İktisat Politikası Araştırmaları Dergisi
Journal of Economic Policy Researches
JEPR 2024, 11(2): 242–262
DOI: 10.26650/JEPR1433315

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Denetimli Makine Öğrenmesi Yöntemleri ile Kredi Kartı Sahteciliğini Tahmin Etme: Karşılaştırmalı Analiz

Predicting Credit Card Fraud using Supervised Machine Learning Methods: Comparative Analysis

Güner Altan[1], Metin Recep Zafer[2]

[1]Dr, İstanbul-Türkiye
[2]Dr, İstanbul-Türkiye

Sorumlu yazar / Corresponding author: Güner Altan
E-posta / E-mail: guner.altan@vakifbank.com.tr

ÖZ

Günümüzde teknolojinin gelişmesiyle birlikte kişi ve kurumların dijital platform aracılığıyla harcama kanal yelpazesi genişlemiştir. Bununla birlikte ödeme yöntemleri dijital çağ ile birlikte kolaylaşmıştır. İnternet aracılığıyla dünyanın bir ucundan yapılan bir harcama saniyeler içinde gerçekleşmektedir. Dijitalleşmenin bu kadar hızlı ve global olması, birçok avantajı barındırırken yapılan harcamaların güvenliğini tespit etmek bir o kadar zor olabilmektedir. Bu bağlamda; bankalar şüphesiz, müşteri ile satıcı arasında güvenli bir alışverişe aracılık eden en önemli kurum haline gelmiştir. Kredi kartı harcamalarının bu denli yoğun olduğu dönemde bankaların söz konusu işlemlerin dolandırıcılık olup olmadığını tespit etmesi hem bankaların karlılığını hem de itibarlarını korumaları açısından çözüme kavuşturulması gereken bir problem olarak görülmektedir. Dinamik bir yapıya sahip olan kredi kartı harcamalarının banka müşterisine ait gerçek bir harcama olduğunu tespit etmek ciddi bir efor gerektirmektedir. Bu bağlamda çalışmanın amacı, denetimli makine öğrenmesi yöntemiyle gerçek ve güncel verilerden yola çıkarak az sayıda öz nitelik ile bir model önerisi sunmaktır. Bu bağlamda bankaların kredi kartı sahteciliği tespitindeki operasyon ve maliyet yükünün hafifletilmesi hedeflenmektedir. Bu kapsamda çalışmamızda kamu sermayeli bir bankaya ait 2023 yılı ocak ayı kredi kartı işlemleri baz alınmıştır. Veri seti 13050 gözlem sayısından oluşmaktadır. Model kurulmasında Python programlama dili kullanılmış olup denetimli makine öğrenmesi tekniklerinden Rassal Orman, Lojistik Regresyon, K-En Yakın Komşu, Karar Ağaçları, Gradyan Güçlendirme gibi sınıflandırmada ayırt etme gücü yüksek olan algoritmalar tercih edilmiştir. Algoritmaların kredi kartı sahtecilik işlemini tahmin etme doğruluk skorları ise Lojistik Regresyon % 92.5, Karar Ağaçları %93.1, K- En Yakın Komşu %86.4, Rassal Orman %91.8, Gradyan Güçlendirme %86. 9 olup bunun yanı sıra kesinlik, duyarlılık, F1 skoru ve ROC-AUC gibi performans metrikleri de incelenmiştir. Çalışmada performanslarından dolayı beş algoritmada önerilmektedir.

Anahtar Kelimeler: Kredi kartı sahteciliği, Makine öğrenmesi, Denetimli öğrenme, Rassal orman, Gradyan güçlendirme

Jel Sınıflaması: C60, C69, C81

Başvuru / Submitted : 07.02.2024
Revizyon Talebi / Revision Requested : 03.06.2024
Son Revizyon / Last Revision Received : 11.06.2024
Kabul / Accepted : 26.06.2024

ABSTRACT

Currently, with the progress of technology, people's and institutions' range of expenditure channels via digital platforms has expanded. In addition, payment methods have become easier with the digital age. An expenditure, made from even a distant corner of the World, takes place instantaneously through the Internet. Although the rapid and global nature of digitisation contains many advantages, ensuring transaction security can be challenging. In this context, banks have undoubtedly become the most crucial institutions that mediate safe transactions between customers and sellers. In an era where credit card transactions are so prevalent, it is seen as a problem that needs to be solved by banks to determine whether these transactions involve fraud or not, both for their profitability and reputation. It takes a serious effort to determine that credit card expenditures, characterised by dynamic nature, are real expenses of the customer. Therefore, the aim of this study is to propose a model based on supervised machine learning with using real and current data with a few key features. The objective is to reduce banks' operational burden and cost when identifying credit card fraud. In this context, the credit card transactions of a state-owned bank in January 2023 were considered, using a dataset comprising 13,050 observations. Python programming language is used for model building, and classification algorithms with high discriminatory power, such as Random Forest, Logistic Regression, K-Nearest Neighbours, Decision Trees, and Gradient Boosting, are preferred, which are machine learning techniques. The accuracy scores of the algorithms used in the model setup were determined as follows: Logistic Regression, 92.5%; Decision Tree, 93.1%; K-Nearest Neighbour 86.4%; Random Forest 91.8% and Gradient Boosting 86.9% and performance metrics, such as precision, recall, F1 score, and ROC-AUC, were also examined. Based on their performances, five algorithms were recommended for this study.

Keywords: Credit card fraud, Machine learning, Supervised learning, Random forest, Gradient boosting

Jel Classification: C60, C69, C81

EXTENDED ABSTRACT

With the progress of digitalisation, customer behaviours in the financial sector are also undergoing transformations. The simplest example of this is the evolution of consumption habits. With the expansion of digital network platforms, consumption has become easier, faster, and more reliable. Undoubtedly, credit card expenditures take precedence over these outlays. In a period characterised by such an elevated intensity of credit card expenditures, the importance of secure shopping has significantly increased for both the customer and the banks. In this context, while banks broaden credit card spending networks, they are simultaneously trying to maintain safety infrastructure. With the progress of online money transactions, banks have abandoned traditional methods and have initiated the use of advanced artificial intelligence-based methodologies to detect fraudulent transactions in credit card expenditures.

In the introductory section of the study, while determining its outlines, it has been noted that credit card expenditures have increased significantly with the globalisation. In parallel with this trend, it has been mentioned that banks may experience challenges because they rely on conventional methods for fraud detection in credit card transactions.

In the second part of this study, a literature review is conducted, and machine learning is briefly mentioned, as well as studies on detecting credit card fraud. In this context, it has been observed that machine learning methods are generally used to detect credit card fraud, and domestic studies are found to be relatively fewer than international studies.

The third and final part of the study covers the practical application phase. This section provides information about the model's data and preparation. In this study, artificial intelligence-based machine learning methods were used with the aim of shedding light on banks' ability to detect credit card fraud. Real data from January 2023 is used to create the model, with an observation count

of 13050. The dataset was obtained from a public capital bank and has not been shared because it contains customer information for security reasons. The dependent variable of the model consists of two categories: fraud and non-fraud. Independent variables are not detailed. However, other studies have observed that independent variables are not shared. Unlike previous studies, a model proposal is prepared using some features.

During model setup, algorithms with high prediction performance for classification problems are preferred. In this context, Logistic Regression, Decision Tree, K-Nearest Neighbour, Random Forest and Gradient Boosting algorithms have been used. The accuracy scores of the algorithms used in the model setup have been determined as, Logistic Regression 92.5‰, Decision Tree 93.1‰, K-Nearest Neighbour 86.4‰, Random Forest 91.8‰, and gradient boosting 86.9‰. A detailed analysis of the models was shared comparatively, and unlike previous studies, both ROC-AUC curves and confusion matrices of the models were individually shared in the test performance metrics. In addition, the precision and F1 score metrics of the models are also presented.

Looking at the test results of the models, it is determined that they have high performance in predicting credit card fraud. In this context, the study has demonstrated the successful construction of prediction models using supervised machine learning techniques. Five algorithms were offered as alternatives to the study. As a limitation of this study, the dataset was not publicly available. In addition, the "transaction time" information from the dataset was excluded due to the risk of anomalies. In this context, by adding this information, which was excluded from the dataset for other studies, a new model proposal can be made.

1. Giriş

Teknolojideki dijitalleşme gelişmelerinin artmasıyla kişi ve kurumlardaki parayı yönetme şekli de beraberinde değişmiştir. Birçok ödeme sistemi dijital platformlara muazzam bir şekilde geçiş yapmıştır (Afriyie ve ark., 2023). Bu bağlamda bankacılık sektörü de dijitalleşme yolunda hızlı bir ivme kazanırken müşterilerine de daha iyi bir hizmet verebilmek ve pazar paylarını artırmak adına dijital platformlarda daha fazla yer almaya başlamıştır. Dolayısıyla günümüz dünyasında ürün ve hizmet pazarlamasında e-ödeme sistemleri vazgeçilmez hale gelmiştir (Unogwu & Filali, 2023).

Dijitalleşmenin gelişmesiyle birlikte kredi kartı harcamaları da e-ödeme sistemlerinde yoğun bir artış göstermiştir. Dijital platformlar üzerindeki bu gelişim ve büyüme müşteri davranışlarının da çok yönlü olmasını beraberinde getirmiştir. Bunun yanı sıra harcama yöntemleri değişmiş ve bunların beraberinde bankaların kredi kartı harcamalarında dolandırıcılık işlemi olan vakaları yakalaması oldukça güç hale gelmiştir.

