T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE MOBİL PARA TRANSFERİ SAHTECİLİĞİ TESPİTİ VE ÖNLENMESİ

YÜKSEK LİSANS TEZİ

Mayata NDIAYE

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. Cemil ÖZ**

Eylül 2019

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE MOBİL PARA TRANSFERİ SAHTECİLİĞİ TESPİTİ VE ÖNLENMESİ

YÜKSEK LİSANS TEZİ

Mayata NDIAYE

Enstitü Anabilim Dalı	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**

Bu tez 30.09.2019 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr.	**Dr. Öğrt Üyesi**	**Doç. Dr.**
Cemil ÖZ	**Serap KAZAN**	**Akif AKGÜL**
Jüri Başkanı	**Üye**	**Üye**

BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunum, başlıklarını eserlerinden yararlanılması durumunda bilimsel normalar uygun olarak atıfta bulunduğunu, kullanılan verilerde herhangi bir kısmın bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Mayata NDIAYE

30.09.2019

TEŞEKKÜR

Tezimin başında bitimine kadar geçen sürede bana sürekli destek olan danışman hocam Prof. Dr. Cemil Öz'e ve desteklerini benden esirgemeyen aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

ATM	: Otomatik vezne makinesi
FDS	: Sahtekârlık Algılama Sistemini
GSMA	: Grup Özel Mobil Birliği
MCC	: Matthews korelasyon katsayısı
MNO	: Mobil Ağ Operatörleri
MVNO	: Mobil Sanal Ağ Operatörü
OS	: İşletim Sistemi
RIM	: Hareket Halinde Araştırma
SE	: Güvenli Öğe
SMS	: Kısa Mesaj Servisi
TEE	: Güvenilir Yürütme Ortamı
UMOA	: Batı Afrika Para Birliği
USSD	: Yapılandırılmamış Ek Hizmet Verileri

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Sınıflandırma Algoritmaları, Veri Madenciliği, Mobil Para Hizmeti, Sahtekarlık tespiti, Kappa katsayısı, Matthews korelasyon katsayısı, Veritabanı**.**

Mobil para kullanım işlemleri dünya çapında, özellikle Afrika'da para temelli ekonomisini nakitsiz bir ekonomiye devretme potansiyel ile birlikte giderek artırmaktadır. Mobil para hizmetlerinin kullanımının artması ve her gün tasarlanan kullanım durumlarının sayısıyla, güvenlik risklerini azaltacak ve sahtekârlığı önleyecek kapsamlı bir mobil para güvenliği yaklaşımı geliştirmek zorunludur. Bazı mobil para servis sağlayıcıları, bu büyüyen tehdide milyonlarca dolar kaybetmiştir.

Bu nedenle bu araştırma, mobil para servisleri sağlayan, mobil ağ operatörlerinin sahtekârlığı önlemek ve tespit etmek için kullanabilecek önlemleri incelemektedir. Çalışma ayrıca, mobil para kullanıcılar cep telefonlarının korunması ile cep telefonlarındaki mobil para hizmetlerinin güvenliği arasındaki bağlantı hakkındaki algılarına da bakmaktadır. Bu çalışma, PAYSIM veri üreteci kullanılarak toplanan nitel ve nicel verileri ve sahtekârlığı tespit etmek için sınıflandırma algoritmalarını kullanmaktadır.

FRAUD DETECTION AND PREVENTION IN MOBILE MONEY TRANSFER BASED ON MACHINE LEARING METHODS

SUMMARY

Keywords: Classification Algorithms, Data Mining, Mobile Money Service, fraud detection; Kappa Coefficient, Matthews Correlation Coefficient, Database

The use of mobile money transaction is growing steadily throughout the world, especially in Africa, with the potential to revolutionize the continent's money-based economy into a cashless economy. With the increased use of mobile money services and the number of use cases designed every day, it is imperative to develop a comprehensive approach to mobile money security that will reduce security risks and prevent fraud. Some mobile money service providers have lost millions of dollars to this growing threat.

This research therefore examines the measures that mobile network operators providing mobile money services can use to prevent and detect fraud. The study also looks at the perception of mobile money users about the link between mobile phone protection and the security of mobile money service on their phones. This study uses qualitative and quantitative data collected using the Paysim data generator, and classification algorithms to detect the fraud in mobile money transaction.

BÖLÜM 1. GİRİŞ

1.1. Çalışmanın İçeriği

Mobil para, bankacılık hizmetlerini gerçekleştirmek için cep telefonu aboneleri tarafından telekomünikasyon platformlarının veya ağların kullanılması anlamına gelmektedir. Kısaca mobil para, abonelerin fiziksel olarak bir finans kurumuna girmeden doğrudan telefonlarından bankalara faturalarını ödemelerini, para almalarını ve m-cüzdan adı verilen sanal mobil hesaplar aracılığıyla işlem yapmalarını sağlamaktadır. Mobil paranın işlemlerinde kullanımı Afrika genelinde artmaya devam etmektedir ve Afrika'nın ekonomik gelişiminde önemli bir rol oynamaktadır. GSMA'nın (Grup Özel Mobil Birliği) mobil para raporuna göre 2017 yılı mobil para kullanımının en üst seviye çıktığı yıldır [1]. Günlük 1 milyar dolardan fazla işlem yapıldığında, mobil para sektörü, finansal hizmetlere erişim ağını genişletmek ve dijital ekonomiye açılan bir kapı olmak için küresel çaba üzerinde somut bir etki yaratmaktadır. Bu rapora göre, mobil paranın Afrika'daki telekomünikasyon şirketleri için "olması gereken" hizmetlerden biri haline gelmiştir. Örneğin, Afrika'daki en üst düzey telekomünikasyon şirketleri: Safaricom, MTN, Orange, Tigo ve Airtel, müşterilerine mobil para hizmetleri sunar ve kullanım istatistikleri gün ve gün artığını göstermektedir.

1.2. Amaç

Mobil para hizmetlerin artan kullanımı ve bunun sonucunda ortaya çıkan yeni kullanım durumları ile mobil ağ operatörlerinin ve kullanıcıların mobil para güvenliğini sağlamak için güvenlik uygulamalarını araştırmak önem kazanmıştır.

Bu çalışmanın temelinde mobil para güvenliğini sağlamak, dolandırıcılık önlemek ve kullanıcıların cep telefonu koruması ile mobil para güvenliği arasındaki bağlantılar hakkındaki algılarının anlatımı sağlanmaktadır. Son zamanlarda, bazı mobil para servis sağlayıcıları dolandırıcılık davası sayısında bir artış görmüş, bu da milyonlarca dolarlık gelir kaybıyla sonuçlanmıştır. Örneğin, Doğu Afrika (2012) gazetesi, MTN Uganda şirketinden bir çalışanın mobil para kullanıcılarından milyonlarca dolar çaldığını bildirmektedir. Ne yazık ki, Afrika'daki mobil para sahtekârlığı konusundaki araştırmalar, Doğu Afrika gibi gazetelerle sınırlı kalmış ve bunun üzerine çok az bilimsel araştırma yapılmıştır. Bundan dolayı, dolandırıcılık sorunlarının kapsamı ve niteliği henüz mobil ağ operatörleri ve mobil kullanıcılar için tam olarak tanımlanmamış, mobil para hizmetinin dolandırıcılara son derece çekici geldiği öngörülmektedir. Dünya çapında 690 milyon hesapla, mobil para, gelişmekte olan birçok pazarda dijital ekonomi için lider ödeme platformu haline gelmiştir. Bu öngörüler ışığında, mobil para hizmetlerinin kullanımının artması ve her geçen gün tasarlanan farklı profesyonel kullanım durumlarında, güvenlik risklerini azaltan ve sahtekârlığı önleyen mobil para güvenliğine yönelik kapsamlı bir yaklaşım geliştirmek zorunludur.

1.3. Çalışmanın Önemi

Mobil paraları elektronik bir ödeme sistemi olarak kullanılması, çoğu Afrika ülkelerinde yer bulunmaktadır. Mobil Ağ Operatörleri (MNO'lar) ile mobil para hizmeti sağlayan teknoloji (mobil telekomünikasyon ve bilgi sistemleri), mevcut güvenlik için belirli riskler ve elektronik ödeme sistemlerinde bulunan riskleri içerir. Bu güvenlik risklerinin nasıl ele alındığı, kullanıcılarının, mobil para hizmetinin güvenliği hakkındaki algılarını etkileyebilir. Ayrıca, mobil para abonelerinin cep telefonlarında servis güvenliği konusundaki sorumluluklarının farkındalığı, e-cüzdanlarını korumak için aldıkları bazı önlemleri etkileyebilir. Bu tez çalışması, mobil para hizmetini güvence altına almak için alınacak risklerin ve alınacak önlemlerin belirlenmesine dayanmaktadır.

1.4. Tezin Organizasyonu

Bu tez çalışması aşağıdaki verilen bölümler altında organize edilmiştir: İkinci bölümde, mobil para transferinin genel anlatımı gerçekleştirmiştir. Mobil para transfer sistemlerinin güvenliği üçüncü bölümde tartışılmıştır. Dördüncü bölüm, mobil paralarda sahtecilik riskinin önlenmesine dayanmaktadır. Beşinci bölümde sahtekârlık tespiti uygulanmaktadır. Altıncı bölümde makine öğrenmesi yöntemleriyle mobil para transferinde sahtecilik tespit çalışmalara verilmiştir. Son bölümde çalışmaların elde edilen sonuçları yorumlanmıştır.

BÖLÜM 2. MOBİL PARA TRANSFER HİZMETİNİN GENEL TANIMI

2.1. Mobil Para Transfer Hizmetlerinin Kullanımı

Mobil para hizmetlerinin kullanımı giderek insanların günlük işlemlerinin bir parçası haline gelmektedir. Bu şekilde para transferi hizmetlerini kolay ve daha az bir maliyetle yapılmaktadır. Mobil para transferinde bir kişi cep para cüzdanına para yatırabilir, bunu mobil para abonelerine ve mobil olmayan para abonelerine aktarabilir. Böylece, mobil cüzdan sahipleri uzun mesafelere para yatırmak için seyahat etmeyecek, başka şehirlerdeki ve köylerdeki ödemeler için kargo, otobüs gibi güvenli olmayan ulaşım yolları kullanmayacaktır. Mobil para transferleri, cep telefonunda birkaç işlem yapılarak gerçekleştirilebilir. Para alıcının mobil cüzdanına çevrim içi olarak aktarılır. Çoğu tüketici, cep telefonundan yapılan işlem ve ödemeleri için bu servisin kullanımı kolay ve rahat olduğu söylenebilir; Sonuç olarak, m-ödeme için pazar hızla büyümektedir. Mobil para kullanımı ve mobil ödeme Afrika ülkelerinin başta olmak üzere birçok ülkede toplumun büyük bir kısmının hayatını nakitsiz bir şekilde sürdürebilmesi için ümit vaat eden bir yeniliktir.

2.1.1. Mobil bankacılık

Mobil parayla, müşteriler artık geleneksel bir bankadaki bir banka hesabında veya elektronik para cüzdanı olarak adlandırılan Mobil Ağ Operatörü ile bir hesapta para biriktirme seçeneğine sahiptir [2]. Bu, paralarını yatırmalarını ve daha sonra, uygun olduklarında, para çekme işlemlerini yapmalarını sağlar. Müşterinin cüzdanında bulunan para, aynı zamanda, hizmet için ödeme yapmasına ve para transferleri yapmasına da izin verir.

