TİDE Academia Research
Sayı 6 / 151-172 (2024)

Case Study/*Vaka Çalışması*

ROLE OF MACHINE LEARNING IN INTERNAL FRAUD DETECTION

Teoman Samet TEMUÇİN[1]
Anıl AY[2]

Submitted/Başvuru:22.03.2025
Last Revised/Son Düzeltme:14.05.2025
Accepted/Kabul: 14.05.2025

Abstract

One of the operational risks faced by the entities is internal fraud. In addition to preventive proactive controls, the existence of reactive continuous risk monitoring to quickly detect them is of great importance. In this paper the big data transformation story of Garanti BBVA - one of the most important banks of Türkiye - is taken one step further regarding detection of internal frauds. It is explained how machine learning was integrated into the "rule-based" approach with proven success thanks to the accumulated data pool. The hybrid model supported with machine learning has established a more effective continuous monitoring approach and also ensured the maintenance of sustainable critical metrics such as high internal fraud detection ratio and low Bank loss. It is expected that the mentioned methodology with proven success in detection of internal frauds and with

1 Dr., Internal Audit Manager, Garanti BBVA Internal Audit Department, e-mail: teomant@garantibbva.com.tr, ORCID ID: 0000-0001-7095-1686

2 Internal Audit Manager, Garanti BBVA Internal Audit Department, e-mail: anilay2@garantibbva.com.tr, ORCID ID: 0000-0001-9612-3045

To cite this article: Temuçin, T. S., Ay, A., (2024). Role Of Machıne Learnıng In Internal Fraud Detectıon, TİDE AcademIA Research, 6(2), 151-172

its recent integration with machine learning would be an inspiration for the sector.

Keywords: Internal fraud, Big data, Machine learning, XGBoost

JEL Classification: C52, C55, C8, M42

İŞLETME İÇİ SUİİSTİMALİN TESPİTİNDE MAKİNE ÖĞRENMESİNİN ROLÜ

Öz

Kurumları tehdit eden önemli operasyonel risklerden biri de işletme içi suiistimaldir. Söz konusu eylemleri önleyici proaktif kontrollerin varlığı kadar, hızlı bir şekilde tespit edilmesini sağlayacak reaktif sürekli izleme mekanizmalarının mevcudiyeti de önem arz etmektedir. Bu çalışmada, Türkiye'nin önemli bankalarından biri olan Garanti BBVA'nın işletme içi suiistimal tespitinde büyük veri dönüşüm hikayesi bir adım ileriye taşınmıştır. "Kural-bazlı" olarak nitelendirilen ve başarısını kanıtlamış mevcut tespit yaklaşımına, biriken veri havuzu sayesinde makine öğrenmesinin nasıl entegre edildiği ele alınmıştır. Makine öğrenmesiyle desteklenen yeni hibrid modelle; daha etkin bir sürekli izleme yaklaşımı kurulduğu gibi, yüksek işletme içi suiistimal tespit oranı ve düşük Banka kaybı gibi kritik göstergelerde de yıllara sari sürdürülebilirlik kazanmak mümkün olmuştur. İşletme içi suiistimalin tespitinde başarısını kanıtlayan ve makine öğrenmesinin entegre edildiği bu metodolojinin sektöre de ilham kaynağı olması beklenmektedir.

Anahtar Kelimeler: İşletme içi suiistimal, Büyük veri, Makine öğrenmesi, XGBoost

JEL Sınıflandırması: C52, C55, C8, M42

1. Introduction

Operational risk is the probability of loss caused by processes, external events, personnel or information systems due to insufficient internal controls. To further explain, it is the probability of any loss which may be caused by failure to detect mistakes and misconducts as a result of the problems in the internal controls; personnel's not acting in accordance with the present conditions; errors and problems in the information systems; internal or external frauds; natural disasters or terrorist activities (Babuşcu et al., 2018).

