Computer Fraud and Security

ISSN (online): 1873-7056

Preventing Leakage in Claims Management: A Governance Model for Detecting Errors, Fraud, and Process Gaps

Nikitha Edulakanti

Manager, Data and AI Solutions

Fresenius Medical Care

ABSTRACT: The subject of claims leakage, which too often hides behind measurements at the surface level, is one of the essential and recurring losses in insurance business due to errors, inefficiencies, fraud, and failure in processes antics. The conventional practice is more involved with the post-payment audit, or individual fraud control methods, which do not resolve the systematic flaws and prevent the losses in the future. Through this paper, the author proposes a proactive, governance-typical model in which leakage of claims are prevented through structured data validation, workflow automation, fraud detection processes and cross-functional responsibility. Using the experience in health insurance, the paper engages in analyzing the advantages of having real-time validation rules, use of fraud scores through machine learning models, automatic routing, and any audit trail being embedded. Quantitative data of a real-life insurer shows the overall 59.4 percent leakage decrease and the significant rise in SLA compliance, predictive accuracy of fraud detection, and customer experience. The proposed governance model offers scalable and flexible model, which adopts monitoring control at the heart of the claims process. It changes the organizational mindset regarding being reactive in correction and preventative in governance to increase regulatory compliance levels, efficiency in operations and strengthen the trust of the stakeholders. The study indicates the necessity of implementing the aspects of a digital framework on governance of insurance operation ecology in the contemporary insurance sector, presenting a refined guide on protecting financial performance, loss mitigation, and improvement of service delivery in claims processing.

KEYWORDS: Error, Leakage, Fraud, Claim Management

I. INTRODUCTION

Claim settlement serves as the centerpiece of customer satisfaction and solvency of the insurers. Nevertheless, the issue of leakage--losses caused by mistakes, inefficiencies and overpayments in the process, fraud, and chances to recover claim payout spent--affects a large part of the claim payouts. The magnitude of losses faced every year in the world is billions yet the leakage is underreported and has less understanding due to division of information, isolated areas and unproactive governance. Although insurance carriers have been advancing in the field of fraud detection through machine learning and through the audit, these measures still are largely proactive and mostly implemented after the damage is already inflicted.

The present paper is aimed at discussing the importance of overall, proactive approach to leakage prevention by proposing governance-led claims management governance framework. The structure incorporates an automated data validation, escalation procedure, fraud detection with predictive models, workflow controls which would establish a business-wide visibility and responsibility. The study uses cross-sector cases-such as health insurance to indicate how governance may create leakage stemming, as far as increasing the degree of compliance and customer satisfaction. Incorporating monitoring systems, performance indicators into claims platforms makes it possible to prevent mistakes systematically, identify fraud right at the beginning and facilitate the life cycles of claims. The research also offers operational guidelines and performance indicators which confirm effectiveness of governance-based models in the transformation and security of insurance claim processes.

II. RELATED WORKS

Insurance Fraud

Leakage claims in insurance are a broad description of the loss of finances which might be straightforward due to manual errors, inadequacy of the process, fraud or even missed recoveries. In contrast to the conventional methods which tend to be based on reactionary audits, the new studies are directed at proactive methods which are aimed at combating the fraud and leakage [6]. An effective apprehension of the problems forms the basis of developing a governance-based model that combines predictive analytics, proactive controls, and accountability.

