory MongoDB instance is started for development and testing. The React frontend sends the stored token in the Authorization header of every request.

VII. RESULTS AND DISCUSSION

A. Prototype Implementation

The prototype was exercised through its web interface. Fig. 3 shows the risk audit view of a transaction, the Finance dashboard, the HR dashboard and the user management screen. Table V lists the functions that were exercised, and Table VI gives the severity index shown on each department dashboard with the data loaded in the prototype, which includes development seed data.

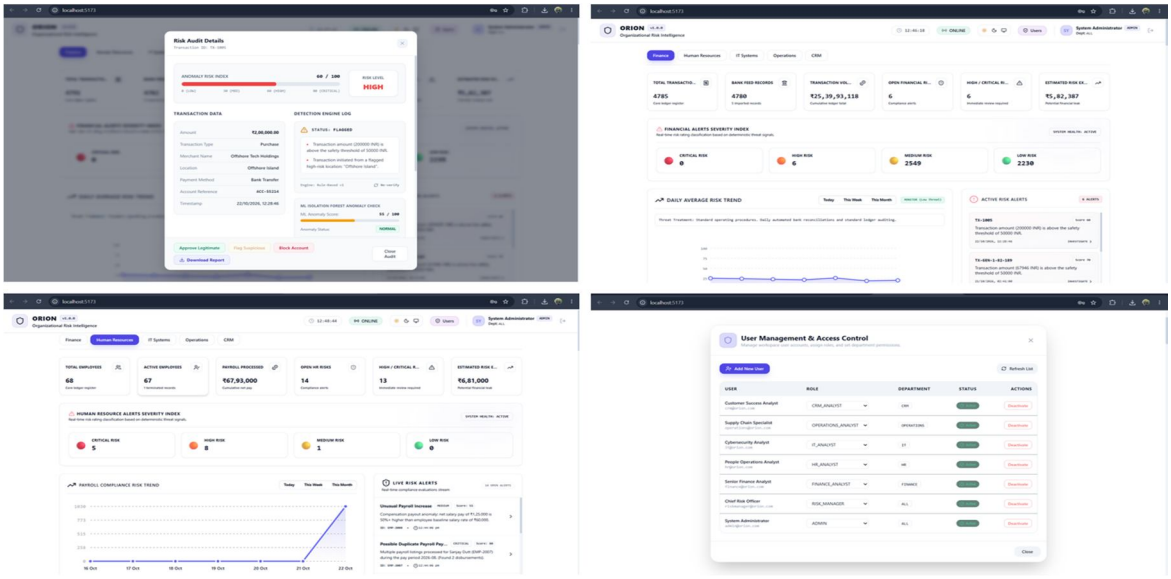


Fig. 3. Prototype screens: risk audit details, Finance dashboard, HR dashboard and user management.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

TABLE V.
FUNCTIONS EXERCISED ON THE PROTOTYPE

Function	Observed behaviour
Login and roles	Sign-in by email and password; role and department shown for the user
User management	Users listed with role, department and status; add, assign and deactivate
Transaction entry	Registration form and bulk import of XLSX, DOCX, CSV and TXT files
Risk audit	Score, level, flag status, reasons, rule-engine log and Isolation Forest check; approve, flag, block, report
Department dashboards	Indicator cards, severity index, trend chart and live alerts for the five departments

TABLE VI.
SEVERITY INDEX SHOWN ON THE DEPARTMENT DASHBOARDS

Department	Critical	High	Medium	Low	Open risks
Finance	0	6	2549	2230	6 (high or critical)
Human Resources	5	8	1	0	14
IT Systems	4	4	0	0	8
Operations	3	5	1	0	9
CRM	1	0	3	0	4

The audit view of Fig. 3 gives a worked example. A purchase of ₹2,00,000 by bank transfer at “Offshore Tech Holdings” in “Offshore Island” received a rule-based score of 60 of 100 and the level High, and was flagged for two reasons: the amount is above the safety threshold of ₹50,000, and the transaction came from a flagged high-risk location. The Isolation Forest check of the same transaction gave 55 of 100 and the status Normal. The two checks thus answered differently, which is why both are shown to the reviewer.