As can be understood from the definition, one of the most important factors causing operational risk is the personnel. This factor may cause operational risk due to unintentional mistakes, omissions or faults as well as intentional actions such as embezzlement, unjust benefits or stealing. These intentional actions of the personnel are called "internal frauds". The internal frauds in the banking sector are generally in the form of embezzlements and unjust benefits. Embezzlement is the misappropriation of funds by the personnel from the bank cash vault or customer accounts. The unjust benefits, on the other hand, are earned by causing loss to the entity the personnel work for by granting improper loans, leaking critical information to outside, intentional pricing made against the entity benefits and abusing one's powers based on agreements reached with internal/external stakeholders, and earning benefits from such losses.

For effective management of the internal fraud risk, the entities should eliminate the opportunities that might make it possible to commit internal frauds and have continuous risk monitoring mechanisms to detect them as soon as possible. Otherwise, frauds may cause loss of trust and reputation as well as high amounts of operational losses.

In this paper, we will explain how machine learning was integrated into our "rule-based" monitoring approach thanks to the accumulated data with the data project conducted in 2023. To do this, we will focus on the selection of the machine learning model generating the best results, its integration into the current model and performance results generated with this new methodology. This new approach integrated with machine learning and challenging big data capabilities is expected to provide guidance regarding internal fraud detection for the sector.

The paper is organized as follows: Section 2 provides a literature review of machine learning models and their usage in fraud detection. Section 3 explains the data and previous internal fraud detection approach at Garanti BBVA and how machine learning was integrated into this rule-based methodology by using big data capabilities. Section 4 presents the comparative results of newly applied methodology and inspires readers for applying a similar approach and finally, Section 5 provides a conclusion on the subject.

2. Literature Review

Deterrent controls aim for preventing frauds while continuous risk monitoring aims for detecting frauds as soon as possible. The early detection of a fraud is of critical importance for the minimization of the operational loss and reputational risk (ACFE, 2024). Therefore, a comprehensive approach combining cutting edge technology, strong internal controls, continuous risk monitoring and proactive risk management is needed for an effective fight against frauds (Ismail & Haq, 2024). The most critical question of continuous risk monitoring is which transactions (sample) will be prioritized from among tens of thousands of transactions (audit universe) by using predefined anomalies and patterns?

The literature mainly focuses on visualization of the data and modeling of fraud incidents by utilizing big data capabilities (Fawcett & Provost, 1997; Rosset et al., 1999; Bolton & Hand, 2002; Becker et al., 2010; Li et al., 2012; Temuçin et al., 2021). According to Baesens et al. (2015), "big data and analytics provide powerful tools that may improve an organization's fraud detection system." Nevertheless, even though several data categories and a range of statistical models are available, it is not easy to develop an effective fraud detection method by using all of them at the same time (Gomes et al., 2021). Similarly, Njoku et al. (2024) argues that "traditional rule-based fraud detection methods have long been employed by banks to identify suspicious transactions. However, these methods often fall short in detecting intricate and evolving fraud patterns. With fraudsters' continually adapting and developing new tactics, there is a pressing need for more effective and adaptive fraud detection solutions that can keep pace with these dynamic threats."

Therefore, the literature goes one step beyond of determination of anomalies by using ma-

chine learning for fraud detection (Baesens et al., 2021; Wei et al., 2020; Ge et al., 2020; Kolodiziev et al., 2020; Shirgave et al., 2019; Soviany, 2018). Machine learning is making estimations regarding existing data by making some interpretations and deductions from previous data by making use of statistical models. Our example aims for facilitating the distinguishing of whether the transactions we detect today are "frauds" or "not frauds" based on the previous "proven fraud" and "false positives" data and determination of a more effective sample. The transactions tagged suspicious with this method are then subjected to a more thorough examination. The data pool growing day by day will enable detection of more suspicious transactions over time and also prevent overlooking the changing fraud patterns. In short, the machine self-learns.

The machine learning models are mainly classified as supervised (Khatri et al., 2020), unsupervised (Srivastava & Salakhutdinov, 2014; Gomes et al., 2021) and semisupervised (Van Engelen & Hoos, 2020). The supervised learning models are used if the data set includes variables that can be "labeled" while unsupervised learning models are preferred if complex and multifaceted data that cannot be labeled are used.