Senegal'deki Orange Money şirketi gibi Mobil Ağ Operatörleri (MNO), elektronik cüzdan adı verilen fon tasarrufu ile sınırlı değildir. Ancak müşterilerine tüm GEM Batı Afrika Para Birliği (UMOA) Bank Otomatik vezne makinesi (ATM'lerine) (Batı Afrika Ekonomik ve Parasal Birliği'nin Inter bank Elektronik Bankacılığı) erişim sağlıyor! Orange Money kartı ile müşteriler paralarını cüzdanlarından doğrudan Otomatik ATM'lere çekebilir. Senegal'de ve hatta alt bölgede her zaman ve her yerde basit, hızlı ve mevcut olmaktadır.

2.1.2. Transfer türü

Günümüzde mobil para transferi hizmetleri ekosisteminde iki ana transfer türü bulunmaktadır: yurt içi para transferi ve uluslararası para transferleri. Yurt içi para transferi, her iki tarafın da aynı ülkede olduğu bir kişiden diğerine para aktarılan fonlar olabilir [2]. Mobil para hizmeti sağlayıcıları, abonelerinin diğer abonelere ve abone olmayan diğerlerine istedikleri zaman para aktarmalarını sağlamak için bu para transferi hizmetini önermektedir. Kayıtlı veya kayıtlı olmayan kullanıcılar her iki tarafa para aktarabilir. Kayıtlı kullanıcı için, transfer, mobil para cüzdanında, mobil paranın alıcıya aktarılacak miktara artı servis ücreti borç kaydedilerek yapılabilir. Para aktarmada sistem sembolik bir kod üretir bu kod kayıtlı olmayan bir alıcıya gönderildiğinde bu alıcı bir satıcıdan veya bankadan bu kod ile parayı çekilebilir. Benzer şekilde, abone olmayan bir mobil para kullanıcısı, bir aracı kuruluş veya bir Mobil Ağ Operatörleri (MNO) servis merkezinin hizmetlerini kullanarak transfer yapabilir. Genel olarak farklı Mobil ağ operatörleri arasında para transfer edilmez; Örneğin, bir kullanıcı A mobil para transfer servisinden B mobil para servisine para transfer edemez. Bu durumda, mobil para transfer operatörlerin birlikte hizmet sunabilmeleri için mobil para transferi ekosisteminin geliştirilmesi ve aktörlerin teşvik etmektedir [3].

Dövizler Yatırımları gelişmekte olan ülkelerde insanlar için istikrarlı bir gelir kaynağıdır. GSMA araştırmasına göre, Mobil Para Afrika'daki yedi kişiden biri (120 milyon) tarafından kullanmaktadır. Afrika ülkelerinin GSYH'sinin üçte biri kadarını temsil eden (60 milyar dolar) tutar yurtdışından kişilerce arkadaş veya aile

bireylerine mobil para transferleridir[4]. Bu göstermektedir ki, mobil para hizmeti ürünlerinin Mobil Ağ Operatörleri (MNO), tarafından ulusal ve uluslararası para transfer için yoğun bir şekilde kullanıldığı ve bu hizmetinin hızlı artırıldığı görünmektedir. Bu işlemler büyük miktarlarda işlem üretebilir ve mobil para hesapları için yeni bir tedarik kanalı sağlayabilir. Bu transferlerin faydalanıcıları, nakit olarak alınan fonları geri çekme veya bunları başka dijital işlemler için kullanma seçeneğine sahip olacaklardır. Günümüzde, 60'tan fazla Mobil Ağ Operatörü (MNO) ortaklığı bulunmaktadır. Bu operatörler küresel oyuncular (Western Union, Money Gram veya World Remit vb.), ulusal veya bölgesel OTF'ler birlikte çalışmak yürütmektedir [4].

2.1.3. Hizmetlerin ödemesi

Cep telefonuyla para ödemesi yenilikçi, hızlı ve güvenli bir ödeme şeklidir. Mobil para operatörü, bu hizmetleri ile müşterileri için daha fazla rahatlık ve verimlilik sunar. Örneğin; mobil para kullanıcısı su, elektrik, telefon, internet, sigorta faturalarını telefon ile ödeyebilir[2]. Platform kullanıcısı aynı zamanda, mobil para operatörleri ile iş birliği olan restoranlar, süpermarketler, televizyon operatörleri, taşımacılık şirketleri, benzin istasyonları vb. gibi kurumlardan almış olduğu mal ve hizmetlerin bedelini de ödeyebilir. Kamu hizmetlerinin yanı sıra kamu hizmeti kuruluşunun ofislerinde veya bankalarda, özel ödeme ağlarının satış noktalarında veya bu hizmetlerle acentelik sözleşmesi bulunan perakende mağazalarında da yapılabilir[5]. Satış noktasında ödeme, mobil para kredisi ile yapılır. Bu işlemler sadece aynı mobil para hizmetindeki aktörler tarafından yapılabilir.

2.2. Çevrenin Kurulması ve Mobil Ödeme Sistemi Arasındaki İlişkiler

Mobil ödeme sistemlerinin uygulanmasında ilgili pazar aşağıdaki aktörleri içerir. Şekil 2.1.'de mobil paranın ekonomik prensibi ve farklı aktörlerin rolleri gösterilmektedir [10].

2.2.1. Aktif kullanıcı

Kullanıcı mobil para servisinin hedefidir, bu kullanıcı abonelikle veya ön ödemeli kartla mobil operatör müşterisi olmalı ve mobil ağları kullanmalıdır. Mobil ödeme hizmetinin kullanıcısı, alıcı tarafından yapılan yakınlık işlemleri durumunda, aynı zamanda satıcı tarafından temsil edilir. Bunlar ödeme yapan ve alan insanlardan oluşur.

2.2.2. Servis sağlayıcı

Ödeme hizmetinin ana sağlayıcıları mobil operatörler ve bankalardır. Ancak, diğer birçok aktör tekliflerini çeşitlendirmek, müşterilerini genişletmek veya elde tutmak ve son olarak yeni gelir kaynakları elde etmek için bu pazara girme ile ilgilenmektedir. Sistem ödeme servis bankası, nakliye şirketi, mobil operatör sağlayan kurumlardan oluşmaktadır. Hizmet sağlayıcı, ödemeyi güvence altına almak için kendi teknolojisini kullanır.

2.2.3. Mobil operatör

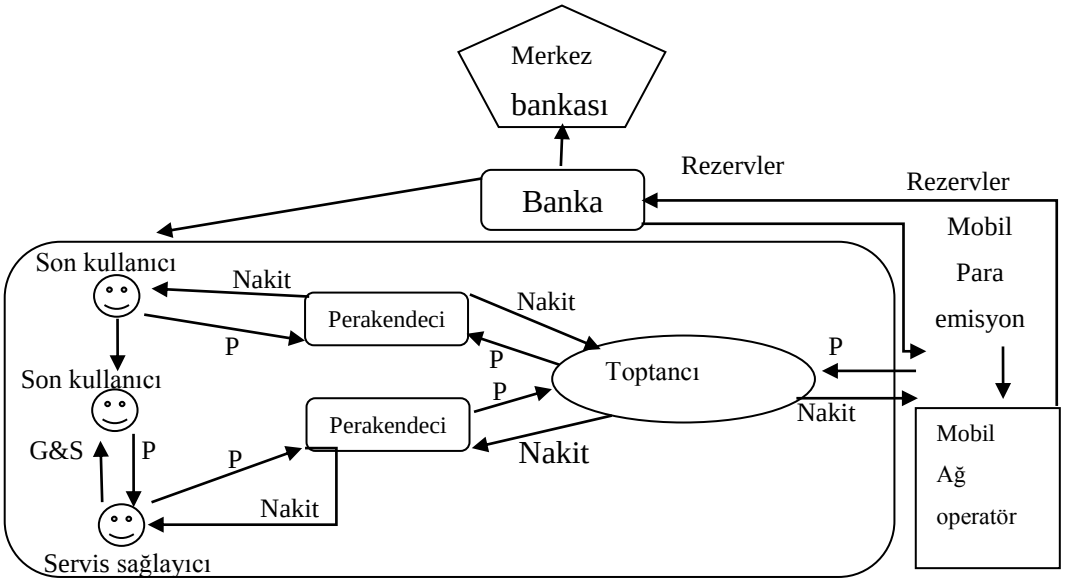
Mobil ödeme hizmeti, iki tür aktör tarafından dağıtılan mobil operatörlerin ağlarından geçer: Mobil Ağ Operatörleri ve (MVNO)Mobil Sanal Ağ Operatörüdür. Böylece, bu aktörler mobil ödeme işlemleri sürecinde neredeyse hiç şeffaf görünmemektedir. Mobil Ağ Operatörün değer zinciri dört elemana bölünmüştür[6]:

- Ağ faaliyeti: operatör, belirli teknik veya uzmanlık görevlerini devrederek, iletişim aktarımı için gerekli altyapıyı da dâhil ederek yönetir;
- Teklif ve yan hizmetler ile ilgili faaliyet: bu faaliyet hizmetini sunan şirketin tüm pazarlama ve iletişim sistemini kapsar;
- Abone yönetimi: Faturalama gibi müşteri odaklı aktivitelerle ilgilidir;
- Dağıtım: Bu son kullanıcı ile tek fiziksel temastır.
- Dağıtımla ilgili servisler arasında mobil çevrimiçi açılış ve kurulum ya da mobil cihazların tedarik edilmesi yer almaktadır.

Afrika'da birkaç (Orange, M-PESA, Tigo, Airtel, MTN, Vodafone) mobil operatör vardır. Çok sayıda aktör, mobil operatörlerin ağlarını kullanarak teklif önerme olanağına sahiptir: sanal operatörler Mobil Sanal Ağ Operatörü ile ilgilidir. Bu nedenle MVNO bir operatör ile bir sözleşme yapar ve ev sahibine daha sonra yeniden satabileceği belirli bir iletişim süresi kurar. Mobil Sanal Ağ Operatör, hizmeti sunmak ve dağıtmaktan sorumludur ve abonelerini tamamen yönetir. Bu nedenle, kendisine toplam tarife teklifi ve hizmetleri özgürlüğü veren SIM kartı elinde bulunduruyor.

2.2.4. Finansal kurumlar

Az sayıdaki bankacılık yeniliği ya yeni bir teklifin ortaya çıkması ya da yeni teknolojilerin entegrasyon ile karakterize edilir[7]. Mobil ödeme bu iki yenilik biçimini birleştiriyor. Bankalar kendi gelirlerini artırmak için yeni bir cazip yol v Bankalar emrinde gelirlerini artırmak için yeni bir çekici yol vardır. Bankalar, mobil bankacılık hizmetleri sunarak başladı, ancak kısa bir süre sonra kullanımların bu hizmeti aştığını fark ettiler. "Mobiquity" [8] ile ilgili tüketici ihtiyaçları, yenilikçi mobil ödeme yöntemleri sunarak bankaları tekliflerini genişletmeye zorlamaktadır.