Kredi kartı dolandırıcılığı hem kredi kartı kullanıcısı için maliyet doğururken hem de bankalar için ciddi maliyetlere sebebiyet vermektedir. Dolayısıyla bankalar dinamik bir yapıya sahip olan kredi kartı harcamalarında dolandırıcılık işlemlerini tespit etmek adına da operasyonel ve mali olarak külfetlere katlanmaktadır. Bununla birlikte bankalar kredi kartı dolandırıcılığını tespit etmek için geleneksel yöntemleri terk edip modern yöntemler diyebileceğimiz yapay zekâ temelli makine öğrenmesi gibi yöntemlere başvurabilmektedir.

Bu çalışmada da amaç bankaların operasyonel yükünü hafifletmek adına bankaların kendi bünyelerinde de kullanabilecekleri modern bir yönteme dayanan yapay zekâ temelli bir yöntem sunmaktır. Kredi kartı sahteciliği ile ilgili literatür incelendiği zaman sınıflandırma problemlerinde (problemlerin kategorik olduğu) denetimli makine öğrenmesi tekniklerinin doğru tahmin etme oranlarının yüksek olduğu tespit edilmiştir.

Yapılan çalışmalar incelendiği zaman gerçek olmayan veriler ile de çözüm önerisi sunulmuş olduğu görülmüştür. Bu bağlamda gerçek veriler ışığında literatürde önerilen söz konusu algoritmaların performanslarının test edilmesinin faydalı olacağı düşünülmüştür. Bilişim sektöründe yapay zekâ temelli makine öğrenmesi kullanımı ivme kazanmıştır. Teknolojinin gelişmesiyle birlikte diğer sektörler gibi bankacılık sektörü de geleneksel yöntemleri terk edip çağa ayak uydurup sistemsel alt yapılarını otomatize etmek adına adımlar atmaktadır. Makine öğrenmesi yöntemlerini kullanmak da bu adımlardan biri olabilir.

Literatürde bulunan/yapılan birçok çalışmanın süreç içerisinde karşılaşıldığı zorlukları olabilir. Bu kapsamda kredi kartı dolandırıcılık işleminin tespit edilmesinin de birçok zorluğu bulunmaktadır. Bunun en temel sebebi de dinamiği yüksek bir yapıya sahip olması ve böylelikle benzersiz senaryolar üretmesidir. Bununla birlikte kredi kartı işlem yapısının dinamik olması problemin çözümsüz olduğu anlamına gelmemektedir. Müşteri harcama davranışlarının daha sistematize edildiği durumda makine öğrenmesi yöntemlerinin kullanılması kredi kartı sahtecilik işlemlerini tahmin etmede yüksek performans sergileyebilir.

Çalışmada Python programlama dili aracılığıyla denetimli makine öğrenmesi teknikleri tercih edilmiştir. Çalışmada literatür baz alınarak bir derleme yapılmış böylelikle sınıflandırma problemlerinde tahminleme performansı en yüksek olan algoritmalar tercih edilmiştir. Bu algoritmalar Rassal Orman, Gradyan Güçlendirme, K-En Yakın Komşu, Karar Ağaçları ve Lojistik Regresyon algoritmaları olup oluşturulan modellerin kredi kartı işlemlerinin sahte olup olmama durumunu tahmin etme performansının yüksek olduğu tespit edilmiştir. Modellerin hata matrisleri tek tek incelenmiş olup en az hata ile tahmin yapan algoritmanın Karar Ağacı algoritması olduğu en fazla hatalı tahmin yapan algoritmanın ise Gradyan Güçlendirme algoritması olduğu görülmüştür.

2. Literatür

Kredi kartı işlemlerinde sahtecilik (fraud) tespiti hakkında yapılan çalışmalarda tespit edilen en önemli bulgulardan biri veri setine ulaşılması ve söz konusu veri setine ulaşıldığı taktirde de veri kümesinde ciddi dengesizlikler görülmesidir. Bu bağlamda da veriler ya simülasyon ortamda oluşturulmakta ya da kaggle gibi kamuya açık platformlardan temin edilmektedir.

İncelenen çalışmalar gerçek olmayan veriler üzerinden yola çıkarak çözüm önerisi sunmuş olup çalışmamızda diğer çalışmalardan farklı olarak gerçek veriler ile literatürde önerilen algoritmalar test edilmiştir. Bu bağlamda bir bankadan temin edilmiş olan veri seti ile sınıflandırma performansı yüksek olduğu kabul gören algoritmalar aracılığıyla model önerisi sunulmuştur. Model kurulumunda algoritmaları yormayan az sayıda öz nitelik ile algoritmaların performansı gösterilmeye çalışılmıştır. Bunun yanı sıra yurt içi çalışmalarında, makine öğrenmesi teknikleriyle kredi kartı sahteciliği tespit etme çalışmaları yurt dışı çalışmalara kıyasla daha az olduğu görülmüştür. Bu çalışmayla birlikte denetimli makine öğrenmesi tekniklerinin öneminden bir kez daha kısaca bahsedilmiştir. Gerek literatürde çalışmaların artması gerekse bankaların ve finans kurumların bu tekniklerden daha çok yararlanabilmesi için; müşteri bilgisi, müşteri davranışı ve harcama bilgilerinin sistematize edilmesi gerekebilir. Makine öğrenmesi yöntemlerinin kullanılabilmesi için verilerin dağınık değil kümelenmiş olması algoritmaların müşteri davranışlarını tespiti öğrenmesi açısından kolaylık sağlayabilir. Veri setinin düzenli olması halinde banka ve finans kurumlarının kredi kartı sahtecilik işlemi tespitinde denetimli makine öğrenmesi tekniklerine yönelmesi sağlanabilir.

Yapılan çalışmalarda ve bu araştırmamızda tespit edilen en önemli bulgunun veri setinin dağınık olması olduğu belirtilmişti. Veri setinin düzenli olması durumunda denetimli makine öğrenmesi

yönteminin doğru tahmin yapabilme başarısı oldukça yüksek olduğu görülmüştür. Bu çalışmada da veri seti düzenli hale getirilmiş ve ayırt etme performansı yüksek olan beş algoritma kullanıcılara kolaylık olması açısından sunulmuştur. Bununla birlikte denetimli makine öğrenmesinin tüm performans metrikleri de gösterilerek kapsamlı bir çalışma elde edilmeye çalışılmıştır.

Osisanwo F.Y ve ark. (2017), denetimli makine öğrenmesi algoritmaları: sınıflandırma ve karşılaştırma adlı çalışmalarında makine öğrenmesinin günümüz bilgisayar teknolojilerindeki öneminden bahsederek denetimli öğrenme tekniklerinden yedi algoritmayı karşılaştırmış ve en iyi performans gösteren algoritmanın Rassal Orman ve Naif Bayes olduğu tespit edilmiştir.

Ren Z ve ark. (2023), yarı denetimli makine öğrenmesi adlı çalışmalarında makine öğrenmesi; denetimli makine öğrenmesi, denetimsiz makine öğrenmesi, yarı denetimli makine öğrenmesi ve pekiştirmeli makine öğrenmesi olarak incelemişlerdir. Araştırmaları neticesinde performansı en yüksek yöntemin denetimli makine öğrenmesi olduğunu belirtmişlerdir.

Afriyie ve ark. (2023), çalışmalarında makine öğrenmesi denetimli öğrenme tekniği kullanarak bir model önermeyi amaçlamışlardır. Tahminleme modellerinde Rassal Orman, Lojistik Regresyon ve Karar Ağaçları algoritmaları kullanılmış olup performans metriği en yüksek olan Rassal Orman (Random Forest) algoritması ile kurulan modeli önermişlerdir.

Unogwu ve Filali (2023), çalışmalarında makine öğrenmesi tekniklerini kullanmış olup verilerin dengesizliğini önlemek adına da SMOTE (sentetik azınlık yüksek örneklem tekniği) tekniği kullanılmıştır. Model oluşumunda Naif Bayes (Naive Bayes), Rassal Orman (Random Forest) ve Çok Katmanlı Algılayıcılar (Multilayer Perceptrons-MLP) algoritmaları kullanılmıştır. Tahminleme modellerinde en yüksek doğruluk skorunu %99,95 ile Çok Katmanlı Algılayıcılar (Multilayer Perceptrons-MLP) modelinin vermiş olduğu ifade edilmiştir.

Göy ve ark. (2020), çalışmalarında kamu kullanımına açık olan bir veri kümesi kullanarak model önerisinde bulunmuşlardır. Aynı zamanda bu veri kümesindeki dengesizlik problemini çözmek için örnekleme yöntemlerinin beraber olarak kullanıldığı hibrit bir yöntem kullanmışlardır. Çalışmada K-En Yakın Komşu, Lojistik Regresyon ve AdaBoost algoritmaları kullanılmış olup modellerin performans metriği olarak AUC leri de paylaşılmıştır. K-En Yakın komşu algoritması ile kurulan modelin doğruluk skoru %99,9 olarak tespit edilmiştir.