The supervised learning algorithms try to find an optimal function in order to associate the input features and outputs based on a labeled dataset. The goal here is to identify the function to best suit to the pattern between the input and output. This allows for estimation of which outputs can be generated by new inputs thanks to this function. The model making the best estimation is generally determined based on parameters such as accuracy, precision, recall, F-score and time (Sinap, 2024). The most preferred supervised learning models are logistic regression, neural network, decision trees, support vector machine and naïve bayes (Albashrawi, 2016).

Unsupervised learning algorithms are used for datasets that cannot be labeled. Unlike supervised models, these datasets are not labeled or in other words, not trained to show which input data generate which output. However, despite the lack of trained and labeled datasets, unsupervised learning is a modeling method that categorized similar results under certain groups with the clustering method based on the features of the available data.

Let us we have unlabeled data consists of multiple modes and each modality has a different kind of representation and correlational structure. For instance, we have a data which consists of "images are tagged with textual information and videos are accompanied by audio. Each modality is characterized by having distinct statistical properties. Text is usually represented as discrete sparse word count vectors, whereas an image is represented using pixel intensities or outputs of feature extractors which are real-valued and dense. Having very different statistical properties makes it much harder to discover relationships across modalities than relationships among features in the same modality. There is a lot of structure in the data but it is difficult to discover the highly non-linear relationships that exist between low-level features across different modalities. Moreover, the data is typically very noisy and there may be missing values." (Srivastava & Salakhutdinov, 2014). Unsupervised models learn by creating meaningful categories from these non-labeled complex datasets.

Semisupervised learning algorithms, on the other hand, learn by using both labeled and non-labeled data. These models generally use large amounts of non-labeled data together with smaller amounts of labeled datasets. Therefore, semisupervised learning algorithms are generally used when the labeled data are very limited. In such cases, if at least sufficient non-labeled data are available, limited labeled data could help with the determination of a better classifier under certain assumptions regarding the distribution of data (Van Engelen & Hoos, 2020).

Since insurance fraud is a complex phenomenon whose results cannot be labeled with certainty and it is not possible to define certain rules, Gomes et al. (2021) preferred to use unsupervised learning approach for insurance fraud detection. However, in our case from a banking industry, we preferred using the supervised learning models since we have a dataset accumulating since 2021 and including labeled "proved fraud" and "false positives" determined as a result of several fraud rules defined over years and assigned with risk scores. When model outputs were compared by using different parameters, we achieved the best performance from Extreme Gradient Boosting (XGBoost) during our recent work.

XGBoost algorithm is inspired by Gradient Boosting algorithm (Friedman, 2001) which

has been successfully used in classification, learning to rank and prediction for many years. The main principle of boosting is the creation of consecutive sub-trees from the original tree by minimizing the mistakes of a previous tree with the next created one. The new sub-trees generated in this way will update the previous residuals to minimize the mistakes of the function. XGBoost is an optimized form of Gradient Boosting to prevent overfitting. The most important features of the revised algorithm are high estimation power, prevention of overlearning, management of empty data and doing all these at a 10x speed (Chen & Guestrin, 2016).

Although, Albashrawi (2016) lists the most used supervised learning models as logistic regression, neural network, decision trees, support vector machine and naïve bayes, his results are based on the studies conducted before 2016. According to the paper explaining the working principle of new XGBoost, 17 out of 29 winning solutions in machine learning competition site Kaggle used XGBoost (Chen & Guestrin, 2016). Moreover, several recently conducted studies confirm that XGBoost shows a faster and more effective performance as compared to other supervised models (Cao et al., 2021; Dhieb et al., 2020).

Therefore, we integrated XGBoost learning algorithm to our "rule-based" approach created by using big data capabilities for the detection of internal frauds generating the best results according to the comparison data. Thus, machine learning has become a part of our anomaly detection system. We refer to it as a part of our system since we have not stopped using our previous "rule-based" approach with a proven performance and have not performed examinations only over the sample generated with the use of the machine learning model. Instead, we assigned a weight coefficient to both approaches ("rule-based" vs. "XGBoost machine learning algorithm") and also continued to use our old system. Therefore, we had the chance to compare the strengths and weaknesses of both methods.