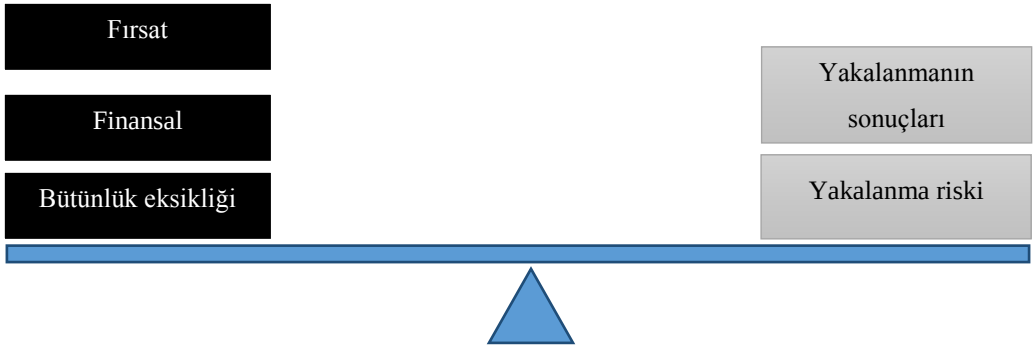


Şekil 2.1. Mobil Para Transferi hizmetlerinin genel gösterim şeması [9].

2.3. Dolandırıcılık ve Sahtecilik Yönetimi

2.3.1. Dolandırıcılık

Oxford Dictionary, sahtekârlığı [10], "Mali veya kişisel kazanımla sonuçlanan yanlış veya kiminle aldatma" olarak tanımlar. Bu nedenle, başkalarına karşı dürüst olmayan mali ya da başka bir avantaj elde etmek için kasıtlı bir hiledir. Kazanılması gereken önemli maddi faydalar ve yakalanma riski sınırlı ise, fırsattan faydalanmaya çalışan ve sahtekârlığa yol açan bazı kişi ve şirketler var. Bu bireyler ve şirketler bağlamında ortaya çıkabilir. Şekil 2.2.'de dolandırıcılık bağlamında önemli olan kilit faktörleri göstermektedir. Doğal olarak, çoğu kişi ve şirket daha yüksek bir bütünlüğe sahiptir ve fırsattan yararlanamaz. Ek olarak, yakalanma olasılığının ve sonuçlarının sahtekârlık olasılığını etkilemesi sayılabilir. Mevcut mobil ve sosyal medya teknolojileriyle, dolandırıcıların daha fazla sayıda potansiyel kurbanlara erişimi ve sonunda tuzağa düşecek olan insanları bulmak için istatistiksel olarak daha iyi bir olasılık vardır [11]. Bu, mobil para biriminde dolandırıcılık riskinin ne olduğunu sormamızı ister.



Şekil 2.2. Potansiyel dolandırıcılığa yol açan temel faktörler [11].

Dünyadaki tüm mobil para hizmetlerinde, müşteri bilgilerini çalma veya elektronik para muhasebesi uzlaşmalarının manipülasyon riski gibi ortak riskler vardır [12]. Bununla birlikte, dolandırıcılık olayının bir operatörden diğerine değiştiğini bilmek, operasyonların yürütüldüğü çevreye göre risklerin tanımlanmasına yaklaşmak daha uygundur. Başka bir deyişle, para sürecindeki hangi noktalarda risk altındaki aktörler

ya da katılımcılar ya da dolandırıcılığı olan? Göz önünde bulundurulması gereken ana aktörler müşteri (işlem riski), para (dağıtım riski) ve şirket çalışanıdır (iç risk).

Tablo 2.1. Mobil parada potansiyel dolandırıcılık

İşlemlere bağlı sahtecilik	Dağıtımla ilgili dolandırıcılık	İç dolandırıcılık
- «Vishing/smishing» : İngilizce terimleri "phising" den (phishing dolandırıcılık) türetilmiştir ve kurban tarafından kişisel kimlik avının kullanımını kod olarak belirtmektedir. Kimliğine ilişkin gizli bilgi veya diğer bilgiler. - Peşin ödeme dolandırıcılık: müşteriler yanlış iddialar altında veya yanlış bir söz karşılığında para göndermeye teşvik edilir. - Hileli bordro: hayali çalışanların veya "hayaletlerin" toplamları toplanması İptal talepleri: müşteri bunlardan faydalandıktan sonra işlemlerin geri ödenmesini talep eder. - Yanlış işlemler: müşterinin yapıldığına inanması için işlem onay SMS'i gönderiliyor. Genellikle iptal talebi ile birlikte.	- Bölme işlemleri: acenteler komisyonlarını artırmak için mobil para yatırma işlemlerini böldüler (sadece miktara bağlı olarak kademeli fiyatlandırma için geçerlidir) - Yanlış işlemler: acenteler müşterilere ait parayı kendi hesabına transfer eder. - Yanlış hesaplar: Tek bir müşteri için birden fazla hesap açmak veya kayıt ücretlerini almak için hayali müşterileri adına hesap açmak.	- İç dolandırıcılık: haksız kişisel mali kazanç için çalışanlar arasındaki gizli anlaşma. - Kimlik hırsızlığı: müşterilerin kişisel bilgilerine erişim ve bunları şirket izni olmadan çalışanların kullanımına sunma.

2.3.2. Ödeme sisteminde sahtecilik riski

Avrupa Merkez Bankası'na göre, Ödemeyi etkileyebilecek çeşitli risk türleri [13]:

- Kredi riski, karşı tarafın, tam olarak bir yükümlülüğü yerine getirmediği (yani, bu yükümlülüğün ne zaman sona ermesi veya ne zamandan sonra gerçekleşmeyeceği) riskidir;
- Likidite riski, bir yükümlülüğün vadesi geldiğinde, bir tarafın elinde bulundurduğu gerekli fon veya varlığa sahip olmaması durumunda gerçekleşir. Bu durum, örneğin, ters piyasa koşullarına bağlı olarak operasyon problemler veya varlıkların nakit olarak dönüştürülebilmesi için geçici olarak yetersizlikten kaynaklanabilir;
- Tarihsel olarak, operasyon risk, bilgisayar çökmesi veya hatalı yazılım gibi teknik arıza riski olarak kabul edilmiştir. Bu yorumun çok dar olduğu ve tanımın genişletildiği kısa sürede fark edilmiştir.
- Yasal risk, bir yasanın ya da yönetmeliğin beklenmedik bir şekilde uygulanmasından ya da bir sözleşmenin uygulanamamasından dolayı meydana gelebilecek kayıp riskidir. Bu genellikle, sistemin sözleşme temelini veya taraflar arasındaki sözleşmelerin temel aldığı mevzuatın öngörülemeyen bir yorumunda kendini gösterir. Mahkeme kararı ile bağlantılı olarak;
- Sistemik risk, bir katılımcının bir sistemdeki yükümlülüklerini yerine getirememesinin, diğer katılımcıların yükümlülüklerini yerine getirmediklerinde yükümlülüklerini yerine getirememelerine neden olma riskidir. Bu, potansiyel olarak, diğer sistemlere veya pazarlara yayılan önemli likidite veya kredi sorunlarına yol açabilir ve böylece finansal sistemin istikrarını tehdit edebilir. Yukarıda belirtilen risk türlerine göre, dolandırıcılık operasyonlu risk kategorisinde sınıflandırılabilir.

Basel Bankacılık Denetim Komitesi, operasyonlu riski “yetersiz veya başarısız iç süreçler, insanlar ve sistemler veya harici olaylardan kaynaklanan kayıp riskleri” olarak tanımlar. Operasyonlu risk sadece teknik hataları değil aynı zamanda kullanılmayan hataları, dolandırıcılıkları veya dış aktörlerin bulunmamasıdır. Bu tanım, operasyonlu riskin finansal kaynakları tehlikeye atabilecek kapsamda tüm

güvenlik açıklarına denk geldiği anlamına gelmektedir. Bu, insan hataları, sistem hataları, personel yönetimi sorunları; kazalar, ticari uyuşmazlıklar, dolandırıcılık ve kötülük gibi çok geniş alanları kapsar.

2.3.3. Dolandırıcılık türü

Dolandırıcılık terimi, hâlâ birçok yoruma tabi olan açık bir kavramdır. Finans alanında dolandırıcılık farklı biçimler alır. Örneğin, yatırımcıların kâr elde etmek amacıyla hile, sahteciliğin yanı sıra paranın sahteciliğini, bir kredinin elde edilmesi için belirli verinin ihmal edilmesini de beraberinde getirir. Telekomünikasyon alanında dolandırıcılık, hizmetin göz önünde bulundurulmadan kullanılması olarak tanımlanabilir. BT durumunda, dolandırıcılık bilgisayarlarda veya ağda gerçekleşir [14]. Dolandırıcılar, bilgisayar sistemlerinin kesilmesi, veri hırsızlığı veya telif hakkı ihlali oluşturmak için bilgisayar araçlarının kullanılmasına karşılık kabul edileceğini tanımlamak gerekir. Bunun için yukarıdaki alanların dolandırıcılığının farklı yönleri devam edecek ve bir araya getirilecektir. Risk kavramı da sahtekârlığı karakterize etmek için incelenecektir.

Laurent ve ark [15] göre risk, belirli bir hedefi, hedef alan ve potansiyel bir etki yaratan tehdit biçimidir. Farklı türden tehditler vardır:

- Operasyonlu / Teknik
- İnsan
- Doğal
- Ekonomik

Operasyon tipi tehdit, bir sistemdeki teknik veya organizasyonlu bir problemden kaynaklanabilir.

Doğal tehdit, doğal afetlerden, örneğin deprem veya yağmurdan kaynaklanır. Ekonomik tip tehdidi, fiyat artışı, vergi artışı gibi ekonomik olaylara karşılık gelir. Son olarak, insan kaynaklı tehdit insanlar tarafından gerçekleştirilen eylemlere

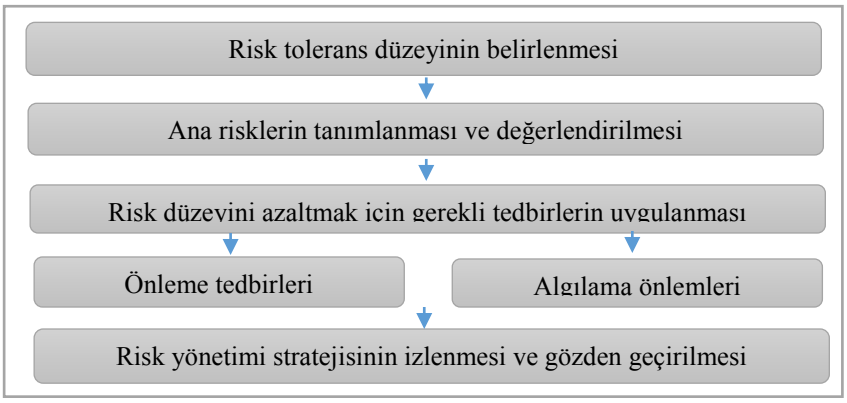
karşılık gelir. Bu tehdidin tanımı, zarar verme iradesini ve eylemin amacını dikkate almak üzere geliştirilmektedir.