B. Evaluation Plan

Because the project is at the prototype stage, a formal protocol is defined rather than reporting unmeasured figures. A labelled test set will be prepared from audited transactions, with a known number of injected anomalies, and the rule engine, the Isolation Forest and their combination will be compared. Because anomalies are rare, precision and recall are reported, as recommended in [7]:

$$P = TP / (TP + FP), \quad R = TP / (TP + FN), \quad F1 = 2 \cdot P \cdot R / (P + R) \tag{4}$$

where TP, FP and FN are the numbers of true positives, false positives and false negatives. The decision limit τ_H will be chosen on a validation subset to balance missed risks against false alerts, and the number of alerts per day will be recorded because it decides the workload of the reviewers. Table VII lists the planned measurements.

TABLE VII.
PLANNED EVALUATION METRICS

Aspect	Metric	Method
Detection	Precision, recall, F1	Labelled test set; rules, Isolation Forest and both
Ranking	Area under the precision–recall curve	Score as the ranking of transactions
Threshold	Missed-risk and false-alert rates	Validation subset, varying τ_H
Workload	Alerts per day	Replay of a month of transactions
Latency	Time to score and display	Registration to dashboard update
Access	Requests refused for a wrong department	Test of each route with each role

C. Discussion

The prototype shows that the risk of five departments can be collected, scored and presented in one platform, and that a rule that states its reasons can be shown next to an independent anomaly check. Three design choices make the platform cautious: a flag always carries its reasons, the two detectors are not merged into one opaque number, and access is restricted by role and department on the server.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The evaluation is limited to the prototype: detection performance and the best decision limit are not yet measured, and the data shown are development data. The rule weights and limits must be calibrated for each organization, an unsupervised model flags rare records that are not necessarily risky [3], and the scoring engine of the prototype works on financial transactions while the other departments are presented as monitoring dashboards. A development default for the token secret exists in the code and must be replaced by a secret of the organization before deployment. The scores support the reviewer and do not replace the reviewer's judgement, in line with the accountability stressed in [8].

VIII. CONCLUSION AND FUTURE SCOPE

ORION combines data import and preprocessing, a weighted rule engine with stated reasons, an Isolation Forest anomaly check, department dashboards with alerts and recommendations, and role- and department-based access control in one platform, functions that existing tools provide separately. Future work includes the quantitative evaluation described above, calibration of the rule weights from audited data, predictive models that warn before a risk occurs, industry-specific indicators for healthcare, banking, manufacturing and retail, automated responses to critical risks, graph-based detection of related accounts [9], richer reports and trend analysis, and cloud deployment.