Nevertheless, examining the applications currently used by the finance system for the detection of frauds, we see that the rule-based methods and machine learning-based methods are used the most. In fact, the system we recommend and actively use is a hybrid approach allocating a weight coefficient to both approaches. Therefore, we can neither disregard

the "expert judgment" provided by the rule-based approach nor the "objectivity" and "accuracy" advantages provided by machine learning (Cao et al., 2021). In every new fraud incident we encounter, we compare the strengths of both methods and change the weight coefficients used to determine the sample, if necessary.

We will explain in following sections the dataset that has been created from 2021 to 2023 with the "rule-based" approach, how we label it, how we trained the model by using these data, the criteria we used to select XGBoost learning algorithm, how we have integrated machine learning to our current method and thus, how we have created a more effective sample pool. The significant results that we have achieved regarding internal fraud detection in 2024 support our arguments regarding our new detection method. Thanks to the accumulating "proven fraud" and "false positives" data, we have achieved a fraud detection system which learn and evolve over time.

3. Data and Methodology

3.1. Data

All money withdrawal and transfer transactions performed from Garanti BBVA branches are used as data for internal fraud detection and a sample is determined with the method named rule-based. The rule-based model ensures that more than 50 risk rules (personnel with high debts, foreign customers, transactions with no receipt etc.) are matched with every money withdrawal or transfer transaction and the final risk score is calculated by adding up the scores for the risk rules that the related transactions were matched with. The final examination sample is determined based on the highest riskiness score.

The most important limitations of the rule-based method are the manual scoring of the related more than 50 risk rules based on previous experiences and the probability that these rules may become insensitive to the changing fraud trends over the years. To address these limitations, a data project was conducted in 2023 to strengthen the current method with the machine learning model. The dataset used in this data project is detailed below. (Table 1)

Table 1: Details about Dataset

Selected Features	Labeled Transactions	Total Transactions	Train Data	Validation Data	Test Data
> 50	~ 860	~ 27,000,000	~ 60,700	~ 15,580	~ 10,400

where,

- *Selected Features:* Riskiness rules used in the rule-based method
- *Labeled Transactions:* Number of proven internal frauds
- *Total Transactions:* Total number of transactions flagged by the rule-based method
- *Train Data:* Number of transactions used to train the model
- *Validation Data:* Number of transactions used to validate the model
- *Test Data:* Number of transactions used to test the model

The machine learning model was designed with the aim of revising the scores assigned to rules by taking into consideration the rules with which the previous internal frauds were matched and to promote the rules regarding the previous fraud incidents. Therefore, the selected features used for the model design were selected from among the rules used in the current model. Taking into consideration that the share of labeled transactions in the total dataset is small, studies were conducted over an imbalanced dataset. The test data selected from among the total number of transactions labeled by the rule-based method was selected as different than the train data and validation data with the goal of testing the model with a more rational dataset.

3.2. Methodology

The dataset detailed above was used for the selection of an algorithm with an in-house application by using SQL and Python coding languages. "Supervised" algorithms were preferred for the selection of an algorithm since the dataset includes "labeled data". The Confusion Matrix digitizing the estimated and actual values for the target values was used to measure the model results. (Table 2)

Table 2: Confusion Matrix Table

Predicted / Observed	**Negative**	**Positive**
Negative	True Negative (TN)	False Positive (FP)
Positive	False Negative (FN)	True Positive (TP)

We compared the performance of XGBoost, Gradient Boost, Random Forest and Decision Tree algorithms based on the Recall, Precision and F1-Score results generated by using the values in the Confusion Matrix. (Table 3)

Table 3: Performance Comparison

Algorithms	**Recall**	**Precision**	**F1-Score**
XGBoost	85%	67%	75%
Gradient Boost	74%	98%	84%
Random Forest	53%	100%	70%
Decision Tree	16%	85%	27%

where,

- *Recall*: TP / (TP+FN)
- *Precision:* TP / (TP+FP)
- *F1-Score:* 2 * (Precision * Recall) / (Precision + Recall)

The highest recall value, which is the ratio of true positives in all positive predictions, is expected for model selection. In addition, the precision and F1-score is expected not differentiated much in compare to other algorithms. While XGBoost algorithm provides speed and performance by using gradient-boosted decision trees (Dhaliwal et al., 2018), it is a popular application that can also process imbalanced data in fields such as fraud detection (Priscilla & Prabha, 2020).