Alraddadi (2023), çalışmasında makine öğrenmesi denetimli öğrenme tekniği kullanmış olup Karar Ağaçları algoritması ile bir model önerisinde bulunmuştur.

Madhurya ve ark. (2022), çalışmalarında makine öğrenmesi tekniklerinde birkaç yöntem kullanarak hibrit bir çalışma göstermişlerdir. Modellerinde Rassal Orman, Destek Vektör Makineleri, K-En Yakın Komşu ve Lojistik Regresyon yöntemlerini denemişlerdir. Çalışma neticesinde K-En Yakın Komşu kredi kartı dolandırıcılığını tespit etmede en etkili yöntem seçilmiştir.

Çilburunoğlu (2023), çalışmasında kredi kartı dolandırıcılığının tespit edilmesi adına makine öğrenmesi teknikleri kullanmış olup karşılaştırmalı bir analiz yapmıştır. Bu çalışmada Rassal Orman, Yapay Sinir Ağları, Destek Vektör Makineleri, Lojistik Regresyon ve Karar Ağaçları algoritmalarını kullanmıştır. Model sonuçları detaylı incelendiğinde her modelin kendi çalışma tekniğine göre farklılık gösterebileceği belirtilmiş olup genel olarak uygulanan tüm modellerin doğruluk skoru ve performans metrikleri yüksek doğruluk göstermiş olduğu ifade edilmiştir.

Kılıç (2023), çalışmasında kredi kartı dolandırıcılığının tespit edilmesi adına simülasyon yöntemi ile elde edilen verilerden makine öğrenmesi tekniklerini kullanarak model oluşturmaya çalışmıştır. Bu çalışmada Rassal Orman, Gradyan Güçlendirme, Yapay Sinir Ağları ve Karar Ağları algoritmaları

kullanarak model oluşturulmaya çalışılmış ve modellerin performans sonuçları karşılaştırılmıştır. En başarılı tahminleme modelinin Gradyan Artırma olduğu ifade edilmiştir.

Noviandy ve ark. (2023), çalışmalarında dijitalleşmeyle birlikte kredi kartı harcamaların artığını ve beraberinde kredi kartı dolandırıcılık işlemlerinin de yükseldiğini belirtmişlerdir. Bu bağlamda bankaların geleneksel yöntemlerinin kredi kartı dolandırıcılığını tespit etme de yetersiz kaldığı ifade edilmiştir. Çalışmada veri düzenleme de SMOTE yöntemi kullanılarak makine öğrenmesi tekniği ile Aşırı Gradyan Güçlendirme (XGBoost) algoritması ile model kurulmuştur. Modelin doğruluk skoru %99,96 olarak tespit edildiği ifade edilmiştir.

Yeşilyurt (2023), kredi kartı sahteciliğinin yapay sinir ağları ile tespiti adlı çalışmasında kaggle veri tabanından elde edilen 5000 veri seti ile bir model önerisinde bulunmuş olup yapay sinir ağları yöntemi ile kredi kartı işleminin sahte olup olmamasını tahmine etme modeli önermiştir. Önerilen modelin performansının %98,44 olduğu tespit edilmiştir.

Ay (2022), kredi kartı dolandırıcılığının tespitinde yeniden örnekleme tekniklerinin kullanımı adlı çalışmasında European Cardholders veri kümesi ile bir çalışma yapmış olup veri kümesindeki dengesizlikleri çözmek için sentetik azınlık örnekleme tekniği ve rastgele az örnekleme metotları kullanmıştır. Çalışma neticesinde Rassal Orman algoritmasının başarılı olduğu görülmüştür.

3. Uygulama- Veri Seti

Literatür incelendiği zaman kredi kartı sahteciliği tahmin etme çalışmalarında veri seti temin etmenin ciddi efor gerektirdiği anlaşılmıştır. Bu kapsamda yapılan çalışmalarda veri setleri ya simülasyon ortamda oluşturulmakta ya da kamuya açık platformlardan temin edilen aynı veriler kullanılmaktadır. Bu çalışmada güncel ve gerçek vakalar ile literatürde performansı yüksek kabul gören algoritmalar ile modellerin kredi kartı sahteciliğini doğru tahmin edip etmediği tespit edilmeye çalışılmıştır.

Kredi kartı işlemlerinde sahte/dolandırıcılık vakalarını doğru ve güvenilir bir şekilde tespit etmek adına yapay zekâ temelli istatistiki yöntemler de kullanılmaktadır. Bu kapsamda sınıflandırma problemlerinde doğru tahminleme performansı yüksek olan algoritmalar bu çalışmada tercih edilmiştir.

Çalışmada denetimli makine öğrenmesi yöntemi tercih edilmiş olup denetimli makine öğrenmesi yöntemlerinde problemler kategorik olmaktadır. Hedef değişken yani bağımlı değişken belirlidir ve makine öğrenmesine uygun bir şekilde hazırlanması açısından kategorik değere 1 (sahtecilik var) ve 0 (sahtecilik yok) gibi sayısal ifade verilmektedir. Örnek vermek gerekirse başarılı-başarısız (0-1), var-yok (0-1), sahte işlem değil- sahte işlem (0-1) gibi ifade edilebilir. Bu çalışmada da hedef değişken (bağımlı değişken) kredi kartı işleminin sahte olup olmadığıdır. Makine öğrenmesinde öncelikle veri setinin ön hazırlığı tamamlanmalıdır. Veri seti ön hazırlığı tamamlandıktan sonra veri seti, eğitim ve test verisi olarak bölünmektedir. Bu çalışmada 13050 gözlem sayısı olup %80'ni eğitim %20'si test verisi olarak ayrılmıştır. Buradaki amaç öncelikle algoritmanın eğitim veri seti ile belli olan davranışları öğrenmesidir. Eğitilen algoritmada hangi işlemlerin sahte olup olmadığı etiketlenerek model çalıştırılır. Algoritma eğitildikten sonra geriye kalan test verisi ile (veri setinin %20'si) modelin doğru tahmin yapıp yapmadığı test edilir. Bu bağlamda modelin, hangi kredi kartı işlemlerinin sahte hangi kredi kartı işlemlerinin sahte olmadığını tespit edebilmekte midir sorusuna cevap buluruz. Algoritmanın doğru tahmin yapıp problemi (Sahte mi? Değil mi?) doğru ayırt edip etmediği ise performans metrikleri ile ölçülür. Makine öğrenmesinde performans ölçümleri makine

öğrenmesinin tekniğine göre değişmektedir. Denetimli makine öğrenmesinin performans ölçütleri ROC-AUC ve hata matrisi olarak belirtilebilir.

Veri setinin detayından bahsetmek gerekirse, çalışmada kamu sermayeli bir bankaya ait güncel ve gerçek veriler kullanılmıştır. Bu bağlamda çalışma dönemi olan 2023 yılı ocak ayına ait veriler temin edilmiştir. Veri setinde toplam gözlem sayısı 13050 olup elde edilen veriler müşteri bilgileri içerdiğinden bağımsız değişkenler hakkında detay bilgi paylaşılamamaktadır.

Kredi kartı işlemleri oldukça dinamik bir yapıya sahip olduğundan veri setinin hazırlanması ve makine öğrenmesi tekniğine uygun hale getirilmesi bir hayli efor gerektirmektedir. Bu bağlamda modelde anomaliler olmaması açısından veri dağılımının dengeli olup olmamasına özen gösterilmiş olup veri setinde sahte işlem ve sahte olmayan işlem dağılımına dikkat edilmiştir. Grafik 1 de hedef değişken dağılımı gösterilmiştir.

Yukarıda da ifade edildiği gibi çalışmada denetimli makine öğrenmesi tekniği uygulandığından veri seti bağımlı ve bağımsız değişken olarak ayrılmaktadır. Bu bağlamda modelin bağımlı (hedef) değişkeni sahtecilik (1), sahtecilik olmayan (0) olmak üzere iki kategoriden oluşmaktadır.

Makine öğrenmesi tekniklerinde veri setinin eğitim ve test verisi olarak bölümlendiği ifade edilmişti. Literatürde kabul görülen bölünme ise veri setini %80 ile eğitip %20 ile test edilmesidir. Bu kapsamda veri setimiz 13050 gözlem sayısından oluştuğundan %80 eğitilmiş %20'si de test edilmiştir.

Model kurulumunda Python (3.9 sürüm) programlama dilinden faydalanılmış olup aşağıda kullanılan kütüphaneler paylaşılmıştır.

```
import pandas as pd
import numpy as np
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score,confusion_matrix, classification_report, roc_curve, auc
from sklearn.metrics import precision_recall_curve
from sklearn.preprocessing import OneHotEncoder
from sklearn.compose import ColumnTransformer
from sklearn.preprocessing import StandardScaler
import matplotlib.pyplot as plt
from sklearn.linear_model import LogisticRegression
from sklearn.svm import SVC
from sklearn.tree import DecisionTreeClassifier
from sklearn.neighbors import KNeighborsClassifier
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier import seaborn
as sns
from sklearn.metrics import ConfusionMatrixDisplay
```

Grafik 1: Bağımlı Değişken Dağılımı

Çalışmada bağımsız değişkenler hakkında detay bilgi vermek gerekirse, toplamda 4 öz nitelik ile model kurulmaya çalışılmıştır (bağımlı değişken hariç). Kredi kartı sahteciliği tespit etme çalışmalarında verinin dengesiz oluşu göze çarpan bir konudur. Aynı zamanda veriler çok fazla tekli bilgiler içerebilir. Bu gözlem sayılarının çok fazla tekli (benzersiz) bilgi içermesi tahmin ediciyi etkileyen bir girdi olarak model kurulumunda engel teşkil edebilir (Çolak, 2021). Bu durumda da müşteriye ait olan bilgiler ya da işleme ait özel nitelikler çok fazla farklılık içerdiğinden müşterilere ait verileri kümelemek zor olabilmektedir. Makine öğrenmesi tekniklerinde ise bilgilerin bu kadar benzersiz, farklı olması istenen bir durum değildir. Makine öğrenmesi yinelemeli verileri kullanarak bir model oluşturur (Şahinaslan ve ark., 2023). Bu bağlamda çalışmada veri setinde işlem saati, müşteri doğum tarihi gibi bağımsız değişkenler çıkartılmıştır. Dolayısıyla az sayıda öz nitelik ile de performansı yüksek bir tahminleme modeli gösterilmeye çalışılmıştır.