Bu çalışmanın bir parçası olarak, mobil ödeme sisteminin finansal kaynaklarını hedef alan ve kâr amacı güden bir gönüllü insan tehdidi ile ilişkili riskleri inceliyoruz. Louisot'un tanımına [15] ve daha önce tartışılan hile tanımlarına dayanarak, sahtecilik, bir kişi veya şirket dışından veya içten bir kişi tarafından gönüllü bir eylem olarak tanımlanabilir. Sistem ve kazanmak için bir sistem güvenlik açığı kullanır. Bu tanım, bizim çalışmamızda inceleyeceğimiz mobil işlem hizmetlerine özgü riskleri belirlemek için bir temel oluşturacaktır.

2.3.4. Dolandırıcılık yönetimi

Dolandırıcılık yönetimi, risk yönetimi yaklaşımının bir parçası olan önemli bir hususdur. Her tür riski yönetmek için çeşitli yöntemler ve araçlar kullanılabilir [12]. Bu yöntemler için ortak temel, sürekli iyileştirme sisteminin kurulmasıdır. Bu, risklerin tanımlanması, değerlendirilmesi ve tedavisinin döngüsel bir sürecine konu olabilir. Bu yaklaşımın önemi öncelikle riskleri tanımlamak ve nihayetinde bu risklerin normale dönmesi için güvenlik politikaları yürütmektir.

Dolandırıcılık yönetimi çerçevesi aşağıdaki ana bileşenleri içerebilir: önleme, tespit, araştırma, uygulama ve kurtarma, analiz ve öneriler. Bu etkili yaklaşım, sahtecilik riskini sınırlamak için her boyutta şirkette uygulanabilir. Şekil 2.3.'te yukarıda belirtilen bu ölçümleri göstermektedir. Şirketinizin ihtiyaçlarına göre uyarlanabilirler.



Şekil 2.3. Mobil Para için Risk Azaltma Önlemlerinin Örnekleri.

Bizim çalışmamız için bu önlemlerden ikisi, takip eden bölümlerde uyarlanacaktır. Bunun için önleme tedbirleri ve ardından tespit tedbirleri ile başlayacağız. Ancak bundan önce mobil transferde güvenlik incelemesine geçeceğiz.

BÖLÜM 3. MOBİL TRANSFER SİSTEMLERİNİN GÜVENLİĞİ

Bu bölümün amacı, mobil işlem hizmetlerini güvenceye almak için mevcut yaklaşımlara ve çözümlere genel bir bakış sağlamaktır. İlk olarak, farklı dolandırıcılık riski kategorileri belirlenmiştir. Ardından, mobil ödeme için bir güvenlik mimarisi sanatı sınıflandırma algoritmaları ile ilgili bir teknoloji yanı sıra gerçekleştirilir.

3.1. Mobil Para Hizmetlerinde Sahtecilik Riskleri

Ödeme güvenliği mimarisine başlamadan önce, dolandırıcılık risklerini oluşturan farklı formları ayrıntılı olarak ele alacağız. Mobil işlem sistemlerinde olduğu gibi ödeme alanında da birçok dolandırıcılık veya aldatmaca tekniği görülebilir. Bu sahtecilikler, bir paranın ya da bir ödemenin yapıldığı bir tüccarın transfer edilmesini sahiplerine kanıtlamak için yalanlara dayanmaktadır. Suiistimalciler ayrıca bilgi sistemine girerek yasadışı işlem yapma olanağına sahiptir. Sistemin bu uzlaşması da sunucu tarafı saldırısı olarak adlandırıldı [16]. Taşıyıcı hesaplar üzerinde işlem yapabilirler, böylece bir davranışsal dolandırıcılık biçimi gerçekleştirebilirler. Her zaman sahtekârlar, elektronik para oluşturma veya silme veya yapılan her işlem için komisyon denilen küçük bir yüzdeyi alma yeteneğine sahiptirler. Çoğu durumda, kötü niyetli operasyonlar yapma haklarını kullandığı veya aştığı bu gerçeğin bu saldırısını gerçekleştiren hizmetin iç aktörleridir. Buna içsel dolandırıcılık deniyor [16]. Kimlik hırsızlığı formları alıntılanabilir:

- Yanlış bir kimlik altında hizmete abone olun
- Teknik veya organizasyon güvenlik açıklarını kullan Kimlik hırsızlığı biçimleri, yasadışı faaliyetleri gizlemek veya sahibinin bilgisi olmadan bir hesap kullanmak amacıyla kullanılır. Bu, kötü amaçlı bir programın yardımı ile yapılabilir.

- Bu durumda, meşru bir taşıyıcıyla aynı davranışı olan bir dolandırıcıdan söz ediyoruz [17]. Bu dolandırıcılık, üst üste gelen sahtekârlık [18] adı altında telekomünikasyon alanında var olmakla birlikte, aynı zamanda İngilizce 'de davranışsal dolandırıcılık adı altında bankacılık alanında da var [19] [20]. Bu konuda davranışsal dolandırıcılık terimi aşağıdaki adımlar için korunacaktır.

3.1.1. Mobil ödeme güvenliği mimarileri

Bu bölümde, mevcut mobil ödemede güvenliği sağlamak için hayata geçirilen farklı olasılıkları inceliyoruz. Bunun için, mobil cihazların ve bütünleşmiş ettikleri mimarinin güvenliği gösterilecektir.

Mobil ödemede, daha yaygın olarak mobil ödeme oyuncuları olarak adlandırılan aktörlerin müdahalesine dikkat çekebiliriz. Bunlar;

- Ödemeyi yapmak için mobil terminalini kullanan bir ödeme hizmetine abone olan ödeme yapan;
- Ödenen parayı toplayan alacaklı;
- Ödeme platformu bir ödeme talimatı alır. Rolü, genellikle mobil ödeme sisteminde tanımlanan dört köşeli veya üç köşeli bir model durumunda farklıdır.

3.1.2. Mobil cihaz güvenliği

İşlemler cep telefonu üzerinden yapıldığından cep telefonu güvenli olmalıdır. Böylece mobil ödeme için güvenlik hizmetleri sağlamak için üç mobil bileşen kullanılabilir. Bu üç bileşen şunlardır:

Mobil işletim sistemleri, Güvenli Yürütme Ortamı (TEE) ve Güvenli Öğe (SE). Bir İşletim Sistemi (OS), bir veya daha fazla aygıtın donanım kaynaklarının kullanılmasına izin veren bir dizi özel programdır. Uygulama yazılımının başlatılmasını ve yürütülmesini sağlar. İki ana işlevi yerine getirir: ilk olarak, farklı

yazılımlar arasında kullanımlarını dağıtarak, donanım kaynaklarının (bellek, işlemci ve çevre birimleri) yönetimi; Öte yandan, fiziksel makineye göre daha yüksek seviyeli bir ara yüz sunan uygulamalara hizmet sağlanması. Bu ara yüz yazma uygulamaları için bir takım temel işlevler (sistem çağrıları) sağlayan "sanal makine" gösterim sunar. En popüler mobil işletim sistemleri, Android, IOS, Symbian, Windows Mobile bunlar, kullanıcı tarafından zorunluluk haline getirilmesi gereken bir dizi güvenlik ayarı sağlar. Kullanıcı, 0000 veya 1234 gibi basit bir PIN kodu belirlememesi, 5 dakika sonra otomatik bekleme ve girişimlerin kilidini kaldırması gerektiğini söyleyen cihaza erişimi yönetmelidir. Kaybolan cihaz başka kişi tarafından bulunursa, arama yapabilir veya uygulamaları kullanabilir. Ayrıca, cihazın iş uygulamalarına sahip olduğu veya şirketin bilgilerine erişebildiği (dosya paylaşım çözümleri) durumdaki bir kimlik doğrulama sistemi olan işlevlere erişimi de uygulamalıdır. Ve son olarak stratejik bilgileri bir mobil terminalde depolamak tavsiye edilmez. Bu zorunluysa, terminal tarafından sunulan şifreleme özellikleri veya indirilen bir uygulama sayesinde veriler şifrelenmelidir. Ancak işletim sistemleri tarafından sağlanan güvenlik, mobil ödeme uygulamaları gibi hassas uygulamaların güvenliğini garanti etmek için yeterli değildir. Bu sorunlar, güvenli yürütme ortamı ve yukarıda listelenen güvenlik öğesi kullanılarak önlenebilir. Bu zorunluysa, terminal tarafından sunulan şifreleme özellikleri veya indirilen bir uygulama sayesinde veriler şifrelenmelidir. Ancak işletim sistemleri tarafından sağlanan güvenlik, mobil ödeme uygulamaları gibi hassas uygulamaların güvenliğini garanti etmek için yeterli değildir. Bu sorunlar, güvenli yürütme ortamı ve yukarıda listelenen güvenlik öğesi kullanılarak önlenebilir.

Güvenilir bir yürütme ortamı, ana işlemcinin güvenli bir alanıdır. Mobil terminallerde bulunan bir donanım ve yazılım elemanıdır. Bu ortamda çalışan uygulamaların bütünlüğünü, gerçekliğini ve gizliliğini korur [21]. Böylelikle, bu ortam cihazları güvenli bir şekilde yönetir ve güvenli elemanlar olarak kapasitede sınırlı değildir. Ancak, güvenli unsurdan farklı olarak, TEE düşündüğümüz kadar güvenli değildir [21].

Güvenli elemanın sağlayıcısı güvenli elemanın kontrolüne sahiptir. Güvenli unsurun (hangi aktörlerin hangi şartlar altında erişebileceği) depolama alanını düzenleyen kuralları tanımlayabilir.

Mobil ödeme böylece iki ortamın merkezinde yer alıyor: bankacılık ve finansal ortam, güvenlik ve veri koruma sorunları ve mobil telefon endüstrisine aşina, hareketlilik fikri üzerine harekete geçti. Bu iki mesleğin, telekomünikasyon ve bankacılık aracının - farklı yönleriyle - birleşmesi, karmaşık düzenlemeleri içeren işlemlere yol açar. Dolayısıyla, bir finansal ortamda güvenlik son derece önemli bir yere sahiptir, işlemlerin aşağıdaki özelliklere sahip olması gerekir [22]:

- Gizlilik: Verilerin ve işlemlerin yetkisiz bir kişi tarafından görüntülenememesini sağlar.
- Doğrulama: İşlemin işlemin iş ortağından yapılmasını sağlar.
- Bütünlük: bilgilerin işlem boyunca sağlam kalmasını ve değiştirilememesini sağlar.
- Yetkilendirme: İlgili tarafların, işlemde yer alan herhangi birinin işlem yapmaya yetkili olup olmadığını doğrulamasını sağlar.
- İnkâr etmeme: kimsenin bir işlemin bilgisi olmadan yapıldığını iddia edemez.