As a result of the selected algorithm, the model assigns a feature importance value shown in percentile to every rule. (Table 4) As a result of these assigned feature importance values, a total fraud probability score is calculated for each transaction by taking into consideration the rules with which a transaction matches. In order to compare this score generated by the rule-based model, this score is multiplied by 100 to generate a final risk score for each transaction and a hybrid scoring is made by using the other risk score generated for the transaction with the rule-based method. In 2024, a final risk score is assigned to all transactions performed on the previous day by using the 70% of the riskiness score generated with the rule-based model and 30% of the riskiness score generated with the machine learning model. The scoring example is presented in Figure 1.

Table 4: Feature Importance Examples

Features	Feature Importance
Rule-1	6.40%
Rule-2	6.15%
Rule-3	5.40%
…	…
Total	**100%**

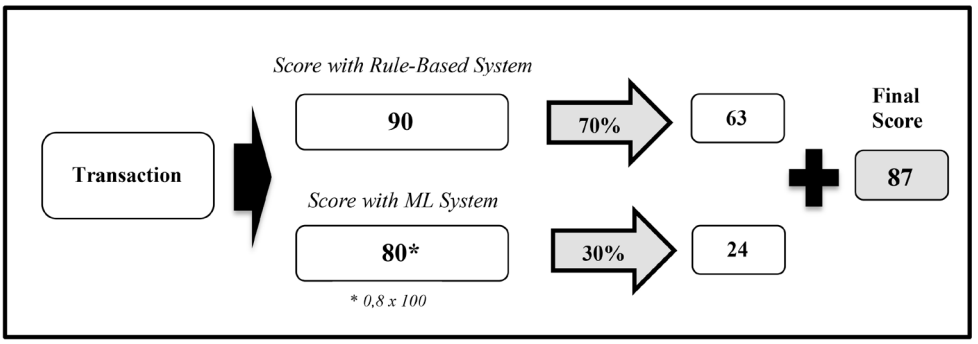

Figure 1: Sample Scoring

The hybrid scoring method shown in Figure 1 aims for ensuring that the proven rule-based method has a higher impact on the scored transactions while observing the machine learning model outputs for some time. The results generated with this hybrid model integrating the machine learning to the existing method are explained in the following section.

4. Comparison of Results

We analyzed the impact of the machine learning on the internal frauds detected in 2024 by considering the machine learning project launched as a reference point and compared the internal fraud detection ratio and the bank losses caused by internal frauds over the years. According to the results of these analyses and comparisons, we revealed that the machine learning integration provides positive support to the existing rule-based method but has some limitations.

4.1. Effectiveness

In order to understand the impact of the machine learning model launched in 2024 to the riskiness of the fraud transactions, the risk ranking of the committed frauds determined with the rule-based approach and their risk ranks assigned by the hybrid model with integrated machine learning were compared. The internal frauds committed at 8 different branch locations in 2024 were used for this purpose. (Table 5)

Table 5: Impact of Machine Learning on Risk Ranking of Internal Frauds Committed in 2024

Case	Fraud Transactions	Non-Affected Transaction (%)	Negative Affected Transaction (%)	Positive Affected Transaction (%)
Branch A	61	25%	0%	75%
Branch B	3	33%	0%	67%
Branch C	8	50%	0%	50%
Branch D	4	50%	0%	50%
Branch E	6	17%	33%	50%
Branch F	8	25%	62%	13%
Branch G	1	0%	100%	0%
Branch H	21	29%	71%	0%
Total	**112**	**28%**	**20%**	**52%**

According to Table 5, the machine learning generated effective results for Branch A, where a total of 61 internal fraud transactions were performed for the fraud committed. 75% of these transactions were ranked as more risky based on the scores assigned to them by the machine learning model. However, the scores assigned by the machine learning model to 25% of the related transactions did not have any impact on the riskiness ranking. In another example regarding Branch H where the machine learning did not generate effective results, a total of 21 internal fraud transactions existed. 71% of these transactions were ranked as less risky based on the scores assigned to them by the machine learning model. Thus, despite a proven fraud, the machine learning model assigned a lower riskiness score to the related internal fraud transaction as compared to the scores assigned by the rule-based approach.