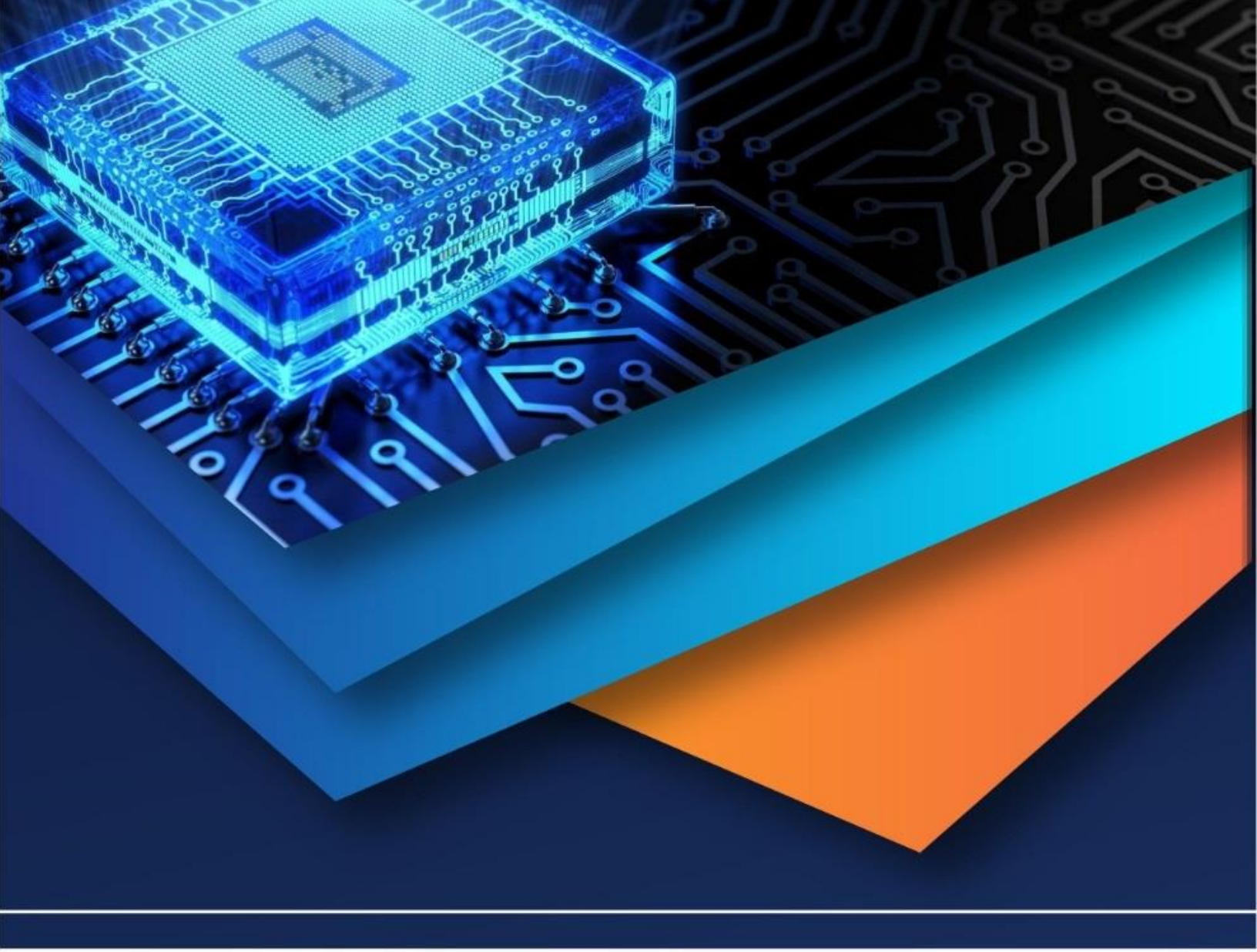
IX. ACKNOWLEDGMENT

The authors thank the Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, for institutional support.

REFERENCES

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management — Integrating with Strategy and Performance, 2017.
[2] International Organization for Standardization, ISO 31000:2018 Risk Management — Guidelines, 2018.
[3] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, Art. 15, 2009.
[4] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235–255, 2002.
[5] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decis. Support Syst., vol. 50, no. 3, pp. 559–569, 2011.
[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. 8th IEEE Int. Conf. Data Mining (ICDM), 2008, pp. 413–422.
[7] T. Saito and M. Rehmsmeier, "The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets," PLOS ONE, vol. 10, no. 3, e0118432, 2015.
[8] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, 2023.
[9] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," Data Min. Knowl. Discov., vol. 29, pp. 626–688, 2015.
[10] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," SN Comput. Sci., vol. 2, Art. 160, 2021.
[11] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," IETF RFC 7519, May 2015.
[12] N. Provos and D. Mazières, "A future-adaptable password scheme," in Proc. USENIX Annu. Tech. Conf., 1999, pp. 81–91.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)