Journal of
Information Systems Engineering
and Business Intelligence

Vol.X, No.X, February/June/October XXXX
Available online at: http://e-journal.unair.ac.id/index.php/JISEBI

AI-Driven Anomaly Analysis Techniques for Fraudulent Claims, Transactions, and High-Risk Activities Across Financial and Healthcare Systems

First Author [1)*], Second Author [2)], Third Author [3)]

[1)3)]Affiliation information, City, Country
[1)]author1@domain.ac.id, [3)]author2@domain.edu

[2)] Affiliation information, City, Country
[2)]author2@domain.com

Abstract

Background: Artificial intelligence has advanced fraud detection across financial and healthcare systems, yet most studies remain domain-specific and lack cross-sector performance evaluation. Complex, noisy healthcare data continue to challenge model accuracy compared to more structured financial datasets.
Objective: This study aimed to compare the performance of AI-driven anomaly-detection models across financial transactions and healthcare claims, and to identify whether a unified framework for multi-domain fraud detection is feasible.
Methods: A quantitative machine-learning approach was used. Two public datasets: the NHIS Healthcare Claims Fraud (2024) and the Credit Card Fraud Detection Dataset (2023) were preprocessed using SMOTE/SMOTE-ENN, feature engineering, and 80/20 train–test splits. Random Forest, XGBoost, and SVM models were trained and evaluated using precision, recall, F1-score, accuracy, and ROC-AUC.
Results: Financial fraud detection achieved near-perfect performance, with Random Forest and XGBoost scoring 99.98% across precision, recall, F1-score, and ROC-AUC. Healthcare fraud detection revealed lower scores: Random Forest achieved 98.42% accuracy, whereas SVM performed the weakest (80.96% accuracy).
Conclusion: Results indicate that ensemble models generalise effectively, but healthcare data require more sophisticated feature engineering. A unified framework is possible, but it must include domain-specific adaptations.

Keywords: AI-driven anomaly detection, financial fraud, healthcare claims fraud, cross-domain analysis, imbalanced learning, explainable AI (XAI).

Article history: Received 5 April 20XX, first decision 22 April 20XX, accepted 22 August 20XX, available online 28 October 20XX

I. INTRODUCTION

The rapid shift toward digital transactions and the electronic processing of claims has increased operational efficiency in both the financial and healthcare sectors; however, it has also increased the risk of fraud [1, 2]. Traditional rule-based audit systems have difficulty keeping up with modern trends in fraud, which are highly unequal, concept-drift-prone, involve hidden tricks, and continuously increase the oppositional disposition [3]. Similar weaknesses exist in healthcare systems, including falsified claims, up-coding, and mind-fraud billing, where manual review processes are too slow and weak [4, 5].

Recent advances in artificial intelligence (AI) have transformed fraud detection by enabling models to detect complex, non-linear, and dynamic anomalies [1, 6, 7]. Deep learning, autoencoders, graph neural networks, ensemble strategies, and explainable AI are among the techniques which have shown high performance compared to high-level rule-based systems [8, 9]. The forthcoming solutions also include adversarial robustness, federated learning, and anomaly detection in time-series and IoT-based healthcare scenarios [10, 11].

Despite these improvements, most available research focuses on individual spheres, such as finance or healthcare. It does not assess the applicability of AI anomaly-detection models across different fraud-related settings [1, 5, 12]. There is a gap in the methodology, as very few studies combine Python-based machine learning with statistical validation across multiple datasets [13].

[*] Corresponding author

ISSN 2443-2555 (online) 2598-6333 (print) © 20XX The Authors. Published by Universitas Airlangga.

doi: http://dx.doi.org/10.20473/jisebi.X.X.pp-pp

This study addresses these gaps through a multi-domain empirical investigation of AI-based anomaly-detection systems in financial transactions, healthcare claims fraud, and high-risk system activity data [3, 13]. The Python framework strengthens analytical reliability while enabling cross-sector comparison of anomaly patterns, model performance, and key risk features [8, 14, 15]. The study aims to contribute to cross-sector fraud analytics by providing insights into the generalisability, performance, and applicability of AI models across varying anomaly settings. In particular, the research questions of the study are the following: (1) How do different AI models compare in detecting anomalies across financial and healthcare datasets? (2) What are the key features that influence model performance in each domain? (3) Can a unified framework be developed for anomaly detection across these sectors?

The novelty of the proposed research lies in its cross-domain analysis, which combines datasets and approaches to provide a holistic view of AI-driven fraud detection. Drawing on the latest developments in machine learning and deep learning, this study provides new insights into the flexibility of AI models across diverse fraud environments. Additionally, incorporating healthcare claim-fraud data [16], financial transaction data [17], and cybersecurity logs provides the literature on fraud detection, as it covers a little-explored field of evidence.

In practice, this study is significant to policymakers, auditors, and IT experts who are charged with developing effective fraud-detection measures. For example, combining AI and standard auditing tools, including the Law of Benford [3, 18], can improve the accuracy of fraud detection in financial statements. Similarly, AI solutions that preserve privacy [19] offer an opportunity to comply with privacy regulations, including the EU AI Act, while retaining detection performance. Furthermore, the results on adversarial attacks and defences in this study [20] still make a vital contribution to existing knowledge on protecting AI models against emerging threats in decentralised finance [21] and IoT-based healthcare systems [15].

II. Literature Review

A. Overview of AI-Driven Fraud Detection

In financial, healthcare, and high-risk online settings, artificial intelligence (AI) has transformed fraud detection by analysing large, complex, and dynamic datasets. Rule-based systems were found to be less valuable in the face of changing fraud trends, especially for less apparent or masked anomalies. Machine learning (ML) and deep learning (DL) models, such as autoencoders, LSTM networks, XGBoost, graph neural networks (GNNs), and hybrid ensembles, are more effective than classical methods because they identify deviations in behaviour and non-linear correlations [1, 6, 9].

Transparency and explainability are the main priorities, particularly in fields such as finance and healthcare [22, 14]. In addition to ethical considerations, the preservation of privacy and governance structures also influence the role of AI in sensitive applications that handle both personal and financial information [19, 23, 24].

B. AI Fraud Detection Performance

The performance of AI fraud detection is the primary objective variable in the study of anomaly detection, and an indicator of how effectively AI systems detect fraudulent activity in digital settings [1, 3]. Performance is evaluated using precision, recall, F1-score, AUC-ROC, confusion matrices, reconstruction errors, and distributions of anomaly scores [14, 25]. These indicators evaluate the model's potential to detect and reduce false alarms.

Some factors that impact performance include the quality of the anomaly features obtained from transactional or claim-level data [8]. The consideration of class imbalance through methods such as oversampling or hybrid sampling also has a significant effect [26, 27]. Inference in complex scenarios requires high-quality AL patterns, whereas LSTMs, CNNs, and transformers in this group have demonstrated excellent performance in such scenarios [9, 25, 28, 29]. Traditional frameworks that combine ML and DL achieve even greater accuracy and robustness [30].