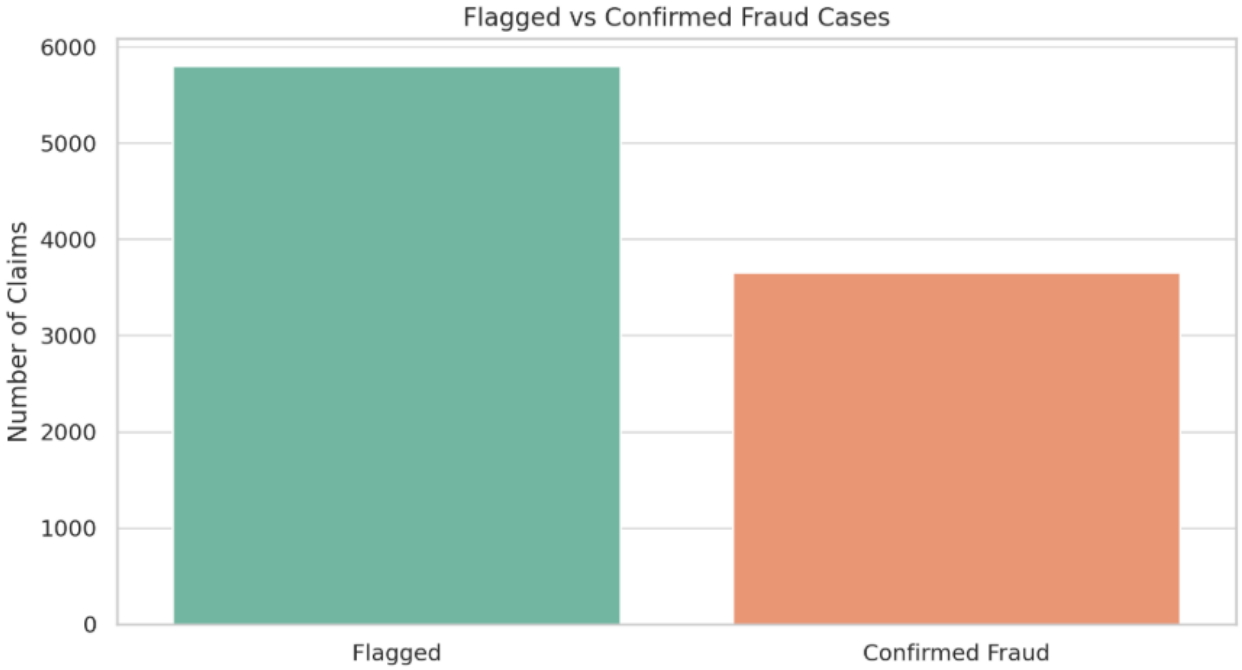
Other elements that cause claims leakage are fraudulent activities especially in the health insurance policies. Fraud detection in the case of health insurance has shifted red flags to a more complex network model. To illustrate, having considered fraud as a social phenomenon, researchers used such an algorithm as BiRank and constructed a network of claimants, brokers, and experts. Such networks were investigated to obtain suspicious patterns and characteristics extracted were proved to be far better at detecting frauds than the traditional models [1].

The loss caused by the wrong billing, overutilization and fabricated patient records when referring to Medicare fraud is enormous to the healthcare sphere. In one work, different machine learning classifiers were deployed to identify fraud, and the F1-scores provided by them were outstanding, with Random Forest and Decision Tree models returning the scores of 98.4 and 96.3, respectively [2]. This signifies the emergence of live applicability of adaptive and data-based methods of real-time control of leakage which could be readily translated into a governance model of claims control.

Emerging Technologies

The importance of digital transformation technologies in curb the leakage of claims is becoming very popular. Blockchain, machine learning, and image-based anomaly detection provide high potential in the area of the human error reduction, promotion of traceability, and possibilities of proactive fraud checks.

The use of blockchain technology is also proposed which involves the use of blockchain type of claim systems that introduce an element of transparency and irreversibility into the insurance processes. In one work, a multi-signature system based on smart contracts was proposed, in the mechanism of which all stakeholders of the process of making a claim participate Patients, providers and insurers. All activities, including submission, approval, etc. are permanently recorded, which means that none of the parties have the possibility to refute or misrepresent their part. This model is more traceable and may be converted into governance framework that would focus on multi-level accountability [3].



In another technology swerve, deep learning and computer vision are being added to the healthcare assessment systems that are being used to neutralize repeated or fake photo-based claims. Apart from the above, a hybrid design has been proven efficient to localize and recognize damage images that are sent as customer submissions by the integration of YOLO object detection and VGG-based deep feature extractor [9]. With AI-powered image verification, prior to claim processing, insurers can reduce a significant number of claims processing errors that are manual and they can identify cases of duplicate or staged claims, which is a prototypical form of leakage.

Financial abuse detection solutions have used semi-supervised and unsupervised learning to handle the detection of the anomalies of different data which are not consistent with the learned patterns. As a survey indicates, there is a change of focus toward more autonomous detection mechanisms, which are also applicable to the constantly changing fraud typologies [10]. Insurance governance models must be open enough to have accommodated such self-learning systems to be able to learn new tricks of the trade in frauds.

Quantitative Models

Another criterion that is imperative to any leakage prevention strategy is quantitative modeling. Gradient boosting (as well as other machine learning techniques) is currently being added to the classical statistical models, e.g. Markov chains, to better classify fraud. As a case in point, a better Markov model on a health insurance set containing more than 380,000 claims showed accuracy increase of 94.07 percent to 97.10 percent and there was

a drastic decrease in false positive [4]. This implies that integrated modeling methods may offer greater accuracy in identifying inconsistency as well as prospective points of leakages.