According to a general evaluation on the results listed in Table 5, the machine learning model scored 52% of 112 internal fraud transactions performed in 8 fraud incidents in 2024 as more risky and 20% as less risky and did not have any impact on the riskiness level of the remaining 28%. In 5 (63%) out of 8 incidents, the machine learning model had a positive contribution of 50% and above and measured the fraud transactions as more risky, yielding positive results. However, the evaluation of the fraud transactions in 3 cases (37%) as less risky as compared to the results generated by the rule-based method reveals the limitations of the hybrid model regarding the frauds not experienced by the model in the past.

4.2. Internal Fraud Detection Ratio

According to the Report to the Nations (ACFE, 2024), 43% of the internal frauds are detected via tip (whistleblowing) while 14% are detected by internal audit teams. (Table 6) Taking into consideration that the internal audit detection ratio was 15% in the previous report (ACFE, 2020), it is seen that the internal audit detection ratio has remained stable and limited over the years despite the increased technology and data capabilities.

Table 6: How is Occupational Fraud Initially Detected?

Type	Ratio
Tip	43%
Internal Audit	**14%**
Management Review	13%
Document Examination	6%
Account Reconciliation	5%
By Accident	5%
External Audit	3%
Automated Transaction/Data Monitoring	3%
Surveillance/Monitoring	2%
Other	2%
Notification by Law Enforcement	2%
Confession	1%

Source: ACFE (2024)

However, it is seen from the year-to-year evolution of the detection of internal frauds at Garanti BBVA by Internal Audit Department (IAD) that the success achieved with the rule-based method in 2020 was maintained during 2021-2023 and the highest detection ratio (50%) was achieved in 2024 when the machine learning was integrated into the model. (Table 7) As discussed in the previous section, the assignment of higher risk scores to the proven frauds by the machine learning model and assignment of higher risk ranking used to create the sample have made a positive contribution to this detection ratio.

Table 7: Internal Fraud Detection Ratio by Garanti BBVA IAD (2016-2024)

Period	IAD Detection Ratio (%)
2016-2019 (Scenario-based)	21%
2020-2023 (Rule-based)	39%
2024 (Machine Learning Integrated)	50%

4.3. Bank Losses Caused by Internal Frauds

The quick detection of frauds is an important contributor to the minimization of the loss experienced by an entity (ACFE, 2024). In order to observe the losses experienced by the Bank due to internal frauds over the years, we examined the average loss amounts in 3 different periods as scenario-based method period (2016-2019), rule-based method period (2022-2023) and the period where the rule-based method was supported with machine learning (2024). (Table 8)

Table 8: Bank Loss Caused by Internal Fraud (2016-2024)

Period	Annual Average Loss Amount (EUR)
2016-2019 (Scenario-based)	1,000,000
2020-2023 (Rule-based)	660,000
2024 (Machine Learning Integrated)	500,000

According to the above table, the average losses have a decreasing trend over the years and the machine learning model has made a positive impact of 24% as compared to the previous period.

Taking into consideration all the outputs explained in this section, supporting of the rule-based method implemented by using big data capabilities with the machine learning model

- Has ensured that the transactions resulting in internal frauds (proven frauds) were generally scored to be of higher risks,
- Made a positive contribution to achieve a sustainable ratio regarding the frauds detected by the internal audit (fraud detection ratio) and
- Supported a similar sustainable decrease in the loss amounts.
- However, the machine learning also has some limitations of assigning lower risk scores to some internal frauds as compared to the rule-based method.

5. Conclusion

Operational risk is the probability of loss caused by processes, external events, personnel or information systems due to the lack of sufficient control mechanisms. Incidents such as embezzlements, unfair benefits, thefts etc. caused by the personnel are called as internal frauds. These incidents might cause financial losses as well as reputation and prestige loss for the entity. Therefore, the availability of a reactive continuous risk monitoring mechanism to ensure the quick detection of internal frauds is as important as the availability of preventive proactive controls.

Continuous risk monitoring is the flagging of potential fraud transactions by using big data capabilities based on anomalies and patterns and then examination of these transactions with proficiency and due professional care. The most important question to be asked at this point is how the most risky transactions to be examined (the sample) will be determined? The paper attempts to answer this question. To this end, the story of transformation at Garanti BBVA one of the most important banks in Türkiye achieved by using big data capabilities is discussed.