Along with accuracy, interpretability, and transparency, these qualities have also become increasingly significant, especially in regulated areas such as healthcare and the financial sector [22]. Explainable artificial intelligence (XAI) algorithms, such as SHAP or LIME, provide insights into model decisions that people can easily understand [14]. The ability to resist adversarial attacks is also an important aspect, as fraudsters exploit model vulnerabilities [20]. Real-time applications, especially those that involve delays, are also highly demanding in terms of computational efficiency, as even small latencies can lead to significant losses [19].

C. Financial Transaction Anomalies

Financial transaction anomalies represent one of the best-studied areas in fraud detection, in part due to the greater susceptibility of online financial ecosystems to malicious activities, synthetic identities, money laundering, and high-frequency micro-fraud [31, 32, 33]. Previous studies have shown that financial anomalies often manifest as unusual transaction flows, unanticipated user behaviour, an abnormal variety of merchants, duplicate payments, or temporal issues with transactions [1, 34, 35]. Machine-learning and deep-learning models, such as Random Forests, XGBoost, Graph Neural Networks (GNNs), Autoencoders, and their hybrids, have demonstrated a strong ability to detect non-linear and textural deviations in financial data [6, 8]. In addition, complex methods such as multiple Benford Law distributions can help auditors identify numerical anomalies early [3].

Recent research combines sampling techniques to balance highly imbalanced financial data, and hybrid oversampling, SMOTE, and undersampling techniques can enhance precision and recall [26, 36, 37]. Detecting temporal or structural anomalies that are not detectable in traditional models can be achieved with deep models that combine CNNs, Transformers, and autoencoders [9, 25, 28]. However, adversarial attacks remain a significant challenge, as scammers increasingly use digital traces to evade detection algorithms [20].

In the current study, financial transaction anomalies are among the main independent variables used to determine AI fraud-detection performance. The influence of variations in anomaly patterns on model measures is critical to the design of robust, generalisable fraud-detection systems.

H1: Financial Transaction Anomalies significantly improve AI-based fraud detection performance.

D. Healthcare Claim Anomalies

Anomalies in healthcare claims constitute a unique and equally valuable fraud category that includes up-coding, unbundling, phantom billing, duplicate claims, overcharging for services, and falsification of procedures [4, 5]. Healthcare claims fraud often manifests in implicit forms that a human operator cannot detect, due to the bureaucratic nature of insurance practices and the dimensional nature of medical billing records. The researchers are increasingly using ML and DL methods, such as Random Forest, SVM, deep autoencoders, and hybrid deep neural networks, to detect inconsistencies in claims, patient histories, and provider behaviour [38, 39].

The combination of blockchain, federated learning, and privacy-preserving AI systems facilitates more effective healthcare fraud detection by improving transparency, traceability, and data security [19, 40, 41]. The literature notes that domain-relevant feature engineering, such as the frequency of procedure codes, provider usage behaviour, and cost-to-service anomalies, is also required for healthcare anomaly detection [42, 43].

Despite being domain-specific, healthcare claim anomalies constitute a second independent variable, providing specific behavioural, financial, and procedural deviation patterns that can directly influence AI detection performance. This paper unites medical data to assess the similarity of irregularity properties to financial transaction irregularities, in relation to detection quality, interpreters, and the strength of machine learning models.

H2: Healthcare Claim Anomalies significantly improve AI-based fraud detection performance.

E. High-Risk System Activity Anomalies

High-risk system-activity anomalies emerge within critical digital infrastructures, i.e., IoMT networks, mentalised finance systems, mobile health devices, cybersecurity logs, and wireless body-area networks. Such anomalies are unauthorised access, uncharacteristic device-to-device communications, suspicious login sessions, suspicious API calls, IoT intrusions, and sensor manipulation [11, 15, 44]. System-level anomalies, compared to financial or healthcare claim anomalies, tend to be more dynamic and change rapidly due to active cyberattacks, malware spread, and attempts to exploit AI vulnerabilities.

Multidimensional behavioural anomalies can be detected by advanced AI-based intrusion-detection systems that use LSTM, RCLNet, autoencoders, and hybrid anomaly-detection structures [45, 13]. In addition, the need for resilient, attack-conscious AI systems that can manage privacy protection, explainability, and adversarial resilience is supported by regulatory focus, including the EU AI Act [19, 23]. Other sources suggest that system-activity anomalies need to be detected in real time, as they are very likely to cause rapid system compromise, operational issues, or massive data breaches [46].

In this study, high-risk system-activity anomalies serve as a third independent variable to determine the impacts of cybersecurity-related deviations on AI model performance and to assess the potential to separate these two detection frameworks for use in financial and healthcare settings.

H3: High-Risk System Activity Anomalies significantly improve AI-based fraud detection performance.

F. Identified Literature Gaps

There are plenty of research works in the financial, healthcare, and system security areas, but many significant gaps remain unfilled. To begin with, the literature focuses on individual sectors and is limited to a few studies that assess the cross-domain generalisability of anomaly-detection models [1, 5]. Second, to date, little empirical literature unites various types of anomalies (including transactional, medical, and system-level) into a single analytical framework, even though multi-domain fraud detection suggests that such strategies can be more effective than others [25, 27]. Third, few studies integrate Python-based MLs with statistical validation tools such as SPSS, creating a gap in empirical rigour and cross-validation [3, 13].

The other significant gap concerns adversarial resilience and explainability. Not all highly performing AI models, such as deep neural networks and autoencoders, have explicit reasoning processes, which makes it hard to regulate their application in medical care and finance [22, 47]. Additionally, most published studies are based on generated or simulated data, which limits their applicability to the real world and reduces reproducibility [20, 21].

In general, the literature lacks comprehensive empirical research assessing the consistency of AI-based anomaly-analysis methods across financial transactions, healthcare claims, and high-risk system logs. This gap is precisely addressed by the proposed study, which combines cross-domain datasets and uses ML techniques to evaluate AI-fraud-detection performance as a single outcome variable.

G. Theoretical Foundation

The theoretical background of the current research is mainly based on Anomaly Detection Theory, Fraud Triangle Theory, and Behavioural Pattern Deviation Theory, which offer different ways of understanding the emergence of fraud and how artificial intelligence (AI) systems respond to anomalous behaviour.

The theory of Anomaly Detection suggests that irregularities in fraudulent behaviour are not normative within a dataset and can be detected using statistical, rule-based, or AI-driven processes [9]. According to this description, anomalies in financial operations, medical reimbursements, and system activity produce signals that can be identified by machine learning (ML) and deep learning (DL) models, enabling automated fraud detection.