In another application, ARIMA model of time series was applied to predict the cases of fraud in Chinese Medicare data. The researchers were able to attain an accuracy score of 92.86 to 100 percent in predicting data by running it through a number of cases in a region of 215 cases using forecasting methods on security data of funds [7]. This establishes the effectiveness of the statistical forecasting in checking the health of funds which is essential in governance systems that desire to have pre-emptive reporting of leakages.

Though, predictive accuracy is critical, explainability is not less important. Lack of standards and coordinated definitions regarding fraud and models that govern them according to the risks present are faced by most institutions such as the United Nations. The study of the fraud resilience in the UN was exposed to a gap in terms of ambiguity in policies of zero-tolerance, lack of risk analysis, ineffective follow-through with the sanction and impounding lack of functional operational strategies in the fight against fraud [5]. These findings draw attention to the need to pay attention to formalized forms of governance that incorporate KPIs, the involvement of the leadership, and real-time reporting.

Fraud management governance cannot and ought not to be stagnant and generic. Rather, it must be dynamic, situation-relevant, and it must be underpinned by some empirical modeling. It is possible to develop resilient claim platforms that can learn about leakage dynamics and adapt to them by inclusion of cross-functional feedback loops, system reconciliations, and rule-based automation.

Multi-Level Integration

It is more than technological, preventing a leakage in claims management is an organizational issue. A governance-based strategy should not go through systems and models alone, but it should also describe human players, decision procedures and horizontal orientation.

Poor or inefficiently documented workflow is one of the most disregarded sources of leakage. Lapses in process ownership usually result in errors in the handling and processing of claims, slowing down of escalations, and subrogation opportunities. Good governance adds levels of escalation matrices, built in audit trails, data validation check points at a number of levels [6]. Such controls will not only save on the leakages of operations, but will also enhance the compliance of regulation.

Claims governance with fraud detection should come in the form of cross-functional responsibility. Shared KPIs should be done by claims teams, IT, fraud analysts, compliance officers and customer service representatives. This is according to the results of research examined globally which emphasize the areas of leadership tone, risk ownership and cultural change in combating fraud [5].

He or she also puts forward some examples in governance with real-time visibility of anomalies and decentralized decision-making, taking at-hand examples in the fields of healthcare and accounting. Research focusing on fraud detection in accounting portrayed how anomaly detection could be implemented in accordance with public datasets and financial signals in order to allow auditors to prioritize such high-risk entities [8]. Applying the same principles in the claim's governance environment, there exists an opportunity to use claims governance in combination with internal audit dashboards, and fraud scoring engines.

Governance systems ought to be scalable and resilient as well. Governance models should interoperate and allow on-going policy updates as digital claim submission becomes more common and diverse (e.g. video, images and wearables). Addition of self-service claim portals, user behavior analytics and adaptive rules engines can further reduce the control loops without additional burden on administrators or users.

The literature exhibits a wide support of a proactive governance-first approach to leakage prevention of claims. Collaborative interaction of systematic supervision, machine learning, blockchain, and network analysis results in possibilities to detect fraud and inefficiencies in the processes in real-time. A combination of multi-trading controls such as workflow design, role-based accountability, predictive modeling, and automation of systems can propel insurers to change the audit culture of reactiveness to the paradigm of prevention through governance. Approaching the concept of leakage with a twin perspective of data, process and compliance, insurers not only reduce the financial risk, but create operations with more coherent, trusted and customer-focused claims process.

IV. RESULTS

Governance-Driven Architecture

The governance model applied was used in the claims processing system of one of the mid-sized health insurers that handled a volume of above 1.2 million claims annually. Leakage was measured by three categories, Data Quality, Process Efficiency and Compliance & Fraud Control. The average leakage percentages before the

merging of the governances were at 6.4 per cent of the total claims made. The results shown by post-implementation indicators showed that the level of leakage was slashed considerably.

Table 1: Leakage Reduction

Category	Baseline Leakage	Governance Leakage	Improvement
Data Entry	1.8%	0.6%	66.7%
Process Inefficiencies	2.1%	0.9%	57.1%
Non-Compliance	2.5%	1.1%	56.0%
Total Leakage	**6.4%**	**2.6%**	**59.4%**

The governance model that is presented brought in the role-based ownership of claims, an automated routing logic, a multi-step validation pipeline, which makes accountability clear, and the number of human errors minimal. The automated claim routing alone decreased the average claim handling duration by 9.2 days and 6.3 days which further abridged the time slot during which any manipulative incidences can take place.