İşlem-kritik bilgilerin, uygulamaların farklı yaşam döngüleri ile bağımsız olarak indirildiği, özelleştirildiği, yönetildiği veya silindiği güvenli öğe adı verilen dinamik bir ortamda dikkatli bir şekilde saklanması gerektiğinin nedeni budur. SE; borçlar, krediler, biletleme, erişim kontrolü gibi tüm finansal işlemler için faydalıdır. Tüketici için önemli olmakla birlikte, şeffaf ve erişilemez durumdadır. Servis sağlayıcı tarafında, güvenli elemanın konumunun önemli ve stratejik bir parametre olduğu açıktır. Gerçekten de, ES'nin depolanacağı yer, bu öğenin sahipliğini ve yönetimini ve büyük ölçüde, hizmet sunumunun kontrolünü belirler. Bu nedenle güvenli elemanın yeri önemlidir. Bu konum, her aktörün karar verme rolünü ve işlem yönetim yeteneğini belirleyecektir. Gerilim, bankalar, mobil operatörler veya mobil üreticiler arasında sayıca çoktur. Bu zorunluluk, teklifin getirdiği gelirlerden ve uygulanmasıyla ilgili stratejik kararlardan faydalanmak için bu unsurun kontrolünü

ele geçirmektir. Bu savaşın en meşhur bölümlerinden biri, üretici Hareket Halinde Araştırma (RIM) (Ocak 2013'Te BlackBerry oldu) ve 2010'larda SE'nin kontrolü için mobil operatörler arasındaki savaşıdır. Operatörler her zaman SIM kartta saklamayı tercih ettiler. Gerçekten de, bu cihaz mobil operatörlerin üyesi olmakta, bu siteye yerleştirilen güvenli bir unsur onların kontrolü altında olacaktır. Mobil operatörler için bu konumla ikinci bir avantaj ilişkilendirilmiştir: SIM kartlar, herhangi bir telefonda kullanıldığında, terminal üreticilerini rekabet eden rakiplerden hariç tutabilir. Mobil cihaz değişebilir, ancak SIM kartta saklandıkları için güvenlik ve işlem bilgileri herhangi bir mobil cihazda erişilebilir kalır. Öte yandan, mobil üretici güvenli unsuru, bulunduğu yerde, yani akılı telefon 'da saklamak istemektedir. Mobil terminalde depolama, operatörlerin etkisini ve kontrolünü kısıtlar ve böylece tüketiciyi mobil cihazına daha fazla bağlar.

Sonuç olarak, güvenli unsurun yeri stratejik bir konudur: bu konumun ardından, mobil ödeme oyuncuları karar verme sürecinde yerlerini alır ve bunların mülkiyet haklarına erişimleri tanımlanır.

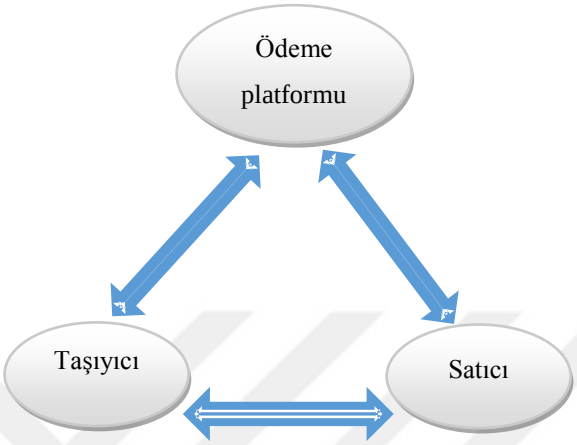
3.1.3. Terminallerin ödeme platformları ile etkileşimi

Yani bir ödeme gerçekleşmesi için bu aktörler arasında bir etkileşime ihtiyaç vardır. Bu etkileşim, farklı mobil ödeme hizmetlerinde mimarileri önermemize neden oluyor. Bu mimariler göre üçtür:

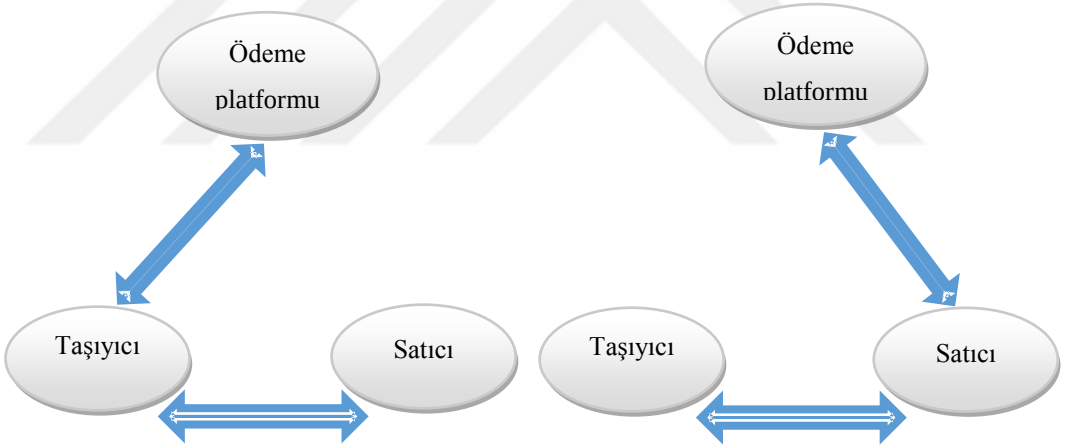
- Tüm bağlı bir söz;
- Yarı bağlı olarak adlandırılan;
- Ve sonunda sözde bağlantı kesildi

Tüm bağlı mimaride, yukarıda bahsedilen üç aktör, ödeme işlemi sırasında birbirine bağlanır ve etkileşim gösterir, bkz. Şekil 3.1.'de Yarı bağlantılı mimari için ödenen ve ödeme yapan kişi etkileşime girer ve bunlardan sadece bir tanesi ödeme platformuna bağlanır. [23] 'a göre, Şekil 3.2.'de temsil edilen iki bağlantılı yarı-mimarisi kategorisini sayabiliriz: Bir ya da hamil, ödeme platformuna bağlı olan

varlığa kullanıcı merkezli denir. Bir veya tüccar, mobil ödeme platformuna bağlı olan köşk merkezlidir. Ve son olarak, Şekil 3.3.'te gösterilen sözde bağlantısız mimari, ödeme yapanın ve ödeme yapan kişinin etkileşime girdiği, ancak bunların hiçbiri ödeme platformuna bağlı değildir.

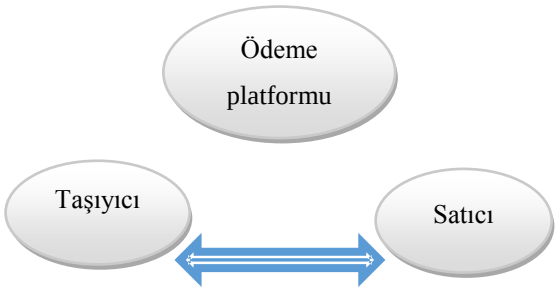


Şekil 3.1. Tüm bağlantılı mobil ödeme mimarisi [23].



(a) Taşıyıcı aracılığıyla bağlantı - kullanıcı merkezli (a) Satıcı üzerinden bağlantı - şube merkezli

Şekil 3.2. Yarı bağlantılı mobil ödeme mimarisi [23].



Şekil 3.3. Tümüyle ayrılan mobil ödeme mimarisi [23].

Orange Money veya M-Pesa gibi birçok mobil para transfer hizmeti, birbirine bağlı mimariye dayanmaktadır. Genellikle transfer prosedürü şu şekildedir: Satıcı, işlemi işlemin miktarını (sunucu) ve alıcının telefon numarasını başkalarına göndererek işlemi başlatır. Ardından ödemeyi onaylamak için alıcıya ödeme platformu tarafından başvurulur. Bireyler arasındaki transfer durumunun, bu bağlantılı mimarinin özel bir kullanımı durumunda olduğunu düşünüyoruz. Sahipler ve satıcılar, Kısa mesaj servisi (SMS) veya Yapılandırılmamış Ek Hizmet Verileri (USSD) kullanarak ödeme platformuna karşılık gelir. Bu sistemlerin güvenliği ağın işlevlerine dayanmaktadır, ancak bu sınırlamaları ve zayıf yönleri temsil eder.

Birkaç yaklaşımın sürdüğü iki mimariye bakıldığında, bunlar bizim çalışmamız için uyarlanmayacaktır. Bildiğimiz kadarıyla, hiçbir mobil işlem sistemi, bugün tamamen ayrılmış bir mimariye dayanmamaktadır.

3.2. Sınıflandırma Algoritmaları

Sınıflandırma algoritmaları çok sayıda olduğundan, bu bölümde veri madenciliğinin ne olduğunu göstereceğiz, daha sonra sınıflandırmadan bahsedeceğiz ve farklı sınıflandırma algoritmaları kategorilerine ayrıntılı olarak yer vereceğiz.

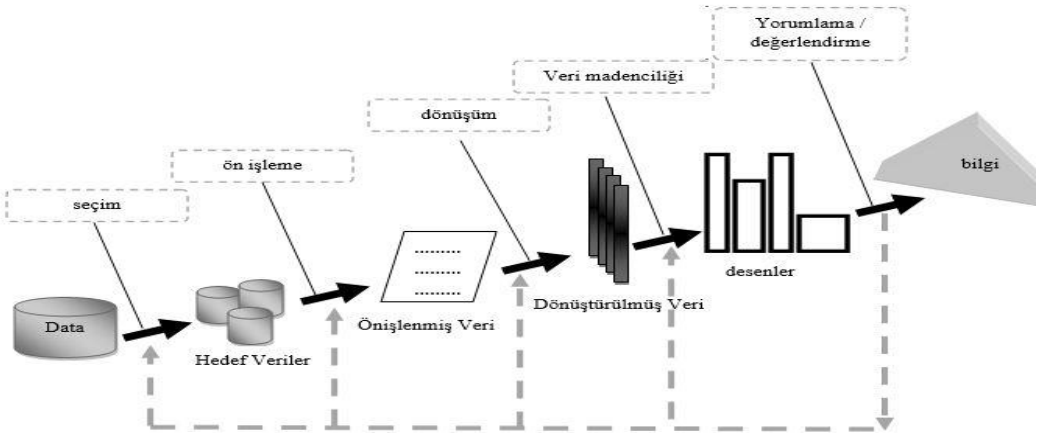
3.2.1. Veri madenciliği nedir?

Veri madenciliği, veritabanlarında veya veri ambarlarında depolanan büyük hacimli verilerden (faydalı ve bilinmeyen) bilgi aramaktan ve çıkartmaktan oluşur [24]. Veri madenciliğinin son gelişmesi (1990'ların başından beri) çeşitli faktörlerle bağlantılıdır. Masaüstlerinde veya hatta evde önemli hesaplama gücü mevcuttur. Veritabanlarının hacmi büyük ölçüde artıyor dünya çapında ağlara erişim, sürekli artan iş hacmine sahip ağlar, dağıtılabilir bilgi işlem ve canlı bir küresel ağ üzerinde bilgi dağıtımı yapan ağlar; Üretim, satış, yönetim, lojistik süreçlerinin en uygun şekle sokma için ticari menfaatin bilincinde olmak. Veri madenciliği, günümüzde büyük bir ekonomik öneme sahiptir çünkü yönetimin optimize edilmesini mümkün kılmaktadır. Kaynaklar (insan ve materyal). Örnek olarak kullanılır:

- Rezervasyonda uçak, otel gibi koltuk sayısının en uygun Sekle sokma;
- Süpermarketlerdeki rafların organizasyonu;
- Reklam kampanyası organizasyonu, promosyonlar;
- Tıbbi tanı;
- Genom analizi ve bioinformatik daha genel olarak;
- Nesnelerin sınıflandırılması (astronomi, ...);
- Veri zamanındaki evrim
- Sahtecilik tespiti...