The Fraud Triangle Theory, which has long been utilised in the study of organisational and financial fraud, posits that fraud results from the interplay of pressure, opportunity, and rationalisation. AI systems cannot directly identify psychological motivators; however, according to the theory, structural opportunities and system weaknesses often reveal themselves as anomalies in a digital ecosystem [3, 24]. Therefore, it promotes the incorporation of cross-domain anomalies, since the three industries have various types of opportunistic fraud.

According to Behavioural Pattern Deviation Theory, individuals, machines, or systems still use consistent behavioural signatures; a breakage in this will not be an indicator of fraud or security risk [11, 15]. This theory lays the foundation for the utilisation of time-series, graph-based, and multivariate models to detect anomalous sequences or structural changes.

Collectively, these theoretical approaches explain why the three independent variables, which include financial transaction anomaly, healthcare claim anomaly, and high-risk system activity anomaly, were chosen and why it is possible to study whether these three independent variables predict the dependent variable, which is AI fraud detection performance. The proposed conceptual model is illustrated in Figure 1.

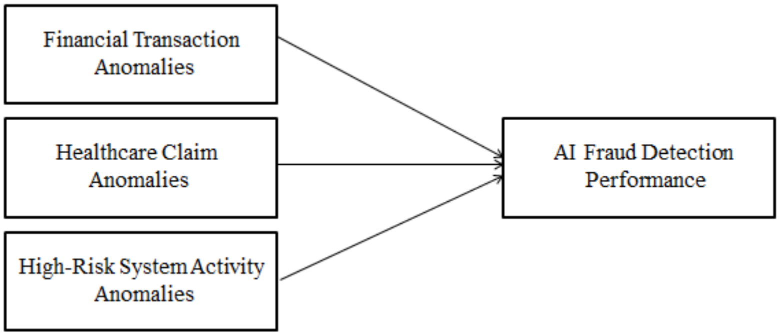
Financial Transaction Anomalies
Healthcare Claim Anomalies
High-Risk System Activity Anomalies
AI Fraud Detection Performance

Fig. 1 Conceptual Framework of AI Fraud Detection Performance Influenced by Three Anomaly Domains

III. METHODS

A. Research Design

This study adopted a quantitative empirical research design, formulating ML-based anomaly detection (in Python) with statistical validation to assess the implications of financial transaction, healthcare claim, and high-risk system activity anomalies on AI fraud detection performance. The design was selected to achieve computational accuracy and statistical rigour, in line with recommendations for multi-method fraud analytics in regulated settings [19, 14].

B. Data Sources

The financial and healthcare fraud domains were represented with two publicly available datasets from Kaggle (Table 1). First, the NHIS Health Insurance Claims Fraud [16] dataset includes beneficiaries' demographics, inpatient and outpatient claim histories, provider identifiers, diagnostic codes, and fraud labels. The data was based on practical trends in fraudulent claims behaviour, such as overbilling, procedural manipulation, and abnormal reimbursement.

Second, the Credit Card Fraud Detection Dataset [17] contains anonymised, PCA-transformed transaction data, which has been widely used in research on financial anomaly detection. It was filled with both legitimate and fraudulent transactions, reflecting the extreme imbalance between the two characteristics of fraud in a financial setting.

TABLE 1
OVERVIEW OF DATASET CHARACTERISTICS

Domain	Dataset Name	Total Records	Fraud Cases	Non-Fraud Cases	Key Components
Healthcare	NHIS Health Insurance Claims Fraud [16]	Beneficiary: 138,556; Inpatient: 404,983; Outpatient: 517,737; Providers: 4,750	534 providers labelled as fraudulent	≈4,216 non-fraud providers	Beneficiary data, inpatient claims, outpatient claims, and provider fraud labels
Financial	Credit Card Fraud Detection Dataset [17]	284,807	492	284,315	PCA-transformed features, transaction time, amount, and binary fraud label

C. Data Preprocessing

Data preprocessing was carried out in Python (pandas, numpy), including schema standardisation and handling missing values. Because of the class imbalance in fraud datasets, the study used post-division resampling with SMOTE and SMOTE-ENN to avoid data leakage, which is a good practice in imbalanced learning [36, 26].

Each domain was engineered using feature engineering, which included transactional behavioural patterns over time, provider-related spending anomalies, and session-related network behaviours.

Strategised train-test (80-20%) splits were then used to divide the cleaned data, and the supervised and unsupervised anomaly detection models were developed and trained in Python (Random Forest, XGBoost, and SVM) [8, 9, 48]. Precision, recall, F1-score, AUC-ROC, and the ability of the anomaly score to be a separate measurement were used to assess AI fraud detection performance multidimensionally [14, 25].

IV. RESULTS

A. Descriptive Analytics

1) Financial Dataset

The financial data indicates a severe imbalance between classes: 284,315 valid transactions (Class 0) and 492 fraudulent transactions (Class 1), resulting in a ratio of 0.17% of the entire dataset (Figure 2). To eliminate this bias, the SMOTE and SMOTE-ENN resampling methods were applied after the split to prevent data leakage, in line with best practices for imbalanced learning [36, 26]. These techniques scaled the fraudsters to the extent of a legitimate group, thus eliminating the imbalance and improving model training (Figure 2). The mean number of fraudulent transactions was lower than that of legitimate transactions, as observed in earlier studies. Features transformed using PCA presented nearly normal distributions, and features V3, V14, and V17 showed skewness.

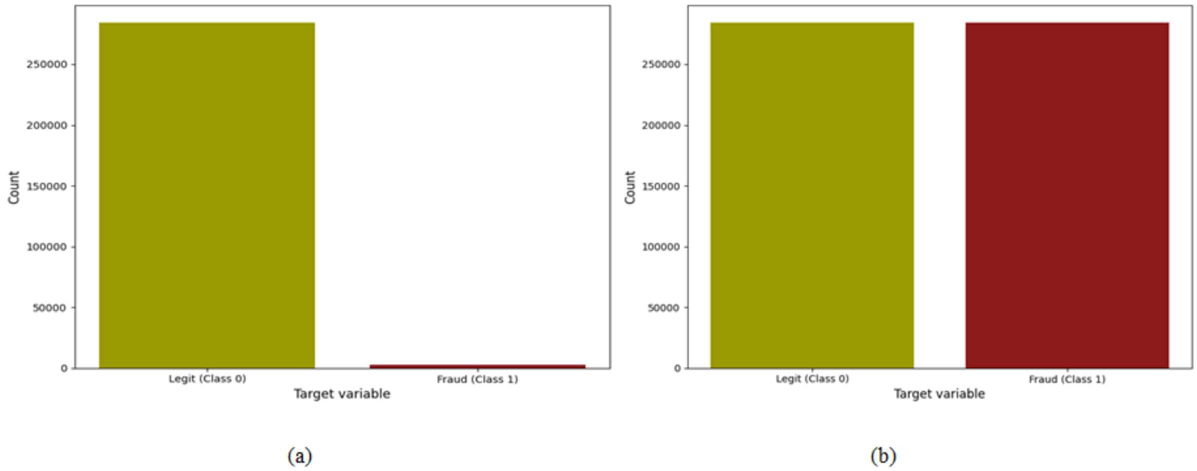

Fig. 2 Class Distribution in the Financial Dataset (a) Before resampling; (b) After resampling

2) *Healthcare Dataset*

The healthcare dataset included 517,737 outpatient and 404,983 inpatient claims (Figure 3). The average reimbursement amounts, abnormal billing frequency, and mismatches between diagnosis and procedure codes were much higher for fraudulent providers. Extensive feature correlations yielded preliminary results, showing that provider-level billing patterns were highly correlated with the likelihood of fraud labelling.