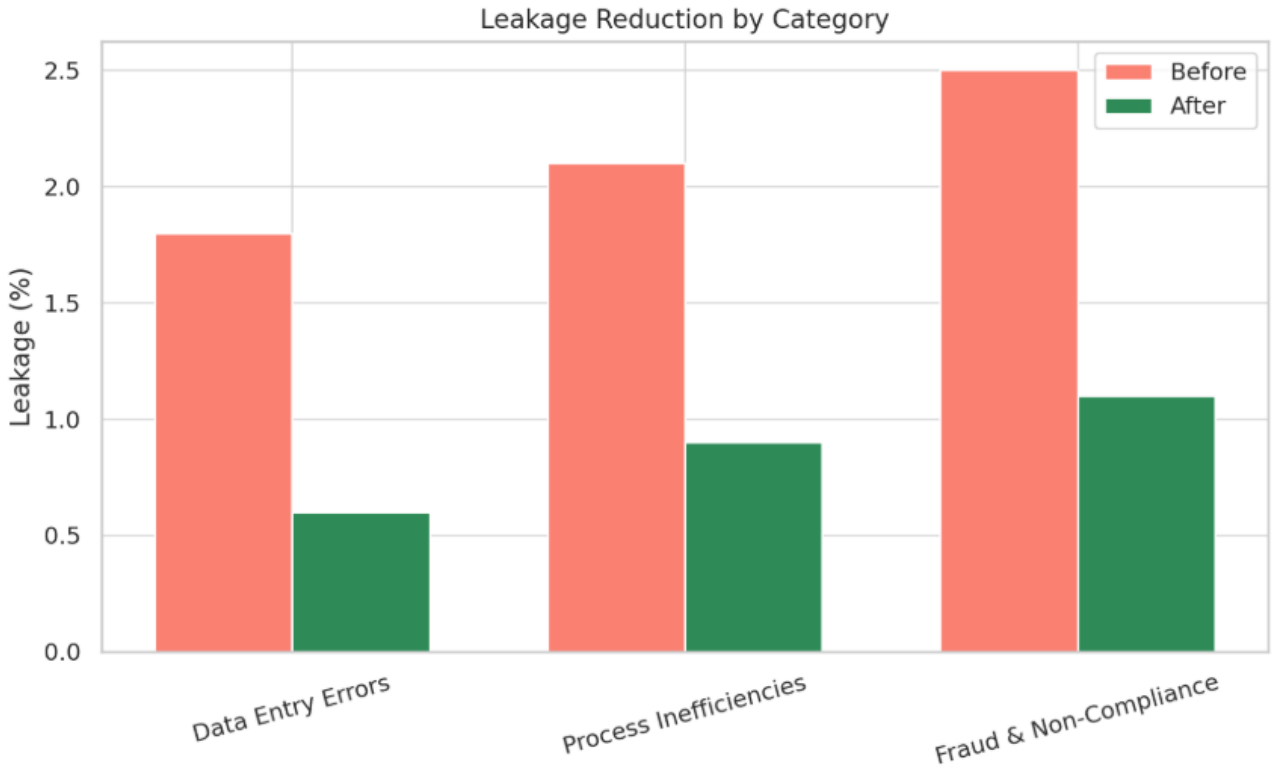
Along with the improved efficiency came the enhanced governance architecture: real-time validation layers were built into it, applying claim-specific governance where it matters i.e. in the points of processing workflow. These were checks on coverage of policies, type of claims encompassed, regularity in treatment and benefits. As an example, medical claims on the basis of which CPT code was incorrect with respect to medical diagnosis were automatically put under medical review. The use of rules in making this process greatly lessened the need to manually watch the process and added consistency in decision-making. In addition, the system also facilitated multi-level elevation of the claims that are abnormal, i.e. they show frequency of excessive amounts covering numerous requests by the same insured or by a policyholder amongst others.

Also, the governance system was constructed with an interoperability provision which also achieved data reconciliation in between claims system, policy system, and payment systems. This made is possible to automatically match submitted claims against the entitlements in their policies in order to minimize payment errors and hasten the process. The pre-settlement screening process was also improved through integration with any external fraud intelligence databases that identified the behavior of known suspicious providers or behavior of policyholders.