Veri madenciliği sürecinin tamamı birkaç adımdan oluşur ve aşağıda adamları gösterilmektedir:

- Bilgi toplamak ve bu bilgiyi bir veritabanında düzenlemek;
- Veritabanını temizlemek: değer olmayan, geçersiz bir değere sahip (gürültü), standardizasyon;
- Yararlı özelliklerin seçimi;
- Veritabanlarında Bilgi Bulma (KDD), Şekil 3.4.'te gösterilmiştir;
- Verilerin görselleştirilmesi: diyagram, pasta grafiği, ağaç, 3D görselleştirme ve daha genel olarak, verilerin etkileşimli araştırılması; Bilgi çıkarımının sonuçlarının değerlendirilmesi.



Şekil 3.4. KDD Sürecini Oluşturan Adımlar.

3.3. Sınıflandırma

Belirli bir veriyi önceden tanımlanmış sınıflara göre etiketleyen bir fonksiyon yaratmanın sınıflandırılması gibi veri madenciliği ile ilgili çeşitli problemler vardır. Regresyon, verilen verilerden gerçek bir değişkeni tahmin edebilecek bir fonksiyon yaratmanıza izin verir. Kümelenme, bunları oluşturan birkaç kategoriyi veya verilerin kompakt gösterimlerini oluşturmayı amaçlayan özeti tanımlayarak verileri yazmaya izin verir. Ancak, [25], bu görevler ortak yöntemlere dayanır ve birbirleriyle de kullanılabilir. Örneğin, verilerin boyutunu azaltmak için özet yöntemleri kullanmak ve sonra bir sınıflandırma aşamasında hangi sınıfların kullanılacağını belirlemek için bir küme yöntemi uygulamak mümkündür. Çalışmamızda sahtekârlık tespitine dayalı olduğu için, bir işlemi veya bir dizi işlemin hileli veya meşru olup olmadığını göstermek için sınıflandırmayı bir çözüm olarak seçmemize zorlamaktadır.

3.4. Otomatik Öğrenme Yöntemi

Makine öğrenimi, bir makinenin bir öğrenme süreci boyunca evrimleşmesini sağlayan ve dolayısıyla gerçekleştirilmesi zor veya imkânsız olan görevleri yerine getirmeye yarayan yöntemlerin geliştirilmesi, analizi ve uygulanması anlamına gelir. Daha geleneksel algoritma yollarla doldurun. Amaç: Bir veri kümesinde bulunan bilgileri ayıklamak ve otomatik olarak kullanmaktadır.

3.4.1. Öğrenme türleri

Öğrenme algoritmaları, kullandıkları öğrenme türüne göre kategorilere ayrılabilir:

- Denetimli öğrenme
- Denetimsiz öğrenim
- Yarı gözetimli öğrenme.

Denetimli öğrenme, otomatik olarak "örnekler" (genellikle işlenmiş ve onaylanmış vakalar) içeren bir öğrenme veritabanından kurallar üretmeye çalışan bir otomatik öğrenme tekniğidir.

Denetlenen öğrenme metodu, f harfinin g ifadesini belirlemek ve yeni bir girişte x çıkışını bir g (x) ile ilişkilendiren bir tahmin fonksiyonu olarak adlandırmak için bu öğrenme tabanını kullanır. Bu nedenle denetimli öğrenme algoritmasının amacı, uzmanlar tarafından hâlihazırda işlenmiş olan veriler sayesinde "öğrenilebilecek" olan bilinmeyen girdiler için genelleştirmektir, bu da "makul" bir şekilde. Denetimli otomatik öğrenme yöntemiyle iki tür çözülebilir problem vardır:

- Y ∪ R: Bir kişinin tahmin etmeye çalıştığı çıktı, sürekli bir dizi istilada bir değer olduğunda, bir regresyon probleminden söz edilir.
- $Y = \{1 \ldots, 1\}$: çıktı değerleri kümesi sonlu olduğunda, her girişe bir etiket atamaktan kaynaklanan bir sınıflandırma probleminden bahsediyoruz.

Dolandırıcılık tespiti durumunda, denetimli öğrenme, etiketlenmiş işlemlerin (Xi), yani hangi bilginin Yi'nin mevcut olup olmadığını gösteren mevcut olduğunu gözlemlemekten ibarettir, dolandırıcılık ya da değil.

Denetlenmeyen öğrenme, gözlemlenen değişkenler ve tahmin edilecek değişkenler arasında ayrım yapmaksızın verilerin dağılımını ve değişkenler arasındaki ilişkileri karakterize etmeyi amaçlamaktadır. Denetimsiz öğrenmenin ana biçimleri şunlardır:

- Yoğunluk fonksiyonu veya olasılık fonksiyonu tahmin ettir. Bu, denetimsiz öğrenmenin en genel şeklidir. Net bir ölçütümüz var, log-olabilirlik (ama bazı sorularım var). Açıkça p (x) fonksiyonunu öğrenmekteyiz.
- Doğal sınıflara veya kümeleme keşfi dağılımının ana modaları keşfetmek istiyor ki, (örneğin K-Means algoritması), vs. " ilk örnek ", ana kategoriler, ... Bu azalmanın bir form verir Her örneğe bir tamsayı ilişkilendiren boyutsaldık.

- Küçük boyuttaki çeşitlerin, yani, verilerin büyük çoğunluğunu bulduğu yüzeylerin (düz veya doğrusal olmayan) yüksek boyutta öğrenilmesi. Bu, verilerin görselleştirilmesi ve / veya denetlenen öğrenmeden önce ön-muamele olarak önemli bir adım olabilen verilerin küçük ölçekli bir temsilini sağlar. Sahte bir işlemin normal işlemlerin bir parçası olduğunu düşünürsek, bu yaklaşım bizi ilgilendirebilir.

Yarı-denetimli öğrenme durumunda, sistem X1, ... Xn ve Y1, alt kümelerini girer. Bu, belirli işlemlerin belirli bir sahtekârlık olarak etiketlendiği bir işlem veritabanımız varsa, diğer işlemlerin, hileli nitelikleri ya da sahtekârlıklarına ilişkin belirsizlik nedeniyle etiketlenmemesi durumunda mümkün olan bir durumdur.

Her zaman, bu yöntemleri birleştirmeyi içeren bir karma öğrenme yöntemi olabilir. Genel olarak, iki veya daha fazla denetlenen yöntem birlikte veya denetimsiz bir yöntem ve denetlenen bir yöntem kullanılır.

3.5. Algoritmalar

Araştırmamızla ilgili olarak, denetlenen öğrenme algoritmalarına dayalı sınıflandırmayı dikkate alacağız. Şimdi bu kategorinin farklı algoritmaları sunulmuştur.

3.5.1. İstatistiksel yöntem

3.5.1.1. Doğrusal regresyon

Doğrusal regresyon bir istatistiksel sınıflandırma yöntemidir. Sınıfın değerini, y = α1x1 + ... + αm x m formundaki lineer bir denklem formundaki örneklere göre ifade etmekten oluşur [26]. Burada y, bir sınıfa ait olanı temsil eden bir ikili değişkendir, αi temsil eder. Katsayılar ve xi, bir referans noktasını açıklamayı mümkün kılan farklı değişkenlere karşılık gelir. Daha sonra, αi parametreleri, veri sınıfını en iyi şekilde tahmin etmek için optimize edilmiştir.

3.5.1.2. Lojistik regresyon

Lojistik regresyon, sınıfı temsil eden sayısal bir değer yerine bir sınıfa ait olma olasılıklarını düşündüğümüz bir doğrusal regresyon şeklidir. Lojistik regresyon gerçekleştirmek için farklı yöntemler vardır. Örneğin, lojistik regresyon ağaçları [24], alanı bölmek ve her parçaya lojistik regresyon uygulamak için karar ağaçlarını kullanırlar. Bu sayede, sadece bir tanesinin yerine birçok lojistik regresyon denklemi kullanılmıştır. Multinomial Lojistik Regresyon Yöntemleri [26], çeşitli sınıflar için lojistik regresyon sağlar. Ek olarak, bu yöntem, bir lojistik kısıtlama katsayıları üzerinde bir sınır parametresi olan bir sınırlama getirmektedir. Bu, lojistik regresyonun hata paylarına belirli bir tolerans sağlar. Böylelikle, fazla ya da düşük öğrenme problemlerinden kaçınmayı mümkün kılar. Doğrusal regresyon için uygulanan, bu minimisera1x1 + ... + amxm - y + ridge

3.5.1.3. Naif bayes

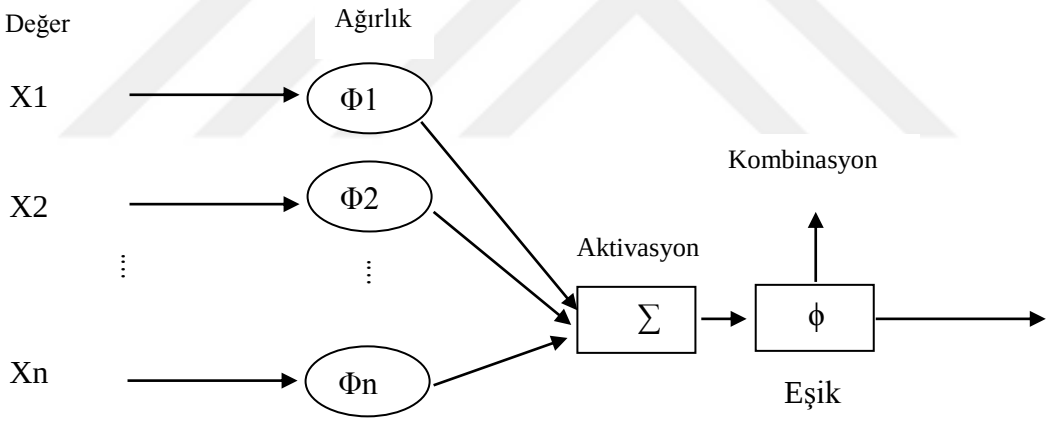
Naif Bayes sınıflaması [26], sınıflara ve koşulların farklı karakteristik değişkenlerine bağlanan koşullu olasılıkları dikkate alarak bir sınıfa ait olma olasılığını tahmin etmeyi amaçlamaktadır. Bayes ilişkisi P (A | B) .P (B) = P (B | A) .P (A) P ile çevrilmiştir (Y | x1, ..., xm) .P (x1, ..) ., xm) = P (x1, ..., xj, ... xm | Y) .P (Y) [24]. Farklı açıklayıcı değişkenler, Bayesien saf sınıflandırmada birbirinden bağımsız olarak kabul edilir. Bayes ilişkisi böylece P (Y) = P (x1, ..., xj, ... xm) olur.