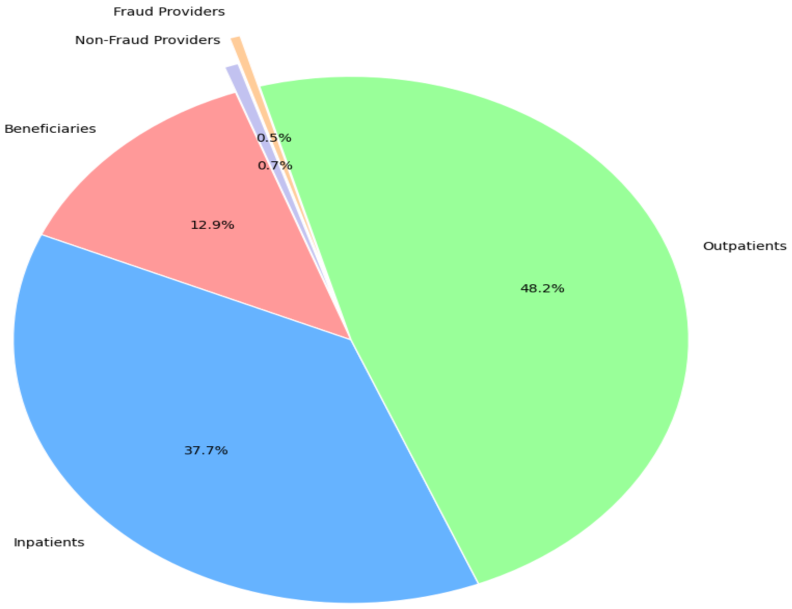

Fig. 3 Distribution of Healthcare Data and Fraudulent Providers

B. *Machine Learning Model Performance*

This study analyses the performance of machine learning algorithms, including Random Forest (RF), XGBoost, and Support Vector Machine (SVM), for fraud detection in the financial and healthcare sectors. It is evaluated using key performance metrics, including Precision, Recall, F1-Score, Accuracy, and ROC-AUC.

Random Forest and XGBoost performed almost equally well in financial fraud detection, achieving nearly perfect results across all metrics, with each achieving 99.98% accuracy. These models demonstrated high accuracy, recall, and F1 Scores, making them reliable for detecting fraudulent deals and limiting false positives. SVM also ran well but showed slight limitations at edges, as evidenced by a lower accuracy of 99.82%. The three models achieved

ROC-AUC scores of 1.00, indicating strong separation between legitimate and fraudulent transactions (Figures 4 and 5).

In the healthcare fraud case, the expected accuracy of the models is 98.42%, and the Random Forest achieved the best results, with a precision and recall of 0.9850, an F1-score of 0.9825, and an accuracy of 98.42%. The number of false positives and false negatives was kept at a subsistence level, thereby making it dependable in this field. XGBoost was the second, with a precision of 0.9725, a recall of 0.97, an F1-Score of 0.97, and an ROC-AUC score of 0.99, indicating that it is a strong discriminative model that successfully separates fraudulent and legitimate cases. Conversely, SVM did not perform as well as the ensemble approaches, achieving a precision, recall, and F1-score of 0.8025, 0.8075, and 0.8050, respectively. It had much lower accuracy at 0.8096, indicating more incorrect classifications. Although the SVM ROC of 0.95 indicated good ranking performance, the model's overall performance was poor (Figures 6 and 7). Detecting fraud in health care poses specific challenges, as the information can be complex and uneven, encompassing not only billing history but also patient history and provider behaviour, further complicating the process.