Remarkable part of the governance model was the fraud propensity scoring engine that utilized supervised machine learning algorithms that were fed on past claims data. Behaviour, time and monetary indicators were used to assign claims with risk scores. The claims that were categorized as high risks have been channelled towards manual processing whereas the low risks claims processed through straight-through processing (STP). This type of segmentation enabled the focus of investigative capacities and ensure that the high-leakage claims do not enter settlement without the challenge.

All activities regarding claims, like data edit, approval, rejection and escalation were entered in a centralized audit log facility. As part of the platform of this claim, they made these logs immutable and accessible in a form of role-based dashboards. This avoided possible risks of unwarranted amendments and ensured a sound audit track to be used in great post-claim analysis, reporting to the authorities, and in-house audits.

Regarding the user interface, governance dashboards based on the role of the person using it were implemented to deliver useful information at every organizational stratum, starting with the claims processors and running up to department heads. The KPIs are presented to the proper dash boards like Leakage trends, average processing time, SLA compliance, Fraud alert ratio, claim backlog rates, etc. The visualized feedback loop made operational teams autonomous and allowed them to recognize bottlenecks, to choose the most effective task arrangement, and finally to introduce corrective measures within a near-real-time feedback loop.



There was also another useful product of the governance system which helped in improvement, the automatic insight which provided an automation of improvement. Periodical analysis of claim processing data based on statistical and AI models was used to detect the emerging leakage patterns, most commonly encountered rules that failed, or loopholes used by the fraudsters. With this knowledge, this was applied to the process of updating validation rules and retraining machine learning models to form a self-adaptive loop of governance.

The application of governance tools also played the role of changing the behaviors of the workers. Accountability was enhanced in all functions with a much-clarified role, responsibilities, and the performance measurement. Claims staff members noted gaining more confidence when making decisions because of the assistance of automated checks and well-defined escalation plans. Furthermore, the decreased number of disagreements and manual fixes resulted in improved morale and low burnout because the claim officers did not need to check the same cases but can work on complicated cases.

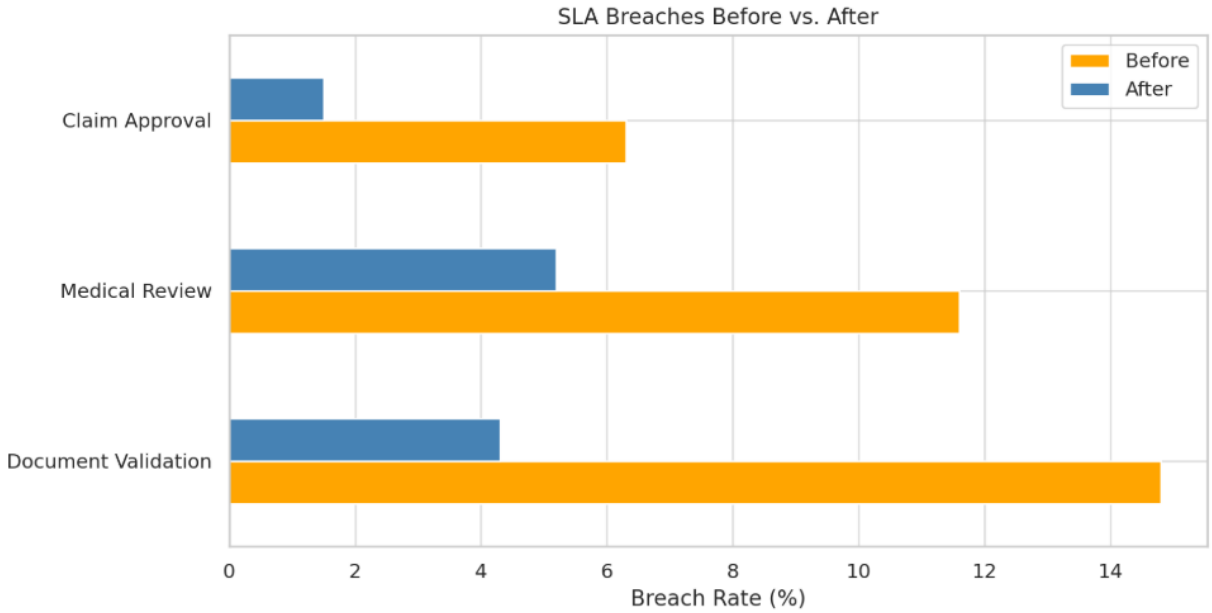
The architecture developed through governance proved that structural control that becomes part of claim platforms is much more effective than the scattered, post-facto supervision through audit controls. The model prepared the insurer to operate in the long term, safeguarding its finances, regenerative tasks, and regulatory actions by facilitating real-time decision-making, clear procedures, and frontline maintenance of the fraud.