Verinin bağımsız değişkenleri aşağıda kısmen paylaşılmış olup bağımsız değişkenlerde öz nitelik çıkartma ve öz nitelik geliştirme yöntemlerine başvurularak bağımsız değişkenler nihai haline getirilmiştir.

Tablo 1: Bağımsız Değişkenler

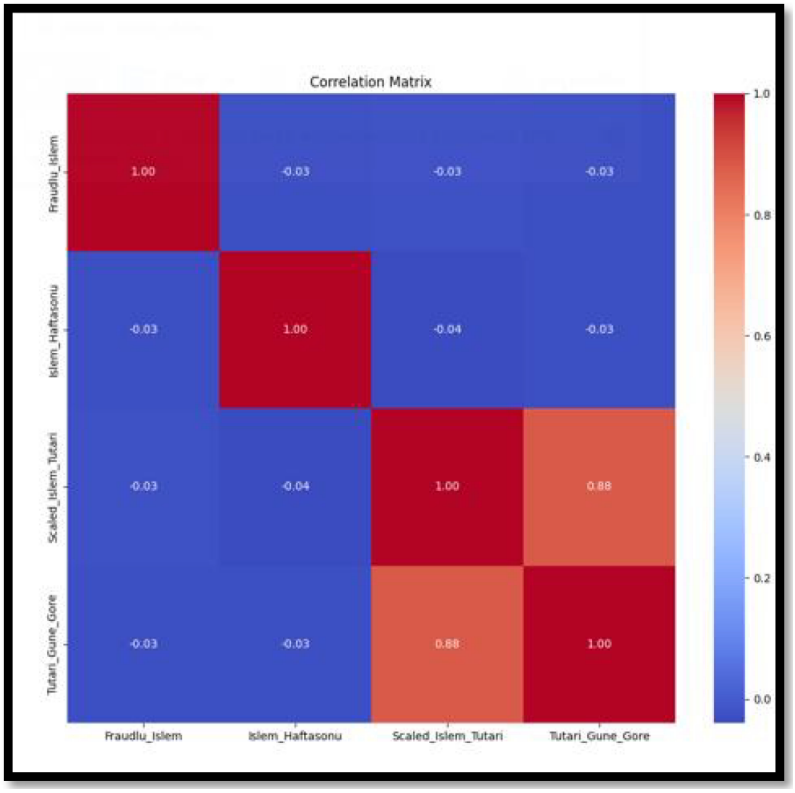
Müşterinin Cinsiyeti (müşteri gerçek kişi ise)
Müşterinin Nev-i (müşteri tüzel kişi ise)
Meslek
Öz nitelik 4
Öz nitelik 5
Öz nitelik 6

3.1. Korelasyon Analizi

Korelasyon analizi, iki değişken arasındaki pozitif ya da negatif ilişkinin olup olmadığını göstermeye yarayan bir analizdir. Uçtan uca yapılan model çalışmalarında, model kurulmadan önce bağımsız değişkenler arasındaki ilişkinin kontrol edilmesi faydalı olabilir. Gerektiği durumda öz nitelik veri setinden çıkartılabilir bu durum çalışmanın içeriğine göre değişebilmektedir. Aşağıdaki grafik bilgi amaçlı paylaşılmış olup bağımsız değişkenlerin aralarındaki ilişkinin modelimizi etkilemediği gösterilmeye çalışılmıştır. Örneğin öz nitelikler (bağımsız değişken) arasında işlem

tutarları için pozitif korelasyon olduğu görülürken diğer değişkenler için ilişkinin çok az olduğu, negatif korelasyon olduğu (-0.03 ve-0.04) tespit edilmiştir.

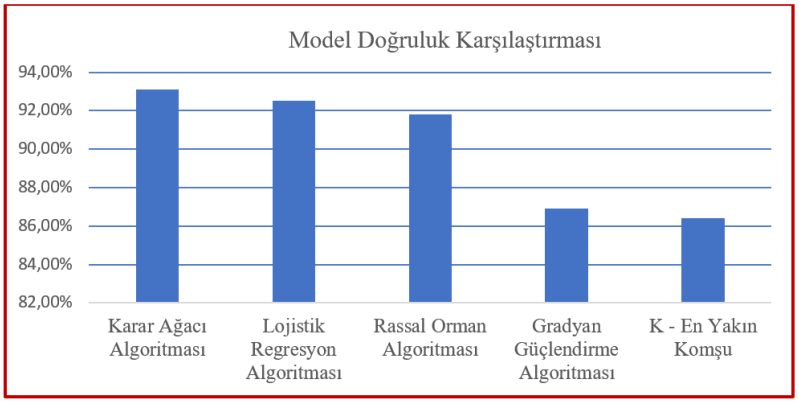
Grafik 2: Korelasyon analizi



3.2. Model Tahmin Sonuçları

Python programlama dili kullanılarak denetimli makine öğrenmesi teknikleriyle Lojistik Regresyon, Karar Ağacı, K-En Yakın Komşu, Rassal Orman ve Gradyan Güçlendirme algoritmaları kullanılmıştır. Modelde verinin %80'ni eğitilmiş %20 si ise test verisi olarak bölümlenmiştir. Bu algoritmalar ile kurulan modellerin doğruluk skor sonuçları genel olarak aşağıda paylaşılmış olup her bir algoritmanın detay sonuçları ise algoritmaların alt başlığı altında ifade edilmiştir.

Grafik 3: Test Doğruluk Skoru (Accuracy)



Denetimli makine öğrenmesi tekniklerinde kurulan modellerin başarısını ölçmek için doğruluk (accuracy) skorlarına bakılabilir. Doğruluk skorları modelin ne kadar doğru tahminleme yaptığını göstermektedir. Ancak bir modelin ne kadar doğru çalıştığını gösteren tek başarı kriteri accuracy değildir. Çalışmada performans metriği olarak ROC-AUC, hata matrisi, precision, F1 skoru ve recall sonuçları da paylaşılmıştır.

Hata matrisinden yola çıkılarak (Sorhun, 2021); doğru negatif (DN), yanlış negatif (YN), yanlış pozitif (YP) ve doğru pozitif (DP) tablosundan hareketle tahmin edilmiş vakalar ile modelin tahmin performansı ölçülebilir. Konuyla ilgili detay bilgi modellerin hata matrislerinde açıklanmıştır.

		Tahmin Edilen Sınıflar	
		Negatif 0	Pozitif 1
Gerçek Sınıflar	Negatif 0	DN	YP
	Pozitif 1	YN	DP

Accuracy (doğruluk), Modelin gerçek bağımlı (hedef) değişkeni ne kadar doğru tahmin ettiğini göstermektedir.

$$Doğruluk = \frac{DP + DN}{DP + DN + YP + YN} \tag{1}$$

Precision (kesinlik), doğru bir şekilde pozitif tahmin edilen gözlemlerin gerçekte ne kadarının doğru olduğunu göstermektedir.

$$Kesinlik = \frac{DP}{DP + YP} \tag{2}$$

Recall (duyarlılık), doğru bir şekilde pozitif olarak tahmin edilen gözlemlerin ne kadar başarılı tahmin edildiğini göstermektedir.

$$Duyarlılık = \frac{DP}{DP + YN} \tag{3}$$

F1 Skoru, Kesinlik ve duyarlılığın harmonik ortalamasıdır.

$$F1 = 2 * \frac{(Kesinlik * Duyarlılık)}{(Kesinlik * Duyarlılık)} \tag{4}$$

Grafik 3 incelendiğinde sırasıyla, Lojistik Regresyon algoritması için verinin %92,5, Karar Ağacı algoritmasının verinin %93,1, K- En Yakın Komşunun verinin %86,4, Rassal Orman algoritması için verinin %91,8, Gradyan Güçlendirme algoritmasının verinin %86,9 oranında doğru tahminleme yaptıkları görülmüştür.

3.2.1. Lojistik Regresyon Algoritması Model Sonuçları

Lojistik regresyon algoritması istatistiğe dayalı bir algoritma olup adında regresyon ifadesi geçse bile bir sınıflandırma problemi algoritmasıdır. Bu algoritma, bağımlı değişkenlerin kategorik olduğu durumlarda bağımlı değişken ile bağımsız değişkenler arasındaki ilişkinin istatistiksel yöntemler sayesinde incelemektedir (Taşçı ve Onan, 2016).