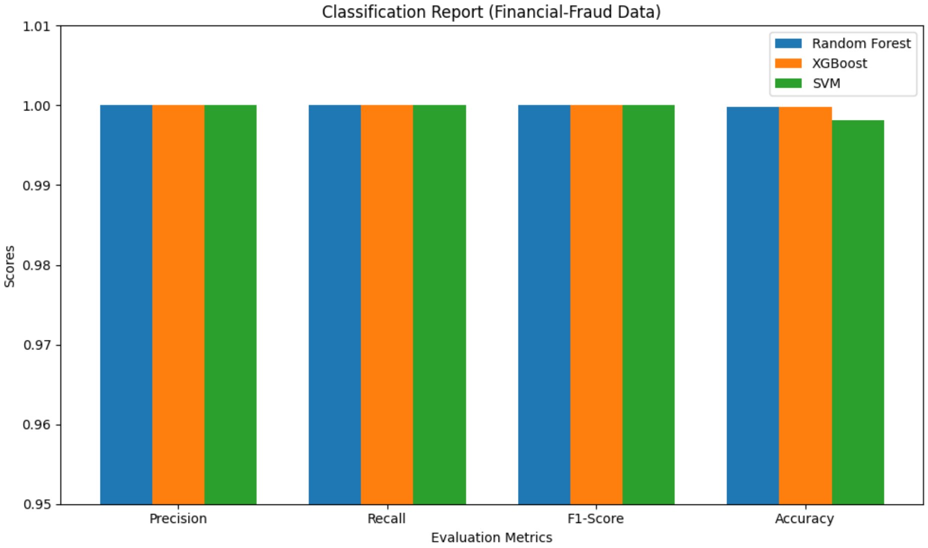

Fig. 4 Evaluation Metrics for Financial Fraud Detection

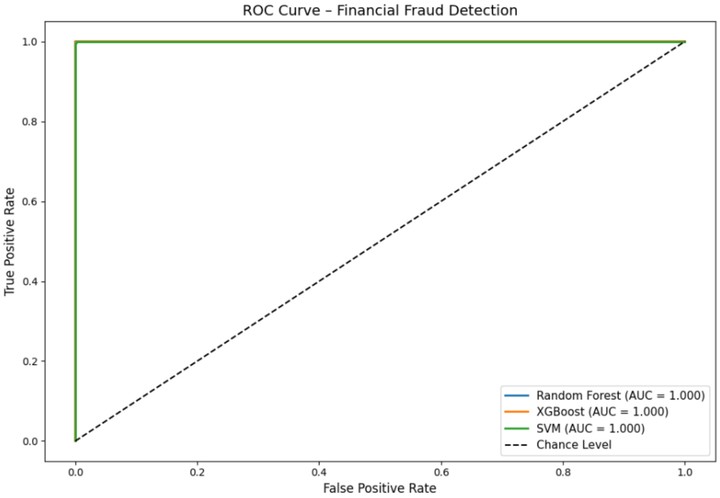

Fig. 5 ROC-AUC for Financial Fraud Detection

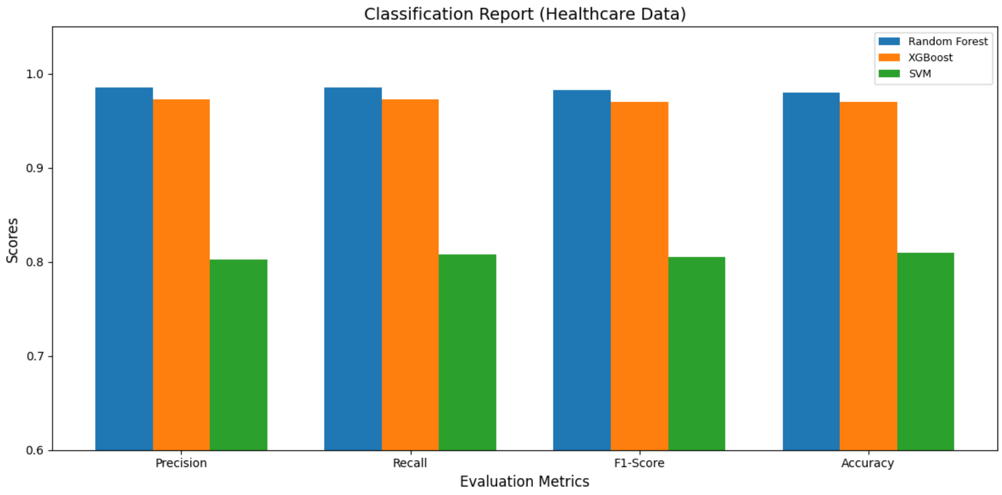

Fig. 6 Evaluation Metrics for Healthcare Fraud Detection

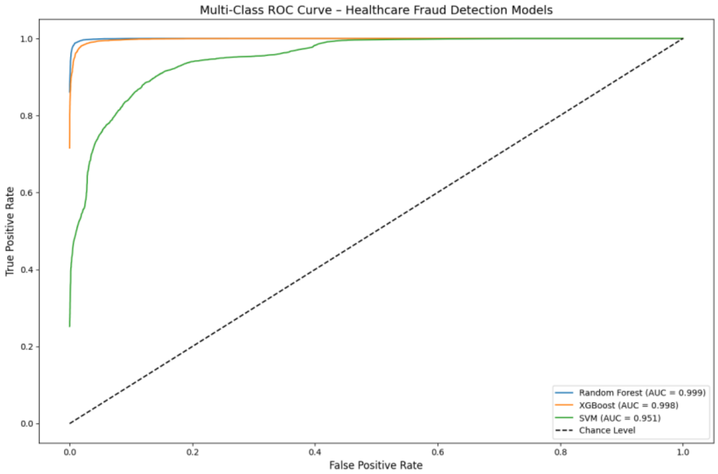

Fig. 7 ROC-AUC for Healthcare Fraud Detection

C. Comparative Performance Across Domains

The results of machine learning models are highly dependent on the field and data complexity, as reflected in comparing Table 2 (Financial Fraud Detection) and Table 3 (Healthcare Fraud Detection).

All three models have scores in all metrics in the field of financial fraud detection (Table 2). Random Forest has impeccable precision, recall, F1-score, and ROC-AUC (all equal to 1.00), with only a statistically insignificant difference in accuracy (0.9998 vs 0.9982 with SVM). This high performance indicates a high level of organisation and comparatively less noise in financial fraud datasets, allowing models to classify transactions as fraudulent or legitimate easily. Such slight variance across the models demonstrates that even more basic algorithms, like SVMs, would perform remarkably well with clean, well-defined data.

TABLE 2
MODEL PERFORMANCE SUMMARY FOR FINANCIAL FRAUD DETECTION

Model	**Precision**	**Recall**	**F1-Score**	**Accuracy**	**ROC-AUC**
RF	1.00	1.00	1.00	0.9998	1.00
XGBoost	1.00	1.00	1.00	0.9998	1.00
SVM	1.00	1.00	1.00	0.9982	1.00

The healthcare fraud sector (Table 3) is more challenging, in contrast to the lower performance indicators in all the models. Random Forest has the highest scores, with a precision and recall of 0.9850, an F1-score of 0.9825, an accuracy of 0.9842, and a high ROC-AUC of 0.99. XGBoost comes in second with less precision, recall, and accuracy (0.9725 and 0.9731, respectively). Nevertheless, SVM is significantly inferior, with precision, recall, F1-score, and accuracy of 0.80, 0.80, 0.8050, and 0.8096, respectively. The SVM ROC-AUC score of 0.95 is average but still weaker than that of the ensemble methods. These findings suggest that healthcare fraud data is more intrinsically complex, noisy, and dimensional, and more challenging to achieve the same performance as with financial fraud detection.

TABLE 3
MODEL PERFORMANCE SUMMARY FOR HEALTHCARE FRAUD DATASET

Model	**Precision**	**Recall**	**F1-Score**	**Accuracy**	**ROC-AUC**
RF	0.9850	0.9850	0.9825	0.9842	0.99
XGBoost	0.9725	0.9725	0.97	0.9731	0.99
SVM	0.8025	0.8075	0.8050	0.8096	0.95

V. Discussion

Random Forest (RF) and XGBoost performed well across all metrics, including precision, recall, F1-score, accuracy, and ROC-AUC, in the field of financial fraud [1]. This performance is credited to the fact that the data on the financial transactions is structured and comparatively clean. The financial dataset PCA-transformed characteristics have probably played a role in the facility with which the models detected fraudulent and legitimate transactions [17]. The results of RF, XGBoost, and SVM demonstrate the power of these algorithms when working with clear datasets. The accuracy of SVM has declined minimally (0.9982 vs. 0.9998) with RF and XGBoost; however, this indicates that ensemble methods are more effective at maintaining consistency in edge cases [8, 49].