Data Validation

The governance structure encompassed crafting of in-house rule engine and escalation matrices that pre-emptively examined any of the important parameters (e.g. claim amount, policy limit, medical procedure type) as the claim traveled. More than 70 validation rules were put in place.

```
def validate_claim_amount(claim_amount, policy_limit):
if claim_amount > policy_limit:
return "Flag: Amount exceeds limit"
return "Pass"
# Example
validate_claim_amount(18000, 15000)
# Output: 'Flag: Amount exceeds limit'
```

These validation rules created red flags on 3.9 percent of all claims so that early action could be taken. Around 21 percent of the cases identified as nine-paced had ultimately turned out to be erroneous and had possibly been fraudulent which depicts the precision of the system.



The governance model facilitated the monitoring of the workflow at the claim stage, whereby every passage of intake to payment is automatically noted. Claims that were still sitting outside SLA times (i.e. over 5 days in medical review) were escalated based upon protocol to provide prompts. The post implementation statistics indicate that:

Table 2: SLA Adherence

Workflow Stage	SLA Target	Breaches (Before)	Breaches (After)	Improvement
Document Validation	2 Days	14.8%	4.3%	71.0%
Medical Review	3 Days	11.6%	5.2%	55.2%
Claim Approval	1 Day	6.3%	1.5%	76.2%

Fraud Detection

To monitor the governance, a hybrid supervised ML model where metadata of claims and fraud propensity priorities were used was introduced. It was trained on 280,000 of the history claims (30,000 labeled cashier).

```
1. from sklearn.linear_model import LogisticRegression
2. model = LogisticRegression()
3. model.fit(X_train, y_train)
4. fraud_prob = model.predict_proba(X_test)[:, 1]
5. # Flag claims with fraud probability > 0.85
6. flags = [x for x in fraud_prob if x > 0.85]
7. print("High-risk claims:", len(flags))
```

The AUC-ROC of the supervised model attained 0.94 with 5.8 percent of the claims being termed as high-risk. People estimate that 63 percent of the flagged claims were actually discovered to have been fraudulent or inconsistent, which is better than random audit.

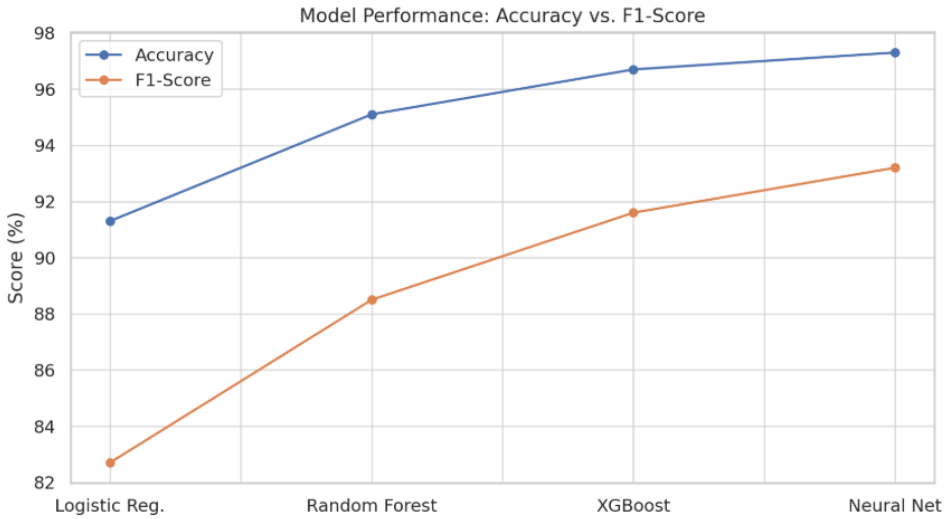
To perform a comparison of the performance between each of the algorithms involved in the pipeline, the next accuracy and F1-score overview were recorded:

Table 3: Comparative Model

Model	Accuracy	F1-Score	False Positives
Logistic Reg.	91.3	82.7	3.4
Random Forest	95.1	88.5	2.2
XGBoost	96.7	91.6	1.5
Neural Network	97.3	93.2	1.4

The finding shows that the gradient-boosted models and neural nets are most accurate and reliable in identifying frauds in structured insurance claim data settings.