3.5.2. Bayes ağları

Bayes ağları [26], grafik teorisi ve olasılık teorisini birleştirir. Koşullu olasılıkları hesaplamayı mümkün kılan Bayes ilişkisi P (A | B) .P (B) = P (B | A) .P (A) 'ya dayanır. Bayes ağları, verileri açıklayan değişkenler arasındaki bağımlılıkların bir açıklamasını sağlamak için çıkarım kurallarını ve olasılıkları birleştirir. Miktar, işlemin türü ve işlem süresi arasındaki bağımlılıkları biliyorsak, örneğin, belirli bir işlem T için bu değerlerden T'nin hileli olup olmadığını belirlemek mümkün olacaktır.

3.5.3. Sinir ağları

Bir sinir ağı, biyolojik nöronların işleyişini kopyalamayı amaçlayan matematiksel bir modeldir. Bu model, algılayıcı veya denetlenmeyen Kohonen haritaları gibi denetlenen öğrenmeyi sağlar [27]. Sinir ağı, bir sınıf ataması gereken bir vektör v = (x1... xn) girişini alır. Bunun için farklı varlıklar, nöronlar aktive edilir. Şekil 3.5.'te sinir ağlarının tabanında resmi bir nöron göstermektedir. Alanı iki sınıfa ayıran ve w1, w2, ... wn katsayıları ile karakterize edilen bir hiper düzlem denklemi ile ilişkilidir. Öğrenme aşamasının amacı, bu değerleri optimize etmek ve sınıfları en iyi şekilde ayıran bir denklem bulmaktır, bir nöronun yarattığı ayrım doğrusaldır. Lineer olmayan bir durumda iki sınıfı birbirinden ayırabilmek için, daha karmaşık modeller oluşturmak için bir ağdaki nöronları bağlamak mümkündür. Diğer sinir ağı türleri de var ama bunlar burada ayrıntılı olarak açıklanmadı.

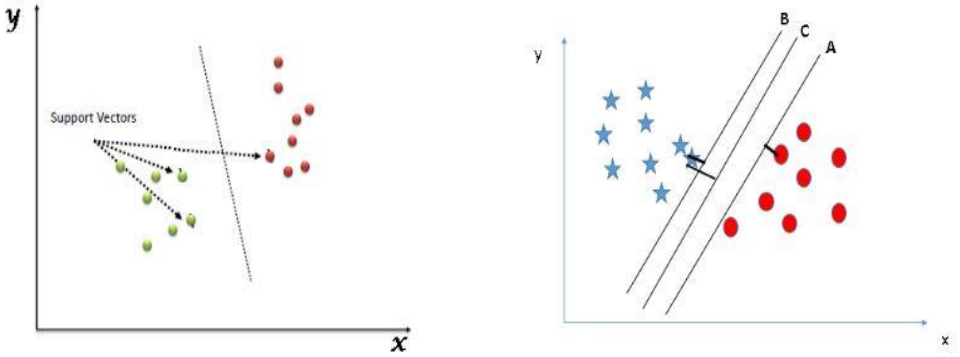


Şekil 3.5. Yapay nöron örneği [27].

3.5.4. Vektör destek makineleri

Geniş kenar ayırıcıları [28] veya SVM, alanı iki bölgeye ayırmak için en iyi karar sınırını bulmayı amaçlar. Bu, SVM'ler sinir ağlarına benzemektedir. Bununla birlikte, kullanımı daha kolaydır, çünkü diğerlerinin yanı sıra, operatör tarafından seçilen bir çekirdek fonksiyonuna da bağlıdırlar. Dahası, nöronların nedenlerine aykırı bir yapı belirtmeleri gerekmemektedir.

SVM'ler iki aşamaya ayrılır. İlk olarak, girdiler bir ürüne sahip olan bir F alanına dönüştürülür. Daha sonra, iki sınıfın verilerini ayırmak için en uygun bir sınır seçmeye çalışırız. Sınırın, tüm örneklerden mümkün olduğunca uzak olması halinde en uygun olduğu söylenir. Bu nedenle, ayırma hiper düzleminin denklemini tanımlamaya ve en yakın noktadan hiper düzeye, yani kenar boşluğuna olan mesafeyi maksimize etmeye çalışacağız (bkz. Şekil 3.6.'da). Pratikte, çekirdek fonksiyonunun kullanılması, bunun başlangıç alanında yapılmasına izin verir.



(a)Optimal bir sınır aramak (b) En üst düzeye çıkarmak için pay.

Şekil 3.6. Optimize edilmiş bir sınır bulma ilkesi [28].

3.5.5. Karar ağaçları

Şekil 3.7.'deki bir karar ağacı, verileri sınıflandıran bir dizi kuralı bir araya getirir. Ağacın her düğümü tanımlayıcı bir değişken üzerinde bir kuralı ve bu kuralı önceki düğümlerin bağlantılarına bağlayan mantıksal AND'yi temsil eder. Ağacın bir yaprağı, kendisine yönelen farklı kuralların birleşmesi sayesinde alınan bir karara karşılık gelir. Her sayfa belirli bir etiket için belirli bir yüzdelik oranla ilişkilendirilmiştir Şekil 2.7.'de karar ağacını göstermektedir.

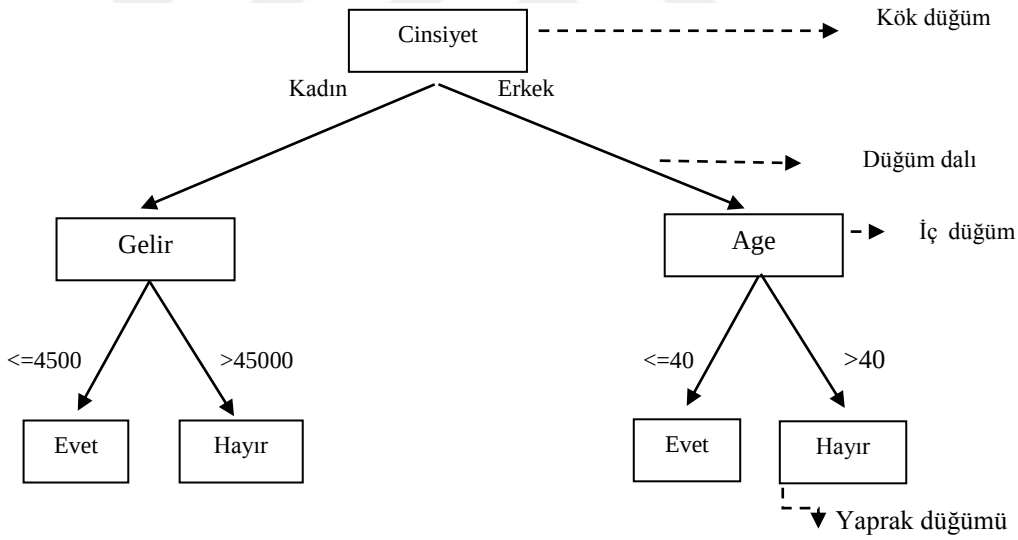
ID3 algoritması [29] böyle bir ağaç oluşturmaya izin verir. Veri setine karşılık gelen kök düğümünden, bu algoritma en iyi tanımlayıcı değişken ve bu değişken için bir değer seçer. Daha sonra, algoritma, seçilen açıklayıcı değişkenin değerine göre verileri böler. Her bir alt-grup için, algoritma iyi açıklayıcı değişken ve bir alt, bir tek öğeleri içerir kadar daha böylece alt grup bölmek ve yeni bir değer seçer sınıf veya

tüm değişkenler dikkate alındıysa. Algoritma C4.5 [29] dikkate sürekli aralıkları ve bir performans muhafaza kolaylaştırmak için ağaç budama iletken alan bir ID3 gelişmedir. Verilen n nitelikleri A1. Bir açıklama alanı X, her bir özelliğin Ai'nin alanlarının Xi Kartezyen ürünüdür özellikler şunlar (denklem 3.1) olabilir:

$$X = \prod_{i=1}^{n} Xi \text{ ou } Xi = Dom(Ai). \quad (3.1)$$

- İkili,
- n - alanlar,
- Gerçek.

Karar ağaçları, kararlarını, özniteliklerle ilişkili bir test paketine dayandıran sınıflandırma kurallarıdır, testler ağaç benzeri bir tarzda düzenlenir. Alan



Şekil 3.7. Karar ağacı örneği

Rastgele ormanlar [30], öğrenme aşamasında kısmen rastgele inşa edilen bir dizi karar ağacından oluşur. Bir girişi sınıflandırmak için, ilk olarak ormanın ağaçları tarafından sınıflandırılır. Ona tahsis edilen sınıf, ormandaki ağaçların çoğunluğu tarafından belirlenen sınıfa karşılık gelir.

3.5.6. Karar tabloları

Karar tabloları iki bölümden oluşmaktadır [31]. İlk gruplar birlikte farklı değişkenler ve olası değerleri. İkincisi, etiketli işlemlerin bir listesini ve ilk bölümdeki değişkenlere dayanan açıklamalarını içerir. Yeni bir örneği sınıflandırmak için mevcut örneklerle karşılaştırılır ve bu karşılaştırmaya göre etiketlenir. Öğrenme algoritması, tanımlayıcı değişkenlerin nasıl seçildiğini tanımlamayı mümkün kılar.

3.5.7. Çoğunluk karar tablosu

Çoğunluk karar tablosu, çoğu durumu birbirinden bağımsız olarak açıklayan açıklayıcı değişkenleri seçen en iyi ilk açgözlü algoritma kullanılarak oluşturulmuştur[31].

3.5.8. PART tipi algoritması

PART tipi karar tablosu, sınıflandırıcı C4.5 ile ilişkilidir [32]. Karar tablosu birkaç kez oluşturulmuştur. Her birinde, C4.5 tipi bir karar ağacı oluşturulur ve çoğu vakayı kapsayan yaprak seçilir. Bu şekilde seçilen sayfalar, karar tablosunun değişkenlerinin listesini ve bunun farklı örneklerini oluşturmayı mümkün kılan bir dizi kurala karşılık gelir.

BÖLÜM 4. MOBİL PARALARDA SAHTECİLİK RİSKİNİN ÖNLEMESİ

Risk yönetimi, herhangi bir işletmenin ticari başarısının önemli bir parçasıdır. Etkin risk yönetimi, iki önemli ticari varlığı - marka imajını ve gelirini koruduğu için sürdürülebilir iş büyümesinin temelidir.

Mobil operatörler, GSM işleriyle ilişkili riskleri yönetmek için kullanılırlar ve mobil para hizmetlerini başlatanlar, mobil paranın dolandırıcılık riski de dâhil olmak üzere belirli riskler taşıdığının farkındadır. Bu bölüm, mobil para transfer sistemindeki dolandırıcılık risklerine karşı önleyici mücadele için bir çerçeve sunmaktadır.

4.1. Risk Tolerans Seviyesinin Belirlenmesi

Dolandırıcılık risklerini etkin bir şekilde yönetmek için, mobil para sağlayıcıları öncelikle bu risk için tolerans seviyelerini anlamalıdırlar ki bu da ödemek istedikleri maliyetleri ifade etmenin bir yoludur. Her risk bir maliyet ve her risk azaltma önlemi de bir tane vardır [12]. Riskten kaçmayan bir mobil para hizmeti, "karşılığında daha yüksek bir büyümeyi kabul ederek riski önlemek" isteyebilir. Tersine, yenilik ve hızlı büyümeye daha fazla odaklanan bir operatör daha yüksek bir risk düzeyini kabul etmeye istekli olabilir. En önemlisi, mobil para yöneticileri ve iş geliştiricileri, iş stratejileri geliştirirken veya yeni hizmet teklifleri çalışırken kabul edilebilir risk düzeylerinden haberdar edilmelidir.