On the contrary, healthcare fraud detection was much harder, and Random Forest and XGBoost scored much higher than their counterparts in financial fraud detection. RF showed the best results in terms of precision and recall (0.9850), F1-score (0.9825), and accuracy (0.9842). XGBoost showed slightly lower precision, recall, and accuracy (0.9725 and 0.9731, respectively). SVM performed very poorly, with a precision, recall, F1-score, and accuracy of about 0.80, 0.80, 0.8050, and 0.8096, respectively. Such findings are consistent with the literature, which notes the complexity and noise inherent in healthcare data, such as billing data, patient histories, and provider behaviour [4, 50]. The increased dispersion of the anomaly scores in health care fraud (illustrated in Figure 8) further explains why models struggle to achieve the same level of performance as in financial fraud detection [14].

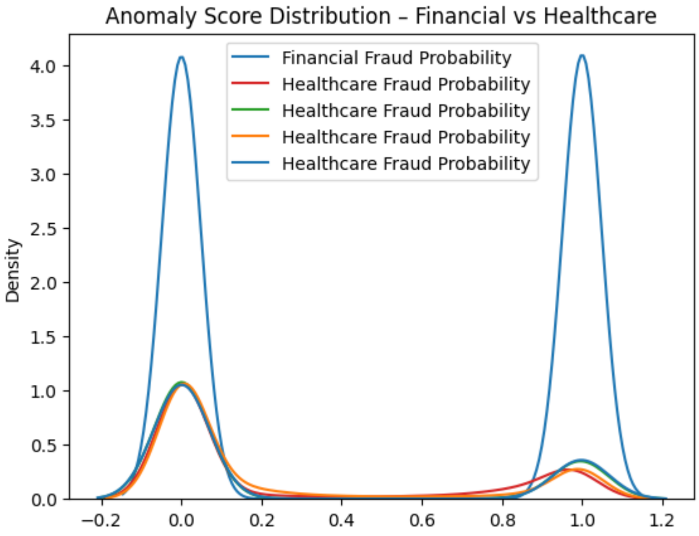

Fig. 8 Anomaly Score Distribution – Financial vs. Healthcare

A. High-Risk System Activity Anomalies

Although this study did not explicitly address this, the theoretical background and gaps suggest that high-risk system activity abnormalities can pose additional challenges because they are dynamic and rapidly evolving [45]. The multidimensional behaviour deviations generated by cybersecurity logs, IoMT networks, and wireless body-area systems need to be addressed by detecting behavioural anomalies in real time [11]. Reducing these issues with advanced AI-based intrusion detection systems that use LSTM, RCLNet, and autoencoders has demonstrated potential [51]. Further research into the comparability of these methods across the financial and healthcare sectors should be conducted to develop a single framework for anomaly detection [19].

B. Cross-Domain Insights

The difference in model performance between the financial and healthcare fields underscores the importance of domain-specific feature engineering and model adoption [9]. Structured data and distinct patterns are helpful for financial fraud detection, whereas noisy, high-dimensional data with complex relationships are helpful for healthcare fraud detection [43]. The Python architecture used in the research supports a high level of analytical reliability by integrating computational scalability and statistically validated methods, and it provides a repeatable approach to cross-domain fraud analytics [3].

C. Theoretical Contributions

The research contributes to theoretical knowledge of anomaly detection by confirming major theories, including Anomaly Detection Theory, Fraud Triangle Theory, and Behavioural Pattern Deviation Theory [22]. The observation of similar performance of the ensemble approach across various fields favours the hypothesis that an anomaly leaves visible traces in modelled data but becomes more difficult to detect in a data-rich setting [23]. Additionally, explanations of artificial intelligence (XAI) methods, such as SHAP and LIME, improve transparency and interpretability, which is significant in regulated industries, such as finance and health care [14]. Resistance to adversarial attacks is also a valuable feature, as fraudsters exploit the vulnerabilities of AI models, particularly in decentralised finance and IoT-based healthcare [20].

VI. CONCLUSIONS

The research fills significant gaps in the literature by conducting cross-domain empirical research on AI-powered anomaly detection systems in the financial transaction sector, fraud in healthcare claims, and risky system events. The results indicated that AI models (Random Forest, XGBoost) are effective at identifying financial fraud cases when provided with organised, clean data. On the other hand, healthcare fraud detection is more difficult and requires more powerful feature engineering and algorithms to support the management of healthcare information. Anomalies in system activities related to high-risk systems are not yet a researched field, but have high potential for future studies. This study examines the generalizability and limitations of AI models across various domains by comparing financial and healthcare fraud detection. By using Python-based machine learning, a sound methodology for fraud analytics is developed to ensure a high degree of both computational accuracy and statistical rigour. These findings can be utilised by policymakers, auditors, and IT experts to create efficient fraud detection systems that meet regulatory requirements, including the EU AI Act, without affecting system performance.

A. Limitations and Future Work

Irrespective of the contributions, this study has some limitations. First, publicly available datasets might be biased toward the true complexities of the real world. The prospective studies are to involve proprietary or real-time data to increase external validity. Second, the research focused on supervised learning methods; unsupervised and semi-supervised methods may offer further insights in this field, particularly for identifying high-risk system activity. Lastly, the concept of adversarial resilience is a subject that requires further investigation, as the number of cases in which fraudsters exploit AI model vulnerabilities continues to grow [20].

As digital ecosystems continue to evolve, the need for adaptive, scalable AI-based fraud detection systems is becoming increasingly acute. The current research lays the foundations for creating single frameworks that address the specific issues in the financial, healthcare, and cybersecurity spheres. It helps close the gap between theory and practice and paves the way for more convenient, transparent, and robust fraud detection strategies in the era of artificial intelligence [52].

Author Contributions: *[First Author]*: Conceptualisation, Methodology, Writing - Original Draft, Writing - Review & Editing, Supervision. *[Second Author]*: Software, Investigation, Data Curation, Writing - Original Draft. *[Third Author]*: Investigation, Data Curation. (A short paragraph specifying the author's contributions must be

provided. Please use the CRediT taxonomy to write this part). – This statement is mandatory.

All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by [Sponsor name] under [Research grand name] Grand number xxx. / This research received no specific grant from any funding agency. **-** this statement is mandatory.

Acknowledgments: You may recognise other people who contributed to the article or data contained in the article, but at a level of effort that does not justify their inclusion as authors. – this statement is optional; you may delete this part.

Conflicts of Interest: The authors declare no conflict of interest. / The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: [First Author] reports financial support was provided by [Sponsor name]. [First Author] report a relationship with [Sponsor name] that includes: employment. No other potential conflict of interest relevant to this article was reported. / First Author is member of Editorial Teams, but had no role in the decision to publish this article. No other potential conflict of interest relevant to this article was reported.   – this statement is mandatory.

Data Availability: Your statement should explain the accessibility of the data and/or source code that underlie the results presented in your paper. If it is stored in a repository, please provide hyperlinks whenever possible. In cases where it cannot be openly shared, such as for the protection of study participant privacy, it is essential to explain this restriction clearly. – this statement is mandatory.