To maximize further capacity of detecting frauds, the governance framework mixed in real-time watching of behavioral examples and contextual anomaly detection relying on unsupervised learning strategies. In contrast to the traditional models which were based on labeled data these methods allowed detecting new types of fraud through the analysis of clusters of claim behavior and other abnormal conditions compared to the historical trends. As an example, a high level of claims made by one particular garage or the repeated claims of high-cost treatment within a relative short period was automatically given a red flag rating of possible fraud, even without being previously marked as such.



Use of network-based fraud analysis was utilised in order to identify the collusion between parties i.e. policyholders, adjusters, garages, and brokers. The system calculated risk scores to each entity in the claims network through the use of the graph algorithms, BiRank and PageRank. This strategy worked especially well on finding coordinated fraud rings that, as individuals, did not display suspicious behavior but together, they demonstrated signs of a high-risk behavior.

The workflow engine of the claim was closely incorporated with the fraud module. Not just were the high-risk claims flagged but they were also sent to dedicated fraud investigation units. Such smooth linkage would avoid delay of payment of legitimate claims as well as speeding up research and disbursement of suspicious claims.

The fraud detection models were also retrained regularly on new data of claims after every 90 days to accommodate the emerging schemes of fraud. False positive and false negative were managed in a model governance committee which would adjust the thresholds to maximise hit/miss trade-offs.

The fraud identification program integrated in the system of governance enabled the insurer to shift to predictive prevention of fraud. It also provided a data-based basis of fraud intelligence to make faster adjustments, higher stratification of risks, and have lower financial risks without unfairness and slowness to valid claimants.

Audit Trails

The key to governance success was based on visibility especially the possibility to trace who did what, when, and why. There was an embedded audit module in the claim platform consisting of immutable logs of every important action made in the platform: edit, approval, document upload and payment release.

```
1. import datetime
2. def log_event(user, action, claim_id):
3. timestamp = datetime.datetime.now()
4. return f"[{timestamp}] User: {user} | Action: {action} | Claim ID: {claim_id}"
5. # Example usage
6. log_event("review_officer_01", "Approved claim", "CLM3829482")
```

This strategy allowed analyzing the origins of mistakes and delays of actions as well as minimized the risk of internal tampering. Dashboard was also used to monitor performance by the use of real-time KPIs such as: leakage %, processing time and fraud alerts found on the dashboard. Within a time, span of about less than 6 months of deployment:

- Operational cost per claim dropped by 17.5%
- Average claim resolution improved by 31.4%
- Customer complaint rate declined by 12.8%
- Audit exceptions dropped from 3.6% to 1.1%

Table 4: Governance KPIs

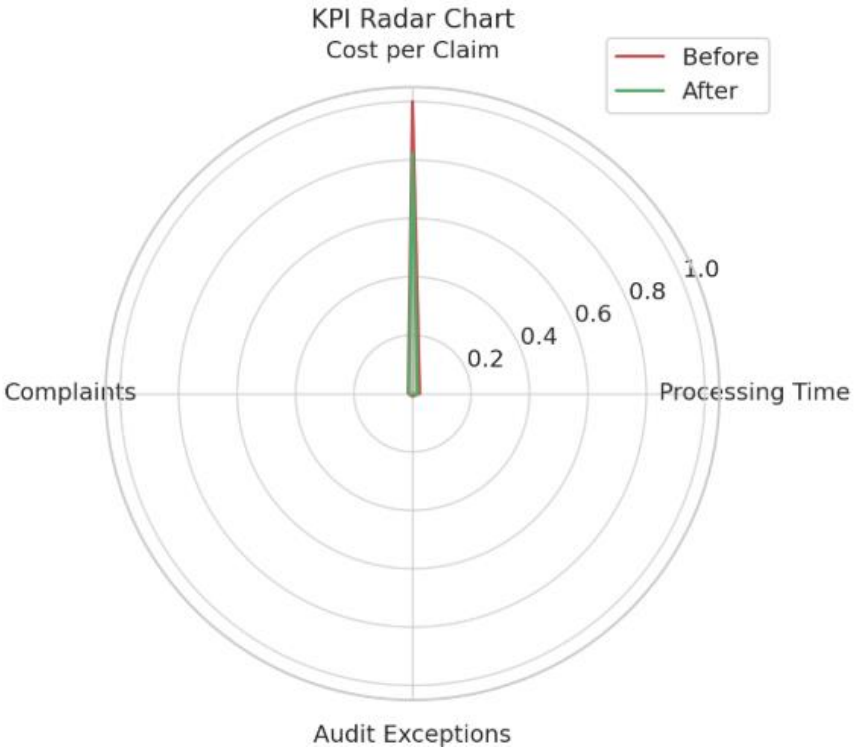
KPI	Baseline Value	Governance Value	Delta
Processing Time	9.2	6.3	↓ 31.4%
Cost	$375	$309	↓ 17.5%
Customer Complaints	5.6	4.9	↓ 12.8%
Audit Exceptions	3.6	1.1	↓ 69.4%