The "scenario-based" method to identify risky transactions implemented for long years was transformed into a "rule-based" approach with the big data project conducted in 2019. The creation of a more efficient and effective fraud detection mechanism by this transformation was proven by the results generated. This transformation has not only provided the entity with the possibility of achievement of a higher internal fraud detection ratio with fewer resources but also laid the foundation for the entity to benefit from machine learning by using ever-accumulating "proven fraud" and "false positives" data. As a matter of fact, the literature was also promoting us the integration of machine learning to the existing method, by taking a step further.

The second phase of the project was finally initiated in 2023 by using the accumulated data and XGBoost supervised learning model considered to show the best performance according to comparative results has become a part of our approach to detect risky transactions. Accordingly, the transactions determined as the most risky by the hybrid model we created by taking into consideration 70% of the riskiness assignment determined with the existing "rule-based" approach and 30% of the riskiness score given by XGBoost machine learning algorithm are ranked every day by riskiness level and examined. This

approach combines the "expert judgment" provided by the rule-based approach and the "objectivity" and "accuracy" advantages provided by machine learning. We also had the chance to observe the outputs of machine learning for some time.

We conclude that the integration of machine learning to the rule-based approach ensures more effective detection of internal fraud incidents. This hybrid continuous risk monitoring where machine learning is integrated into the rule based approach contributes to the creation of a more risky transaction pool (sample), increasing both the ratio of detection of frauds and decreasing the loss amount that might be caused by internal frauds. Therefore, we believe that this new approach we use to detect internal frauds by making use big data capabilities and machine learning will guide the sector.

However, the transformation from a rule-based approach to a more advanced detection approach with machine learning should be realized in a controlled way and the machine learning model to be used should be continuously challenged. Accordingly, we believe that the observation of the transformation by using a hybrid model for some time like we did at Garanti BBVA would be beneficial.

Author Contribution

The authors have equal contribution to the paper.

Conflict of Interest

There is no conflict of interest among the authors.

Financial Support

The authors have not received any financial support for this study.

Peer-Review

Externally peer-reviewed

Acknowledgments

The authors would like to express their sincere gratitude to Merve KIRAN for contributions to translation and Osman Bahri TURGUT, CAE of Garanti BBVA, for his support and vision for continuous development and progress.

References

Albashrawi, M. (2016). Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015, *Journal of Data Science*, 14(3), 553-570.

Association of Certified Fraud Examiners (ACFE) (2024). Occupational Fraud 2024: A Report to the Nations. Retrieved from https://legacy.acfe.com/report-to-the-nations/2024/

Association of Certified Fraud Examiners (ACFE) (2020). Global Study on Occupational Fraud and Abuse: Report to the Nations. Retrieved from https://legacy.acfe.com/report-to-the-nations/2020/

Babuşcu, S., Hazar, A., & Iskender, A. (2018). *Banka Risk Yönetimi: Basel I - II - III - IV Düzenlemeleri*. Bankacılık Akademisi Yayınları.

Baesens, B., Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. Wiley Publishing.

Baesens, B., Höppner, S., & Verdonck, T. (2021). Data Engineering for Fraud Detection, *Decision Support Systems*, vol. 150, 113492.

Becker, R., Volinsky, C., & Wilks, A. (2010). Fraud Detection in Telecommunications: History and Lessons Learned. *Technometrics*. 52(1), 20-33.

Bolton, R. & Hand, D. (2002). Statistical Fraud Detection: A Review, *Statistical Science*. 17(3), 235-255.

Cao, R., Liu, G., Xie, Y., & Jiang, C. (2021). Two-Level Attention Model of Representation Learning for Fraud Detection, *IEEE Transactions on Computational Social Systems*, 8(6), 1291-1301.

Chen, T. & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System, *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge, Discovery and Data Mining*, NY, USA, 785-794.

Dhaliwal, S.S., Nahid, A.A., & Abbas, R. (2018). Effective Intrusion Detection System Using XGBoost. *Information, 9(7),* 149.

Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020) A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement, *IEEE Access*, vol. 8, 58546-58558.

Fawcett, T. & Provost, F. (1997). Adaptive Fraud Detection, *Data Mining and Knowledge Discovery*, 1(3), 291-316.

Friedman, J.H. (2001). Greedy Function Approximation: A Gradient Boosting Machine, *The Annals of Statistics*, 29(5), 1189-1232.

Ge, D., Gu, J., Chang, S., & Cai, J. (2020). Credit Card Fraud Detection Using Lightgbm Model, *2020 International Conference on E-Commerce and Internet Technology,* 232-236.

Gomes, C., Jin, Z., & Yang, H. (2021). Insurance Fraud Detection with Unsupervised Deep Learning, *Journal of Risk and Insurance*, 88(3), 591-624.

Ismail, M.M. & Haq, M.A. (2024). Enhancing Enterprise Financial Fraud Detection Using Machine Learning, *Engineering, Technology & Applied Science Research*, 14(4), 14854-14861.

Khatri, S., Arora, A., & Agrawal, A. (2020). Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison. 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), *IEEE*, 680-683.

Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic Machine Learning Algorithms for Fraud Detection in Digital Payment Systems. *Eastern-European Journal of Enterprise Technologies*, 5(107), 14-26.

Li, S.H., Yen, D.C., Lu, W.H., & Wang C. (2012). Identifying the Signs of Fraudulent Accounts Using Data Mining Techniques. *Computers in Human Behavior*, 28(3), 1002-1013.

Njoku, D., Iwuchukwu, V., Jibiri, J., Ikwuazom, C., Ofoegbu, C., & Nwokoma F. (2024).

Machine Learning Approach for Fraud Detection System in Financial Institution: A Web Base Application. *International Journal of Engineering Research and Development*, 20(4), 1-12.

Priscilla, C.V., & Prabha, D.P. (2020). Influence of Optimizing XGBoost to Handle Class Imbalance in Credit Card Fraud Detection, *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 1309-1315.

Rosset, S., Murad, U., Neumann, E., Idan, Y, & Pinkas, G. (1999). Discovery of Fraud Rules for Telecommunications - Challenges and Solutions, In Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, NY: Association for Computing Machinery Press, 409-413.

Shirgave, S. K., Awati, C. J., More, R., & Patil, S. S. (2019). A Review on Credit Card Fraud Detection Using Machine Learning, *International Journal of Scientific and Technology Research,* 8(10), 1217-1220.

Sinap, V. (2024). Comparative Analysis of Machine Learning Techniques for Credit Card Fraud Detection: Dealing with Imbalanced Datasets. *Turkish Journal of Engineering*, 8(2), 196-208.

Soviany, C. (2018). The Benefits of Using Artificial Intelligence in Payment Fraud Detection: A Case Study, *Journal of Payments Strategy and Systems*, 12(2), 102-110.

Srivastava, N., & Salakhutdinov, R. (2014). Multimodal Learning with Deep Boltzmann Machines, *Journal of Machine Learning Research*, 15(84), 2949-2980.

Temuçin, T. S., Erbaş, S., & Ay, A. (2021). Using Big Data in Internal Fraud Detection, *TIDE AcademIA Research*, 3(1), 55-82.

Van Engelen, J.E., & Hoos, H.H. (2020). A Survey on Semi-supervised Learning, *Machine Learning*, 109, 373-440.

Wei, Y., Qi, Y., Ma Q., Liu Z., Shen C., & Fang C. (2020). Fraud Detection by Machine Learning, *2nd International Conference on Machine Learning, Big Data and Business Intelligence*, 101-115.

Resume

Teoman Samet Temuçin, is Internal Audit Manager at Garanti BBVA. Experienced and skilled mainly in Capital, Market, Structural, Business Model, Governance, Compliance and Operational (internal fraud, investigation and branch audits) risks. In addition to job functions, he holds a Ph.D. in Banking and Finance and contributed to various teaching and research activities.

Anıl Ay, is Internal Audit Manager at Garanti BBVA. Currently managing Conduct, Compliance, AML, CFT and Governance risks at Audit Department. He holds M.Sc. degree in Data Science and B.Sc. degree in Economics.