Informed Consent: There were no human subjects. / Informed Consent was obtained, and a detailed explanation was presented in the Methods section. / The consent cannot be obtained; *Providing an explanation is necessary, and the text should include a description of an alternative process that has received ethical approval and should be followed.* – this statement is mandatory.

Institutional Review Board Statement: Not applicable. / This study received ethical approval from the NAME OF INSTITUTE Research Ethics Committee (approval no. XYZ123) on Month DD, YYYY.

Animal Subjects: There were no animal subjects. / This research involved animal subjects and it complies with ARRIVE guidelines. / This research involved animal subjects but did NOT comply with ARRIVE guidelines, *Kindly provide a rationale for why your research did not adhere to the ARRIVE guidelines.* – this statement is mandatory.

ORCID:
First Author: https://orcid.org/0000-0002-0622-3374
Second Author: https://orcid.org/0000-0002-8560-8626
Third Author: **-**

REFERENCES

[1] A. Ali, “Financial fraud detection based on machine learning: A systematic literature review,” *Applied Sciences*, vol. 12, no. 19, 2022, doi: 10.3390/app12199637.

[2] M. N. U. Milon, “Gravitating towards artificial intelligence on anti-money laundering: A PRISMA based systematic review,” *International Journal of Religion*, vol. 5, no. 7, pp. 303–315, 2024, doi: 10.61707/py0fe669.

[3] D. Wiryadinata, A. Sugiharto, and T. Tarno, “The use of machine learning to detect financial transaction fraud: Multiple Benford Law model for auditors,” *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 239–252, 2023, doi: 10.20473/jisebi.9.2.239-252.

[4] Q. He et al., "A data-driven intelligent supervision system for generating high-risk organised fraud clues in medical insurance funds," *Electronics*, vol. 14, no. 16, p. 3268, 2025, doi: 10.3390/electronics14163268.

[5] E. Nabrawi and A. Alanazi, “Fraud detection in healthcare insurance claims using machine learning,” *Risks*, vol. 11, no. 9, p. 160, 2023, doi: 10.3390/risks11090160.

[6] M. Thilagavathi et al., “AI-driven fraud detection in financial transactions with graph neural networks and anomaly detection,” in *Proc. IEEE*, 2024, doi: 10.1109/icstem61137.2024.10560838.

[7] N. E. Ellahi, "Fraud detection and prevention in finance: Leveraging artificial intelligence and big data," *Journal of Ballistics*, vol. 36, no. 1, pp. 54–62, 2024, doi: 10.52783/dxjb.v36.141.

[8] V. D. Akhare and L. K. Vishwamitra, "Machine learning models for fraud detection: A comprehensive review and empirical analysis," *Journal of Electrical Systems*, vol. 20, no. 3s, pp. 1138–1149, 2024, doi: 10.52783/jes.1427.

[9] Z. Z. Darban, G. I. Webb, S. Pan, C. Aggarwal, and M. Salehi, "Deep learning for time series anomaly detection: A survey," *ACM Computing Surveys*, 2024, doi: 10.1145/3691338.

[10] B. R. Ande, "Federated learning and explainable AI for decentralised fraud detection in financial systems," *Journal of Information Systems Engineering and Management*, vol. 10, no. 35s, pp. 48–56, 2025, doi: 10.52783/jisem.v10i35s.5921.

[11] J. A. Shaikh et al., "RCLNet: An effective anomaly-based intrusion detection for securing the IoMT system," *Frontiers in Digital Health*, vol. 6, 2024, doi: 10.3389/fdgth.2024.1467241.

[12] A. H. Ali and A. A. Hagag, "An enhanced AI-based model for financial fraud detection," *International Journal of Advanced and Applied Sciences*, vol. 11, no. 10, pp. 114–121, 2024, doi: 10.21833/ijaas.2024.10.013.

[13] R. Rawat et al., "Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments," *Informatica*, vol. 47, no. 9, 2023, doi: 10.31449/inf.v46i9.4538.

[14] P. Thanathamathee et al., "SHAP-instance weighted and anchor explainable AI: Enhancing XGBoost for financial fraud detection," *Emerging Science Journal*, vol. 8, no. 6, pp. 2404–2430, 2024, doi: 10.28991/esj-2024-08-06-016.

[15] S. Masengo Wa Umba, A. M. Abu-Mahfouz, and D. Ramotsoela, "Artificial intelligence-driven intrusion detection in software-defined wireless sensor networks," *International Journal of Environmental Research and Public Health*, vol. 19, no. 9, p. 5367, 2022, doi: 10.3390/ijerph19095367.

[16] National Health Insurance Service, "NHIS health insurance claims fraud dataset," Kaggle, 2024. [Online]. Available: https://www.kaggle.com/datasets/bonifacechosen/nhis-healthcare-claims-and-fraud-dataset

[17] N. Elgiriyewithana, "Credit card fraud detection dataset 2023," Kaggle, 2023. [Online]. Available: https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023

[18] E. Hariyanti et al., "Implementations of artificial intelligence in various domains of IT governance: A systematic literature review," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 305–319, 2023, doi: 10.20473/jisebi.9.2.305-319.

[19] K. Kalodanis et al., "A privacy-preserving and attack-aware AI approach for high-risk healthcare systems under the EU AI Act," *Electronics*, vol. 14, no. 7, p. 1385, 2025, doi: 10.3390/electronics14071385.

[20] M. Gupta et al., "Adversarial attacks and fraud defenses: Leveraging data engineering to secure AI models," *Nanotechnology Perceptions*, pp. 1196–1222, 2024, doi: 10.62441/nano-ntp.vi.4706.

[21] B. Luo et al., "AI-powered fraud detection in decentralised finance: A project life cycle perspective," *ACM Computing Surveys*, vol. 57, no. 4, 2024, doi: 10.1145/3705296.

[22] J. Chaquet-Ulldemolins et al., "Non-linear analysis through interpretable autoencoders for fraud detection," *Applied Sciences*, vol. 12, no. 8, p. 3856, 2022, doi: 10.3390/app12083856.

[23] C. Macrae, "Managing risk and resilience in autonomous and intelligent systems," *Risk Analysis*, 2024, doi: 10.1111/risa.14273.

[24] G. Pavlidis, "Deploying artificial intelligence for anti-money laundering and asset recovery," *Journal of Money Laundering Control*, vol. 26, no. 7, pp. 155–166, 2023, doi: 10.1108/jmlc-03-2023-0050.

[25] Y. Zhang et al., "Multivariate time series anomaly detection in financial risk assessment," *Journal of Organizational and End User Computing*, vol. 36, no. 1, pp. 1–19, 2024, doi: 10.4018/joeuc.342094.