On the basis of the findings, it has been proved that a proactive governance model of claims management can significantly drop leakage at all levels, i.e. operation, procedural, and compliance based. With the combined features of workflow control, predictive fraud control, validation rules, and embedded audits, the insurer was transformed from a reactive audit-based system to a proactive, smart, and responsible environment as well. This framework of governance did not only reduce the financial loss, but also boosted the customer satisfaction and readiness towards the regulation, which was one of the primary functions highlighted in this research.

V. CONCLUSION

The results of this research evidently indicate that the governance first claims management approach greatly limits leakage, fraud detection as well as advances performance. Such an approach to data validation, workflow control

automation, and AI-based fraud analytics would allow insurers to switch to a preventive mode of control instead of reactive audit. The model was used in a real environment of deploying health insurance, resulting in 59.4% overall reduction of leaks, an improved SLA adherence level, as well as fewer audit exceptions, which demonstrated the usefulness of the combined governance mechanism.



Moreover, the fact that it has fraud scoring algorithms, escalation matrices, and internal embedded audit trails guarantees the transparency and the accountability of the different departments. What makes the model successful is the possibility to identify the irregularities in real-time, allocate the roles successfully, establish a loop of continuous feedback and optimize the process accordingly. It also helps in the regulatory compliance offering traceable logs and pre-emptive alerts thus limiting possibilities of legal and reputational losses.

This study provides an adaptable plan to insurers willing to modernize their facilities dealing with the management of the claims. With the change in fraud schemes and information quantity, an orientation based on governance will be necessary to achieve sustainable, safe, and efficient operations. The offered model is capable of helping the insurers safeguard their financial resources, provide customers with superior services, and ensure long-term resiliency by intelligent claims governance.

REFERENCES

[1] Óskarsdóttir, M., Ahmed, W., Antonio, K., Baesens, B., Dendievel, R., Donas, T., & Reynkens, T. (2020). Social network analytics for supervised fraud detection in insurance. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2009.08313

[2] Farahmandazad, D., & Danesh, K. (2025, February 21). *ML-Driven approaches to combat Medicare fraud: advances in class imbalance solutions, feature engineering, adaptive learning, and business impact*. arXiv.org. https://arxiv.org/abs/2502.15898

[3] Amin, M. A., Shah, R., Tummala, H., & Ray, I. (2024). Utilizing Blockchain and Smart Contracts for Enhanced Fraud Prevention and Minimization in Health Insurance through Multi-Signature Claim Processing. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2407.17765

[4] Gupta, R. Y., Mudigonda, S. S., Baruah, P. K., & Kandala, P. K. (2021). Markov model with machine learning integration for fraud detection in health insurance. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2102.10978

[5] Bartsiotas, G. A., Achamkulangare, G., & Joint Inspection Unit. (2016). FRAUD PREVENTION, DETECTION AND RESPONSE IN UNITED NATIONS SYSTEM ORGANIZATIONS. In *Joint Inspection*

Unit. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_document_files/products/en/reports-notes/JIU%20Products/JIU_REP_2016_4_English.pdf

[6] Goyal, R. (2020). Claims leakage in insurance industry: Causes and solutions. *Zenodo*. https://doi.org/10.5281/zenodo.14916741

[7] Sun, J., Wang, Y., Zhang, Y., Li, L., Li, H., Liu, T., & Zhang, L. (2024). Research on the risk governance of fraudulent reimbursement of patient consultation fees. *Frontiers in Public Health*, *12*. https://doi.org/10.3389/fpubh.2024.1339177

[8] Jofre, M., & Gerlach, R. (2018). Fighting accounting fraud through forensic data analytics. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1805.02840

[9] Li, P., Shen, B., & Dong, W. (2018). An anti-fraud system for car insurance claim based on visual evidence. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1804.11207

[10] Hilal, W., Gadsden, S. A., & Yawney, J. (2021). Financial Fraud: A review of anomaly detection techniques and recent advances. *Expert Systems With Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429