Lojistik regresyon algoritmasının formülasyonu aşağıda paylaşılmıştır (Goy ve ark., 2019).

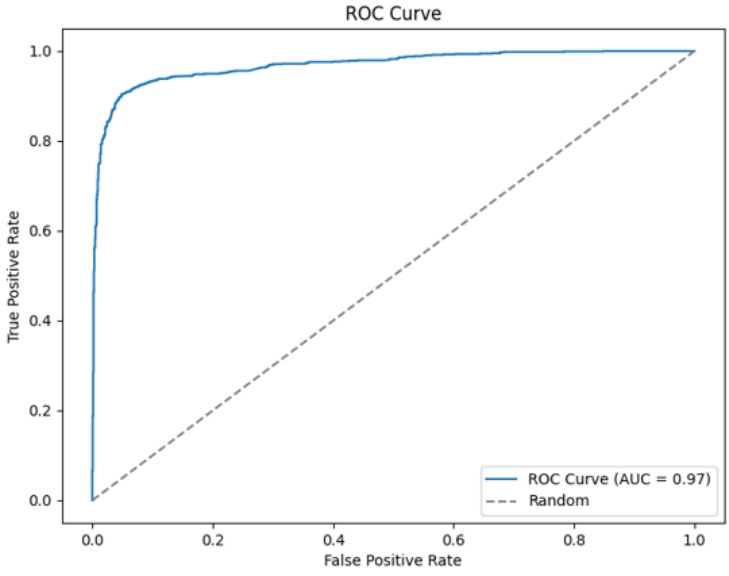
$$y = \frac{1}{1 + e^{-(a_0 + a_1 x)}} \tag{5}$$

Tablo 3: Lojistik Regresyon Test Model Sonuçları

Lojistik Regresyon Accuracy: 0.92
Lojistik Regresyon AUC: 0.97
Lojistik Regresyon Precision: 0.93
Lojistik Regresyon Recall: 0.92
Lojistik Regresyon F1-Score: 0.91

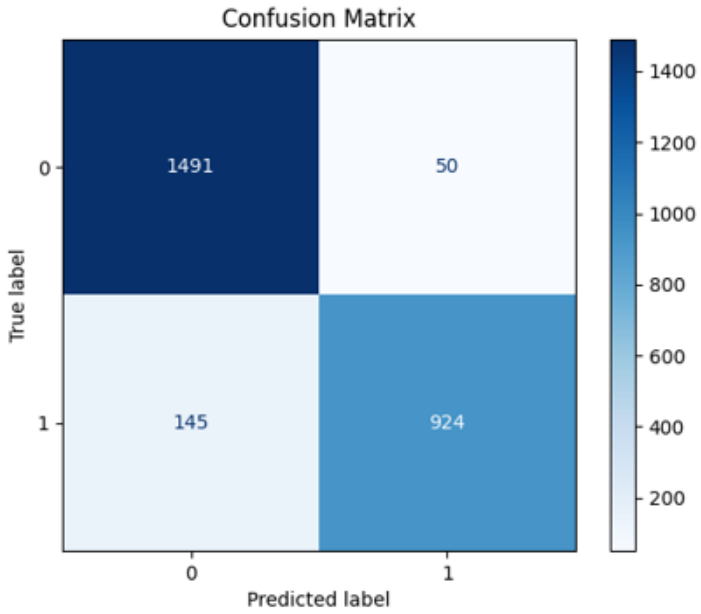
Tablo 3 incelendiğinde, modelin doğru çalışıp çalışmadığını test edebilmek adına veri setinde bölümlenen %20'lik test veri seti için model çalıştırılmıştır. Bu bağlamda 2610 gözlem sayısı için verilerin etiketleri (hedef değişken) verilmeksizin model çalıştırıldığında modelin kredi kartı işleminin sahte olup olmadığını %92 oranla doğru tahmin ettiği tespit edilmiştir. Performans metriklerinde ROC -AUC grafiği ayrıca paylaşılmış olup AUC değeri 1'e ne kadar yakın ise modelin o kadar doğru çalıştığını ifade etmektedir.

Grafik 4: Lojistik Regresyon ROC AUC Eğrisi



ROC sınıflandırma problemlerinde kullanılan ve modelin ne ölçüde başarılı öngördüğünü gösteren performans ölçüm tekniğidir. ROC -AUC eğrisi bize modelin ne kadar başarılı olduğunu gösterir. Bu eğri de AUC değerinin 1'e yakın olması istenen bir durumdur (Sorhun, 2021).

Grafik 5: Hata Matrisi (Confussion Martix)



Grafik 5 incelendiğinde, lojistik regresyon algoritması ile kurulan modelin test sonuçlarında hata matrisine bakıldığında grafiğin sol tarafında görülen gerçek etiketlerde (true label) kredi kartı sahteciliği (fraud) olarak belirlenen 145 işlem olduğu ancak modelin bu 145 işlemi sahtecilik olmayan (0) kredi kartı işlemi olarak tahmin ettiği görülmektedir. Bu bağlamda modelin dolandırıcılık olan 145 adet işlemi kaçırdığı yani yakalayamadığı görülmüştür. Aynı şekilde 50 kredi kartı işlemin aslında sahtecilik işlemi olmadığı (0) ancak modelin sahtecilik olmayan bu 50 işlemi sahte işlem olarak (1) tespit ettiği görülmüştür.

3.2.2. Karar Ağacı Algoritması Model Sonuçları

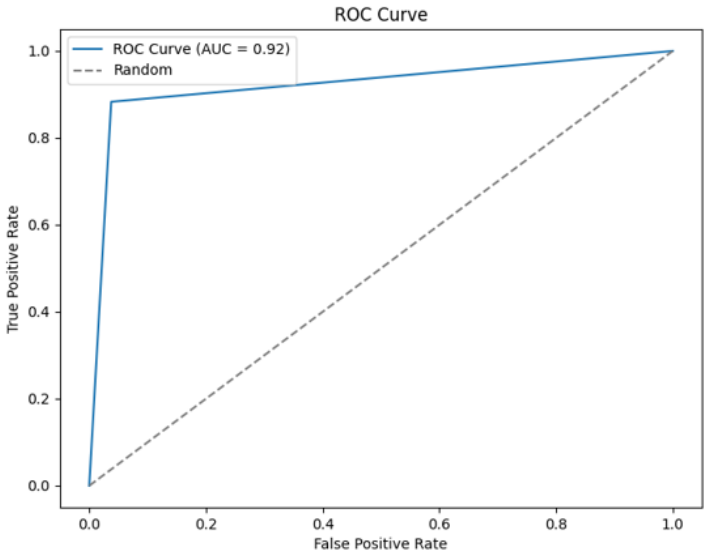
Karar ağacı algoritması şematik olarak ağaca benzeyen kök, boğum, dallar ve yaprak görüntüsünü anımsatmaktadır. Makine öğrenmesi tekniğinde hem sınıflandırma hem de regresyon problemlerinde başvurulan bir yöntemdir (Nie ve ark., 2011).

Tablo 4: Karar Ağacı Test Model Sonuçları

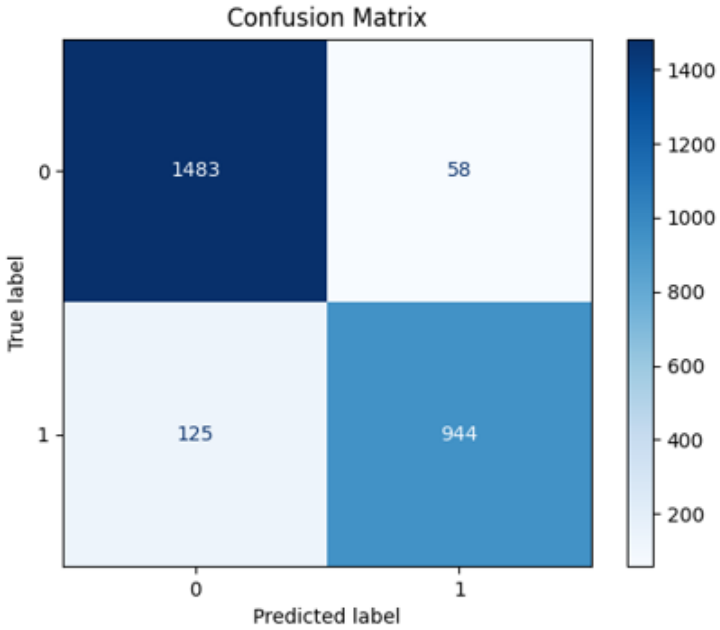
Karar Ağacı Accuracy: 0.92
Karar Ağacı AUC: 0.92
Karar Ağacı Precision: 0.93
Karar Ağacı Recall: 0.92
Karar Ağacı F1-Score: 0.91

Karar ağacı algoritması sınıflandırma problemlerinde performansı yüksek olan bir algoritmadır. Tablo 4 test sonuçları incelendiğinde yapılan kredi kartı işlemlerinin %92'sini doğru tahmin ettiği tespit edilmiştir. Hata matrisinden hareketle kesinlik, duyarlılık ve F1 skoru oranları da benzerdir. ROC eğrisine bakıldığında da eğrinin yukarı kaydığı görülmektedir. Bu durum modelin ne kadar doğru sınıflandırdığını göstermektedir.