[26] A. Ruchay et al., "Imbalanced classification of fraudulent bank transactions using machine learning," *Mathematics*, vol. 11, no. 13, p. 2862, 2023, doi: 10.3390/math11132862.

[27] H. Du et al., "A novel method for detecting credit card fraud problems," *PLOS ONE*, vol. 19, no. 3, e0294537, 2024, doi: 10.1371/journal.pone.0294537.

[28] Z. Ahmed, S. S. Shanto, and A. I. Jony, "Advancement in Bangla sentiment analysis," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 181–194, 2023, doi: 10.20473/jisebi.9.2.181-194.

[29] [R. Ming et al., "Enhancing fraud detection in auto insurance and credit card transactions using CNNs," *PeerJ Computer Science*, vol. 10, e2088, 2024, doi: 10.7717/peerj-cs.2088.

[30] R. Udayakumar et al., "Integrated SVM-FFNN for fraud detection," *Journal of Internet Services and Information Security*, vol. 13, no. 4, pp. 12–25, 2023, doi: 10.58346/jisis.2023.i4.002.

[31] K. Vermani et al., "Malicious node detection in SDN-based VANETs," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 136–146, 2023, doi: 10.20473/jisebi.9.2.136-146.

[32] W. Winanti and E. Fernando, "Brand image and trust in the adoption of FinTech digital payment," *Journal of Information Systems Engineering and Business Intelligence*, vol. 10, no. 1, pp. 126–138, 2024, doi: 10.20473/jisebi.10.1.126-138.

[33] V. H. P. Ranatawijaya, N. Noor, R. A. Rahman, E. Christian, and S. Geges, "Unveiling user sentiment: Aspect-based analysis and topic modeling of ride-hailing and Google Play app reviews," *Journal of Information Systems Engineering and Business Intelligence*, vol. 10, no. 3, pp. 328–339, 2024, doi: 10.20473/jisebi.10.3.328-339.

[34] K. Pelechrinis, X. Liu, P. Krishnamurthy, and A. Babay, "Spotting anomalous trades in NFT markets: The case of NBA Topshot," *PLOS ONE*, vol. 18, no. 6, e0287262, 2023, doi: 10.1371/journal.pone.0287262.

[35] A. S. Nurqamarani, S. Fadilla, and A. Juliana, "Revolutionising payment systems: The integration of TRAM and trust in QRIS adoption," *Journal of Information Systems Engineering and Business Intelligence*, vol. 10, no. 3, pp. 314–327, 2024, doi: 10.20473/jisebi.10.3.314-327.

[36] M. Alamri and M. Ykhlef, "Survey of credit card anomaly and fraud detection using sampling techniques," *Electronics*, vol. 11, no. 23, p. 4003, 2022, doi: 10.3390/electronics11234003.

[37] M. Ankita, "Credit risk assessment and fraud detection in financial transactions using machine learning," *Deleted Journal*, vol. 20, no. 3s, pp. 2061–2069, 2024, doi: 10.52783/jes.1807.

[38] J. Hawayek and O. AbouElKhir, "Problems with medical claims that artificial intelligence (AI) and blockchain can fix," *Blockchain in Healthcare Today*, vol. 6, 2023, doi: 10.30953/bhty.v6.273.

[39] C. Chakraborty, S. M. Nagarajan, G. G. Deverajan, T. V. Ramana, and R. Mohanty, "Intelligent AI-based healthcare cyber security system using multi-source transfer learning," *ACM Journal*, 2023, doi: 10.1145/3597210.

[40] D. Jadav et al., "A trustworthy healthcare management framework using amalgamation of AI and blockchain network," *Mathematics*, vol. 11, no. 3, p. 637, 2023, doi: 10.3390/math11030637.

[41] E. Flondor, L. Donath, and M. Neamtu, “Automatic card fraud detection based on decision tree algorithm,” *Applied Artificial Intelligence*, vol. 38, no. 1, 2024, doi: 10.1080/08839514.2024.2385249.

[42] S. Mahabub, B. C. Das, and M. R. Hossain, “Advancing healthcare transformation: AI-driven precision medicine and scalable innovations,” *Edelweiss Applied Science and Technology*, vol. 8, no. 6, pp. 8322–8332, 2024, doi: 10.55214/25768484.v8i6.3794.

[43] M. Ferrara et al., “Risk management and patient safety in the artificial intelligence era: A systematic review,” *Healthcare*, vol. 12, no. 5, p. 549, 2024, doi: 10.3390/healthcare12050549.

[44] H. W. Awalurahman, I. H. Witsqa, I. K. Raharjana, and A. H. Basori, “Security aspect in software testing perspective: A systematic literature review,” *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 1, pp. 95–107, 2023, doi: 10.20473/jisebi.9.1.95-107.

[45] M. A. Rassam, “Autoencoder-based neural network model for anomaly detection in wireless body area networks,” *IoT*, vol. 5, no. 4, pp. 852–870, 2024, doi: 10.3390/iot5040039.

[46] M. E. Ward et al., “A systems approach to managing the risk of healthcare-acquired infection supported by human factors, data science, data governance and AI,” *Ergonomics*, pp. 1–19, 2024, doi: 10.1080/00140139.2024.2396527.

[47] H. Yaseen and A. Al-Amarneh, “Adoption of artificial intelligence-driven fraud detection in banking,” *Journal of Risk and Financial Management*, vol. 18, no. 4, p. 217, 2025, doi: 10.3390/jrfm18040217.

[48] A. Arega and D. P. Sharma, “Towards smart and green features of cloud computing in healthcare services: A systematic literature review,” *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 161–180, 2023, doi: 10.20473/jisebi.9.2.161-180.

[49] M. Maashi, B. I. Alabduallah, and F. Kouki, “Sustainable financial fraud detection using Garra Rufa Fish optimisation with ensemble deep learning," *Sustainability*, vol. 15, no. 18, p. 13301, 2023, doi: 10.3390/su151813301.

[50] M. K. A. Ismaeil, “Harnessing AI for next-generation financial fraud detection,” *Journal of Ecohumanism*, vol. 3, no. 7, pp. 811–821, 2024, doi: 10.62754/joe.v3i7.4248.

[51] W. Maharani, H. Daud, N. Muhammad, and E. A. Kadir, “Leveraging social media data for forest fires sentiment classification,” *Journal of Information Systems Engineering and Business Intelligence*, vol. 10, no. 3, pp. 392–407, 2024, doi: 10.20473/jisebi.10.3.392-407.

[52] Raja, “AI in fraud detection: Evaluating the efficacy of artificial intelligence in preventing financial misconduct,” *Deleted Journal*, vol. 20, no. 3s, pp. 1332–1338, 2024, doi: 10.52783/jes.1508.

Publisher’s Note: Publisher stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.