Grafik 6: Karar Ağacı ROC AUC Eğrisi



Grafik 7: Hata Matrisi (Confussion Martix)



Grafik 7 incelendiğinde, karar ağacı hata matrisinde gerçek etiketlerde (true label) kredi kartı sahteciliği (fraud) olarak gerçek 125 işlem olduğu ancak modelin bu 125 işlemi dolandırıcılık olmayan (0) kredi kartı işlemi olarak tahmin ettiği görülmektedir. Model dolandırıcılık olan 125

işlemi kaçırmıştır. Aynı şekilde 58 işlemin aslında dolandırıcılık olmadığı (0) ancak modelin dolandırıcılık olmayan 58 işlemi dolandırıcılık işlemi olarak (1) tahmin ettiği görülmüştür.

3.2.3. K En Yakın Komşu Algoritması Model Sonuçları

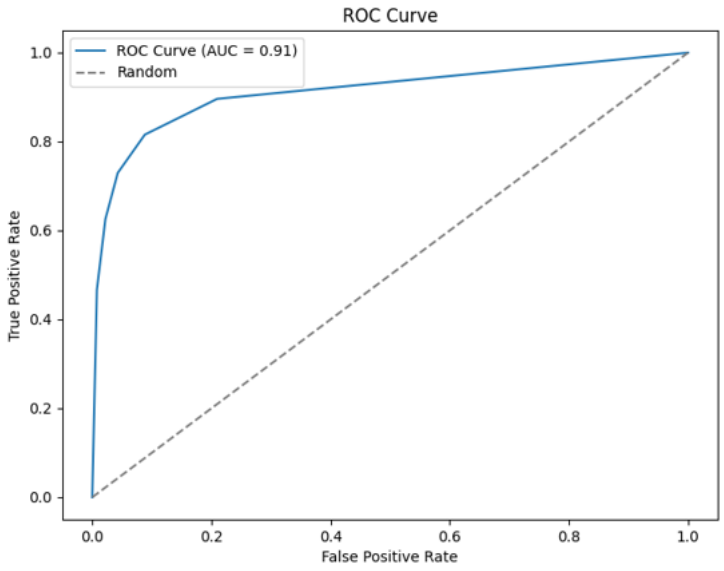
K-En Yakın komşu kategorik sınıflandırma problemlerinde sıklıkla başvurulan bir algoritma yöntemidir. "K" harfi komşu sayısını ifade ediyor olup en yakın komşu sayısını belirlemektedir. Bu algoritma en yakın mesafedeki "K" adet komşulara olan uzaklığı hesaplarken üç tip fonksiyon kullanmaktadır. Bunlar; Öklid mesafesi, Manhattan mesafesi ve Minkowski mesafesidir. Fakat en yaygın kullanılan Öklid mesafesi olmaktadır (Sorhun, 2021).

Tablo 5: K-En Yakın Komşu Test Model Sonuçları

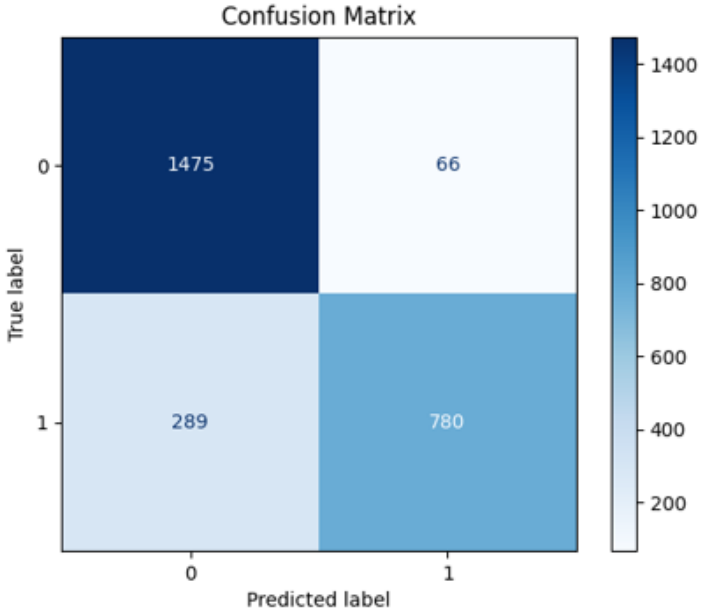
K En Yakın Komşu Accuracy: 0.86
K En Yakın Komşu AUC: 0.91
K En Yakın Komşu Precision: 0.87
K En Yakın Komşu Recall: 0.86
K En Yakın Komşu F1-Score: 0.83

Tablo 5 incelendiğinde, modelin performansı makine öğrenmesi tekniğine göre "çok iyi" olarak kabul edilen bir performans sergilemiştir. Bunun anlamı model kredi kartı işlemlerinin sahte olup olmadığını ayırt etmekte başarılıdır. ROC-AUC eğrisine de bakıldığında AUC değeri 1'e yakın, ROC eğrisi de yukarı yönlüdür.

Grafik 8: K En Yakın Komşu ROC AUC Eğrisi



Grafik 9: Hata Matrisi (Confussion Martix)



Hata matrisi incelendiğinde, gerçek etiketlerde kredi kartı sahteciliği (fraud) olarak etiketlenen 289 dolandırıcılık işlemi olduğu ancak modelin bu 289 işlemi dolandırıcılık olmayan (0) kredi kartı işlemi olarak tahmin ettiği görülmektedir. Aynı şekilde 66 işlemin gerçek etiketinde dolandırıcılık olmadığı (0) ancak modelin dolandırıcılık olmayan 66 işlemi dolandırıcılık olarak (1) tahmin ettiği görülmüştür.

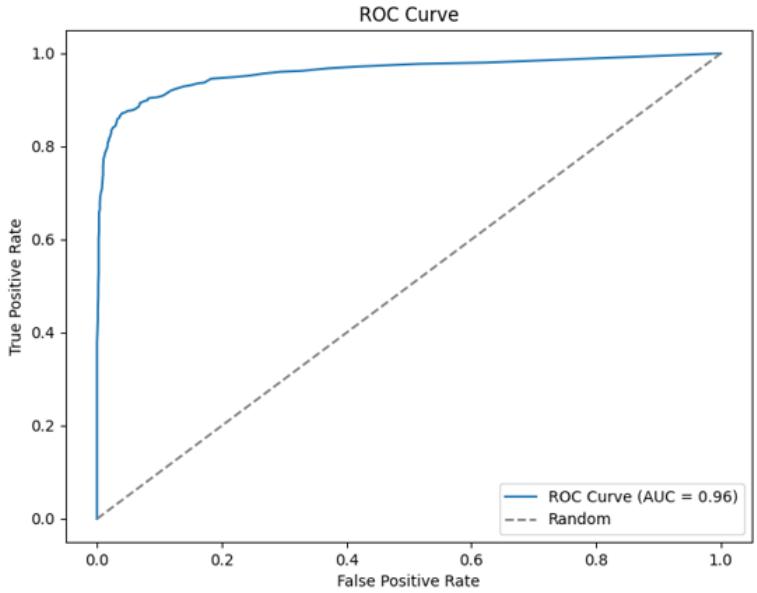
3.2.4. Rassal Orman Algoritması Model Sonuçları

Rassal orman algoritması bir ormandaki tüm ağaçlar için aynı dağılıma sahip olan ağaç tahmincilerinin bir birleşimidir. Böylece her ağaç, bağımsız olarak örneklenen ve ormandaki tüm ağaçlar için aynı dağılıma sahip rastgele bir vektörün değerlerine bağlı olmaktadır. Nihayetinde her bir ağaç ayrı bir model üretip bu modellerin performans skorlarının ortalaması alınmaktadır (Breiman, 2001).

Tablo 6: Rassal Orman Test Model Sonuçları

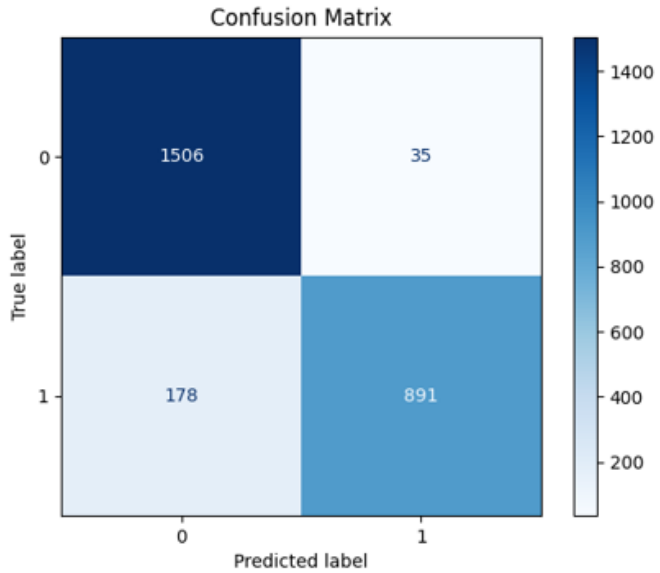
Rassal Orman Accuracy: 0.91
Rassal Orman AUC: 0.96
Rassal Orman Precision: 0.92
Rassal Orman Recall: 0.92
Rassal Orman F1-Score: 0.90

Grafik 10: Rassal Orman ROC AUC Eğrisi



Modelin performans sonuçları incelendiğinde; doğruluk, kesinlik, duyarlılık ve F1 skoru sonuçlarıyla problemi ayırt etme yeteneği sergilemiştir. ROC eğrisi yukarı yönlü olup AUC eşik değeri de 1'e yakın tespit edilmiştir. Bu bağlamda Rassal Orman algoritması sınıflandırma problemlerinde ayır etme performansı yüksek olan algoritmalardan biridir.

Grafik 11: Hata Matrisi (Confussion Martix)



Hata matrisi incelendiğinde, gerçek etiketlerde kredi kartı sahteciliği (fraud) olarak etiketlenen 178 işlem olduğu ancak modelin bu 178 işlemi kaçırarak dolandırıcılık işlemi olmayan (0) kredi kartı işlemi olarak tahmin ettiği görülmektedir. Aynı şekilde 35 işlemin gerçek etiketinde dolandırıcılık olmadığı (0) ancak modelin dolandırıcılık olmayan 35 işlemi dolandırıcılık olarak (1) tahmin ettiği görülmüştür.

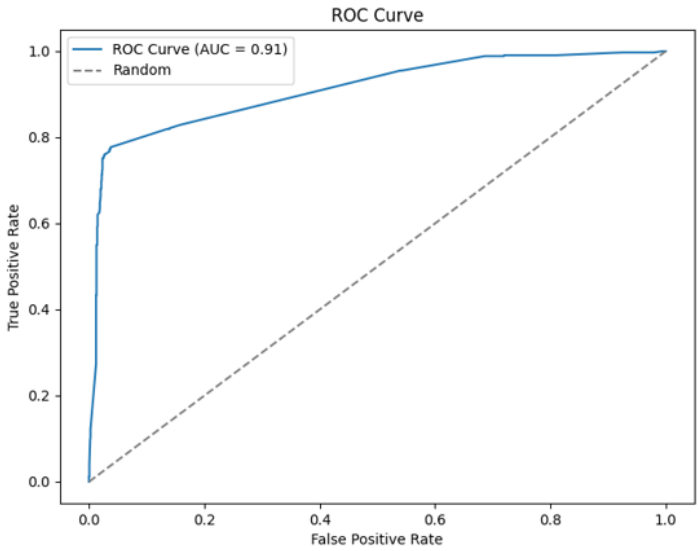
3.2.5. Gradyan Güçlendirme Algoritması Model Sonuçları

Gradyan Güçlendirme algoritması, denetimli makine öğrenmesi yöntemlerinde kullanılan bir diğer algoritmadır. Gradyan güçlendirme denmesinin sebebi, modellerin sırasıyla eğitilip ve her yeni bir modelin bir önceki modelin kusurlarını düzeltmeye odaklanmasından kaynaklanmaktadır (Hild, 2021).

Tablo 7: Gradyan Güçlendirme Test Model Sonuçları

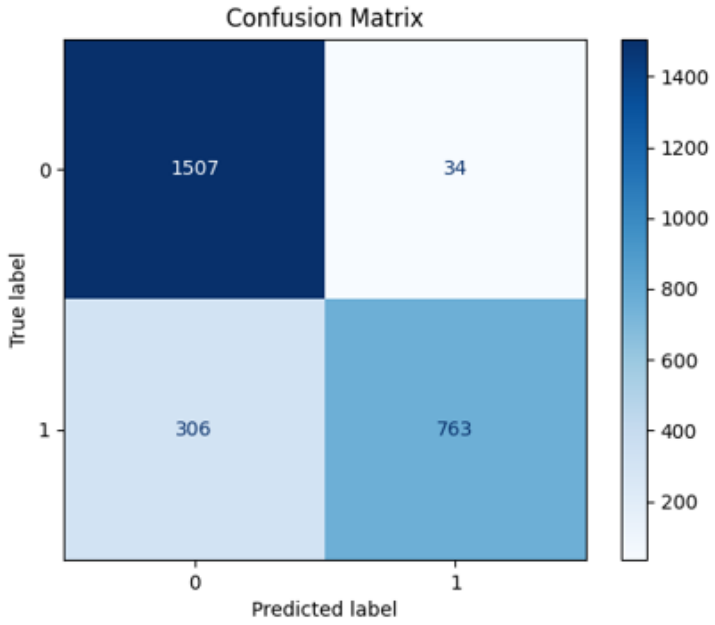
Gradyan Güçlendirme Accuracy: 0.86
Gradyan Güçlendirme AUC: 0.91
Gradyan Güçlendirme Precision: 0.88
Gradyan Güçlendirme Recall: 0.87
Gradyan Güçlendirme F1-Score: 0.84

Grafik 12: Gradyan Güçlendirme ROC AUC Eğrisi



Model performans sonuçları incelendiğinde, doğruluk (accuracy), kesinlik (precision), duyarlılık (recall) ve F1 skor (F1-score) sonuçları %80 üzeri olduğundan modelin veri setini sahte işlem olup olmadığını ayırt etme performansının yüksek olduğu tespit edilmiştir. ROC-AUC eğrisi incelendiğinde de AUC eğrisinin 1'e yakın olduğu görülmüştür.

Grafik 13: Hata Matrisi (Confussion Martix)



Hata matrisi incelendiğinde, gerçek etiketlerde kredi kartı sahteciliği (fraud) olarak etiketlenen 306 işlem olduğu ancak modelin bu 306 adet kredi kartı işlemini kaçırarak dolandırıcılık olmayan (0) kredi kartı işlemi olarak tahmin ettiği görülmektedir. Aynı şekilde 34 işlemin gerçek etiketinde dolandırıcılık olmadığı (0) ancak modelin dolandırıcılık olmayan 34 işlemi dolandırıcı işlemi olarak (1) tahmin ettiği görülmüştür.

4. Tartışma ve Sonuç

Teknolojinin gelişmesiyle birlikte globalleşme de artmıştır. Bu gelişmelerin beraberinde kişi ve kurumların ödeme alışkanlıkları da bir hayli değişmiş e-ödeme sistemi hayatımıza oldukça yerleşmiştir. Bundan yıllar önce tüketiciler nakit ödemesiz harcama alışkanlığı yokken günümüz dünyasında ise artık tüketiciler kredi kartı kullanımının birçok avantajlarından dolayı neredeyse tüm harcamalarını kredi kartı ile yapmaktadır. Özellikle dijital platformlardaki harcamalar yadsınamayacak derecede artış göstermiştir.

Modernleşmeyle birlikte bankaların kredi kartı pazar payı da artmıştır. Böylelikle bankalar, müşterilerine birçok avantaj sunan prestijli kartlar piyasaya sürmüştür. Yaşanan bu olumlu gelişmelerin yanı sıra hızlı ve kolay alışverişin güvenli bir şekilde yapılması da bankalar için çözülmesi gereken bir problem olarak gündeme gelmiştir. Bu kapsamda bu denli yoğun kredi kartı harcaması yapılan, dinamik bir yapıya sahip olan dijital platformda kredi kartı dolandırıcılığını tespit etmek bir hayli zor olabilmektedir.

Literatür çalışmaları incelendiğinde kredi kartı dolandırıcılığı ile ilgili çalışmalarda veri dengesizliği ile ilgili ciddi problemler olduğu dolayısıyla da bazı çalışmaların veri setinin simülasyon yöntemi ile elde edildiği görülmüştür. Bunun yanı sıra kamuya açık platformlarda da aynı verilerin kullanıldığı tespit edilmiştir. Bu çalışmada diğer çalışmalardan farklı olarak gerçek ve güncel verilerden yola çıkarak model oluşturulmaya çalışılmıştır. Ancak kredi kartı işlemlerinin sahte olup olmadığını tespit etme sürecinde zor olan veri setinin dağılımıdır. Saniyeler içinde milyonlarca işlem olabilmektedir. Bu bağlamda veri seti dağınık yani düzensiz olabilmektedir. Veri dağılımı düzenli

olduğunda ise yani öz nitelikleri (meslek, cinsiyet, işlem tutarı, işlem saati, işlem günü, harcama kanalı gibi) kümelenebildiğinde denetimli makine öğrenmesi tekniği sahtecilik işlemlerini tahmin etme performansı yüksek olduğu görülmüştür.

Bankalar kredi kartı işlemlerinin sahte olup olmadığını tespit edebilmek adına ciddi maliyetlere katlanabilmektedir. Bu işlemler banka bünyesinde ya da danışman firma eşliğinde hem operasyonel maliyetlere sebep olmakta hem de banka gelirini etkilemektedir. Bu çalışma ile birlikte veri setleri sistematize edilebilirse denetimli makine öğrenmesi yöntemlerinin kullanılabileceği gösterilmeye çalışılmıştır. Kullanıcılara faydalı olması açısından da bu tekniklerden başarılı performans sergileyen algoritmalar paylaşılmıştır. Bunun yanı sıra çok fazla öz nitelik kullanarak algoritmaları yoran, algoritmanın çalışma performansını etkileyen bir veri setinden ziyade az sayıda öz nitelik ile de yüksek performans sergileyen algoritma örnekleri önerilmiştir.

Çalışmanın kısıtı ise, veri seti dağılımının düzenli olması ve anomaliler olmaması açısından öz nitelik çıkartma işlemi uygulanarak "işlem saati" bilgisinin öz nitelikten çıkartılmasıdır. Bir başka çalışmada işlem saati de veri setine dahil edilerek yeni bir model önerisi sunulabilir. Bununla birlikte sınıflandırma problemlerinde yüksek performans sergileyen Naif Bayes, Aşırı Gradyan Güçlendirme gibi diğer denetimli algoritmalar denenebilir.

Çalışmada veri setinin manuel düzenlenmesi de efor maliyetini artıran bir süreçtir. Bu kapsamda bankalar veri setini otomatize eden bir sistem ile denetimli makine öğrenmesi algoritmalarında çalışabilecek bir veri dağılımı oluşturabilirlerse çalışmada önerilen algoritmalar ile yüksek performans elde edilebilen modellerin kullanılabileceği düşünülmektedir.

Çalışmanın sonuçları incelendiği zaman modellerin doğruluk skorlarının, kesinlik, duyarlılık, F1 skorları ve ROC-AUC eğrilerinin yüksek performans sergilediği gözlemlenmiştir. Çalışmada yüksek performans sergileyen algoritmalar tercih edilerek kullanıcılara alternatifler sunulması hedeflenmiştir. Bu bağlamda özellikle bir model seçimi yapılmamış olup beş başarılı algoritma alternatifi sunulmuştur. Modellerin hata matrisleri incelendiği zaman en çok hatalı tahmin yapan algoritmanın Gradyan Güçlendirme algoritması ile kurulan modelin olduğu görülmüştür.

Gradyan Güçlendirme algoritması, veri setinde gerçekte etiketi sahte işlem (fraud) olan 306 işlemin sahte olmayan (fraud olmayan) işlem olarak tahmin ettiği görülmüştür. Bu kapsamda Gradyan Güçlendirme algoritması 306 adet sahte işlemi kaçırdığı ifade edilebilir. Karar Ağacı algoritmasına bakıldığında ise, en az hata ile tahmin yapan algoritma olduğu görülmüştür. Bu bağlamda veri setinin gerçekte etiketi sahte işlem (fraud) olup ancak modelin 125 adet işlemi sahte olmayan (fraud olmayan) işlem olarak tahmin ettiği görülmüştür. Hata matrislerine bakıldığında sırasıyla en iyi performansı gösteren yani en az hatalı tahmin yapan algoritmalar; Karar Ağacı algoritması, Lojistik Regresyon algoritması, Rassal Orman algoritması, K-En Yakın Komşu ve son olarak Gradyan Güçlendirme algoritmasıdır.

Bu çalışmada Python (3.9 sürüm) programlama dili aracılığıyla yapay zekâ temelli denetimli makine öğrenmesi yöntemleri kullanılmıştır. Bu çalışmayla birlikte bankacılık sektöründe kredi kartı dolandırıcılığı tespit etme anlamında ışık tutması, bankaların veri setlerini sistematik hale getirebilmeleri durumunda yani makine öğrenmesi yapısına uygun hale getirebilmeleri durumunda (algoritmaların eğitilmesi için çok fazla tekli senaryo olmamalı) kendi bünyelerinde makine öğrenmesi tekniklerini kullanabilecekleri gösterilmeye çalışılmıştır. Çalışmada diğer çalışmaların aksine gerçek veri seti kullanılarak sınıflandırma problemlerinde performansı yüksek kabul gören algoritmalar test edilmiştir. Öz nitelik değişken sayısı az tutularak da algoritmaları yormayan bir yöntem denenmiş modellerin performanslarının yüksek olduğu görülmüştür. Denetimli makine

öğrenmesi performans ölçütleri olarak ROC-AUC, hata matrisi, doğruluk (accuracy), kesinlik (precision), duyarlılık (recall) ve F1 skor (F1-score) gibi metriklere de bakılarak çalışma güçlendirilmiştir. Bu bağlamda beş algoritmada performanslarından dolayı önerilmekle birlikte hata matrislerine bakıldığında Karar Ağacı algoritmasının daha az hata ile tahmin ettiği görülmüştür.

Hakem Değerlendirmesi: Dış bağımsız.

Yazar Katkıları: Çalışma Konsepti/Tasarım- G.A., M.R.Z.; Veri Toplama- G.A., M.R.Z.; Veri Analizi/Yorumlama- G.A., M.R.Z.; Yazı Taslağı- G.A., M.R.Z.; İçeriğin Eleştirel İncelemesi- G.A., M.R.Z.; Son Onay ve Sorumluluk- G.A., M.R.Z.

Çıkar Çatışması: Yazarlar çıkar çatışması beyan etmemişlerdir.

Finansal Destek: Yazarlar finansal destek beyan etmemişlerdir.

Peer Review: Externally peer-reviewed.

Author Contributions: Conception/Design of Study- G.A., M.R.Z.; Data Acquisition- G.A., M.R.Z.; Data Analysis/Interpretation- G.A., M.R.Z.; Drafting Manuscript- G.A., M.R.Z.; Critical Revision of Manuscript- G.A., M.R.Z.; Final Approval and Accountability- G.A., M.R.Z.

Conflict of Interest: Authors declared no conflict of interest.

Financial Disclosure: Authors declared no financial support.

ORCID:

Güner Altan 0000-0001-6189-7104
Metin Recep Zafer 0000-0002-6508-6170

KAYNAKLAR / REFERENCES

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., ... & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal, 6*, 100163.

Alraddadi, A. S. (2023). A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm. *Engineering, Technology & Applied Science Research, 13*(4), 11505-11510.

Ay, A.K. (2022). Kredi Kartı Dolandırıcılığının Tespitinde Yeniden Örnekleme Tekniklerinin Kullanımı. (Yüksek Lisans Tezi), Eskişehir Osmangazi Üniversitesi Fen Bilimleri Enstitüsü.

Breiman, L. (2001). Random forests. *Machine learning, 45*, 5-32.

Çilburunoğlu, K. (2023). Kredi Kartı Dolandırıcılık Tespitinde Makine Öğrenme Algoritmalarının Karşılaştırmalı Analizi. (Yüksek Lisans Tezi), İstanbul Gedik Üniversitesi Eğitim Enstitüsü.

Çolak, U. (2021, 30 Mayıs). https://ufukcolak.medium.com/makine-öğrenmesi-veri-ön-işleme-5-58e1ce73c1fb.

Goy, G., Gezer, C., & Güngör, V. C. (2019). Makine Öğrenmesi Yöntemleri ile Kredi Kartı Sahteciliği Tespiti. *4. Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (UBMK)*

Hild, A. (2021). Estimating And Evaluating The Probability Of Default- A Machine Learning Approach. (Master Thesis). Uppsala Universitet, Statistics İn The Faculty Of Social Sciences.

Kılıç, N. (2023). Makine Öğrenimi Algoritmaları ile Kredi Kartı İşlemlerinde Dolandırıcılık Tespiti. (Yüksek Lisans Tezi). Hitit Üniversitesi Eğitim Enstitüsü.

Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. *Global Transitions Proceedings, 3*(1), 31-37.

Nie, G., Rowe, W., Zhang, L., Tian, Y., & Shi, Y. (2011). Credit card churn forecasting by logistic regression and decision tree. *Expert Systems with Applications, 38*(12), 15273-15285.

Noviandy, T. R., Idroes, G. M., Maulana, A., Hardi, I., Ringga, E. S., & Idroes, R. (2023). Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques. *Indatu Journal of Management and Accounting, 1*(1), 29-35.

Sorhun, E. (2021). Python ile Makine Öğrenmesi. İstanbul: Abaküs Yayınları.

Şahinaslan, E., Günerkan, M., & Şahinaslan, Ö. (2023). Makine Öğrenmesinde Kategorik Veri Kodlama Tekniğinin Kullanımına Alternatif Bir Çözüm Yöntemi. *Journal of Intelligent Systems: Theory and Applications, 6*(1), 1-11.

Ren, Z., Wang, S., & Zhang, Y. (2023). Weakly supervised machine learning. *CAAI Transactions on Intelligence Technology, 8*(3), 549-580.

Taşcı, E., & Onan, A. (2016). K-en yakın komşu algoritması parametrelerinin sınıflandırma performansı üzerine etkisinin incelenmesi. *Akademik Bilişim, 1*(1), 4-18.

Osisanwo, F. Y., Akinsola, J. E. T., Awodele, O., Hinmikaiye, J. O., Olakanmi, O., & Akinjobi, J. (2017). Supervised machine learning algorithms: classification and comparison. *International Journal of Computer Trends and Technology (IJCTT), 48*(3), 128-138.

Unogwu, O. J., & Filali, Y. (2023). Fraud detection and identification in credit card based on machine learning techniques. *Wasit Journal of Computer and Mathematics Science, 2*(3), 16-22.

Yeşilyurt, F. (2023). Kredi Kartı Sahteciliğinin Yapay Sinir Ağları ile Tespiti. (Yüksek Lisans Tezi), Kütahya Dumlupınar Üniversitesi Lisansüstü Eğitim Enstitüsü.

Atıf biçimi / How cite this article

Altan , G., Zafer, M.R.(2024). Predicting credit card fraud using supervised machine learning methods: comparative analysis. *İktisat Politikası Araştırmaları Dergisi - Journal of Economic Policy Researches, 11*(2), 242-262. https://doi.org/10.26650/JEPR1433315