Aynı şekilde, risk toleransının seviyesi mobil para hizmetleri arasında değişebileceği gibi, bu tolerans seviyesini belirlemek için kullanılan yöntemde değişebilir. Bazı operatörler, hoşgörü düzeylerinin niceliksel bir ölçümünü (örneğin, hileli veya talep

edilen işlemlerin azami yüzdesi), diğerleri ise nitelik bir ölçek kullanacaklardır [15]. Örneğin, sağanak, en az, temkinli, açık veya yüksek tolerans seviyelerini tanımlayarak. Birtakım müdahalelerin kabul edilebilir kabul edilen risk seviyesini belirleme sürecini desteklemesi muhtemeldir. Bazı operatörlerin kabul edilebilir risk seviyelerini nasıl tanımlayabilecekleri konusunda tavsiye almak için bankacılık ortaklarına güven duyduklarını gördük. Diğerleri grup seviyesinde mevcut desteği kullanır, bazı operatörler ise şirketin GSM işinden sorumlu sahtecilik önleme ve gelir koruma ekibi aracılığıyla tolerans seviyelerini tanımlar. Sürecin bu aşaması biraz kavramsal olsa da, etkili ve uygun risk azaltma önlemleri için hala önemlidir.

4.2. Risk Azaltma Önlemlerinin Uygulanması

Ana riskler belirlendikten sonra, bir sonraki adım, operatörün, ucuz önlemler veya belirli bir risk yönetimi politikası olabilecek etkili bir risk azaltma önlemleri uygulamaya koymasıdır. Etkili önlemler, kısıtlama olmadan sürdürülebilir iş gelişimini sağlayan önlemlerdir.

4.3. Mobil Para İle İlişkili Riskleri Azaltmak İçin Kontrollerin Kullanımı

Mobil para kontrol önlemleri ya sahtecilik olasılığını azaltmayı amaçlayan önleyici tedbirler ya da hâlihazırda gerçekleşmiş hileli faaliyetleri izleme ve raporlamayı amaçlayan tespit tedbirleridir [12]. Tablo 4.1.'de, mobil para hizmetlerinin çoğu için kilit risk azaltma tedbirlerini özetlemektedir, ancak kapsamlı bir liste değildir, söz konusu tedbirlerin her biri, mobil para ile ilgili belirli risklerden en az birini ilgilendirmektedir. Örneğin, erişim haklarının kontrol edilmesi, müşteri bilgilerinin çalınması riskini azaltırken, şüpheli işlemlerin takibi ve analizi, hileli faaliyetlerin görünürlüğünü artırır.

Tablo 4.1. Ana risk azaltma önlemleri

Önleyici tedbirler	Algılama önlemleri
- Müşteri bilgilerini korumak için erişim haklarının kontrolü - Yüksek riskli prosedürler için görevlerin ayrılması (örneğin, e-paranın muhasebe mutabakatı) hataları veya sahtekârlığı önlemek için - Kara paranın aklanması ve terörün finansmanı ile ilgili risklerin azaltılması için sınırlar (AML / CFT) - Müşterileri eğitmek ve korumak için müşteri bilgilendirme kampanyaları - Acentelerin kabul edilebilir uygulamalara ve hizmetin işleyiş şartlarına ve koşullarına göre eğitimi - Görev ve sorumluluklar konusunda çalışan eğitimi	- Şüpheli faaliyetlerin izlenmesi ve analizi - Sistem erişim etkinliklerini izleme - Güçlü müşteri tazminatı prosedürlerinin oluşturulması ve potansiyel sorunların tırmanması - Bayların işlem aktivitelerini izleme - Müşterilere SMS uyarısı - Hiyerarşi ile Yüksek Miktarlı İşlemlerin Gözden Geçirilmesi

Önleyici tedbirler genellikle, özellikle mobil para sisteminin teknik özelliklerine göre başlangıçta bütünleşmiş edildiğinde, tespit tedbirlerinden daha etkili kabul edilir. Görevlerin ayrıştırılması, erişim haklarının kontrolü veya ağların güçlendirilmesi gibi önlemler uygulamaya konulduğunda, bu uygulamanın uygun bir şekilde, uygun bir şekilde gerçekleştirilmesi önemlidir. Tedbirler mevcutsa ancak kolayca atlatılabilirse (örneğin, görevlerin ayrıştırılması varsa, ancak kullanıcılar düzenli olarak parolalarını önlemek için parola verirse), sahtekârlık riski devam eder.

Hizmetin ve mevcut kaynakların boyutu, önleme tedbirlerinin göreceli ağırlığını veya bir ağdaki tespit önlemlerini etkileyebilir.

4.4. Riskleri Azaltmak İçin Gerekli Araçlar

Mobil para hizmetleri, etkili kontrol önlemlerini uygulamak için üç araç içerir:

- Güvenilir ve ilgili istatistiksel bilgi ve gösterge panoları;

- Müşteriler de dâhil olmak üzere çeşitli paydaşlar ile iyi araçlar ve iletişim kanalları;
- Bilgilerin nasıl bildirildiğini ve şüpheli etkinlik tespit edilirse ne yapılacağını tanımlayan dâhili prosedürler.

İstatistiksel bilgi, mobil para dolandırıcılığının önlenmesi ve izlenmesi için önemli bir varlıktır. İşlem izleme, herhangi bir etkili stratejinin önemli bir parçasıdır, ancak tüm mobil para hizmetleri için geçerli tek bir gösterge paneli yoktur. Güvenilir istatistiksel bilgi elde etmek için, idari ekipler ve / veya platform sağlayıcıları ile çalışmak gereklidir. Safaricom M-PESA: Önleyici tedbir olarak müşteri eğitimi veya iletişimi.

Safaricom şirketinin M-PESA servisi ana önceliklerinden biri, müşterilerine karşı sahtecilik riskini azaltmaktır. Basit algılama önlemleri ile içerik almaktan ziyade, Safaricom müşterilerine karşı sahtecilik riskini azaltmak için önleyici tedbirlere dayanır. Şirket, en etkili önleyici tedbirin müşterileri açık iletişim yoluyla bilgilendirmek olduğunu bulmuştur. M-PESA müşterilerine ulaşmak için, Safaricom çok yönlü bir yaklaşım kullanır. SMS'lerin toplu postaları, yerel lehçelerde radyo mesajları ve gazete reklamları müşteri bilgilendirme kampanyalarında kullanılır. Net iletişim yoluyla müşteri bilgilerinin iyileştirilmesi, Safaricom ‘un M-PESA müşterilerine karşı sahteciliği önlemedeki başarısı için kritik öneme sahiptir [33].

4.5. İletişim

İç veya dış iletişim, mobil para hizmetlerinin risk kontrol önlemlerine uyumu sağlamak için kullanması gereken ikinci araçtır. Yürürlükteki risk azaltma önlemlerinin sayısına ve karmaşıklığına bağlı olarak, süreçte çok sayıda paydaş bulunabilir. Dâhili olarak, mobil para yöneticileri, idari destek ekipleri, müşteri hizmetleri personeli ve finans ve yönetim kontrol personeli, herhangi bir şüpheli olayı veya şüpheli faaliyeti bildirmek için bilgilendirilmeleri ve teşvik edilmeleri gereken normal katılımcılar arasındadır.

Önleyici tedbirlerin etkinliği için aracılara ve müşterilere dış iletişim eşit derecede önemlidir [12]. Müşterileri dolandırıcılık riskini nasıl davet edebilecekleri konusunda eğitmek, M-PESA örneğinde de belirtildiği gibi, müşteri dolandırıcılığı sıklığını azaltmak için kritik önleyici bir tedbirdir.

Son olarak, dolandırıcılık veya şüpheli faaliyet tespit edildiğinde, bu tür şüpheli faaliyetlerin sorumlulara uygun şekilde bildirilmesini sağlamak için iç prosedürler yürürlükte olmalıdır. Bu bilgilerin iletilmesi ve uygun önlemlerin alınması için bu iç prosedürler eksiksiz olmalıdır.

Bir müşteri paranın kendi hesabından kaybolduğundan şikâyetçiyse, müşteri hizmetleri merkezinin bu bilgiyi nasıl alacağını bilmesi gerekir. Benzer şekilde, eğer iddia belirli bir memur için ise, para ile ilgili disiplin cezasını öngören bir süreç de olmalıdır. En ciddi durumlarda, bir aracı bir müşterinin PIN kodunu kullanarak bir müşterinin hesabına eriştiğinde, bazı mobil operatörler genellikle derhal hesabını daha fazla araştırmayı beklemeden engellerler. Aracılar tarafından küçük çaplı ihlal durumunda, operatörler daha fazla harekete geçmeden önce genellikle bir uyarı yayınlar. Dolandırıcılığın önlenmesi, kuruluşunuzdaki sahtecilik karşıtı program hakkında temel olarak iletişim kurmaktadır [12]. Gerçekten de, eğer herkes sahtekârlık veya kontrol ihlallerini tespit edebilecek sistemlerin varlığından haberdarsa ve sisteminizdeki her işlemin izlendiğini herkes bilirse, mükemmel bir önleyici tedbirin sahibi olursunuz. Personelin, dolandırıcılığın hızlı bir şekilde fark edileceğinden dolandırıcılığa düşmek için işe yaramadığını bildirmekten oluşur.

BÖLÜM 5. SAHTEKÂRLIK TESPİTİ

Bu bölüm mobil işlem hizmetleri için davranışsal sahtekârlık tespiti alanındaki katkılara ayrılmıştır. Bir işlem simülatörü sunuyoruz, tasarımı gerçek verilerin kullanımına dayanıyor. Bu şekilde üretilen sentetik veriler, sınıflandırma algoritmalarını mobil işlem servislerine uyarlamak için kullanıldı.

5.1. Sentetik Veri

Dolandırıcılık tespiti, dolandırıcılık nedeniyle gelir kaybını ortaya çıkarmak ve sınırlamak için giderek daha önemli hale geliyor. Sahtekârlıklar hizmetleri yasadışı olarak ödemeden veya kâr etmeden kullanmaya çalışır. Bu hizmet sağlayıcılara maddi zarar sağlar. Sahtekârlıktan kaynaklanan kayıpları azaltmak için bir sahtekârlık algılama sistemi devreye alınabilir. Bununla birlikte, kapsamlı ayarlama ve testler yapılmazsa, algılama sistemi tüm yanlış alarmların sahtekârlık azaltma kazanımından ziyade insanca araştırılması açısından daha pahalıya mal olabilir. Modelleri, mekanizmaları ve tespit sistemlerini değerlendirmek için uygun test verileri bu gereklilikleri karşılamak için esastır. Verilerin hedef sistemdeki normal davranışı ve saldırı davranışını temsil etmesi gerekir. Çünkü algılama sistemleri giriş verilerindeki değişikliklere karşı çok hassas olmalıdır. Bu veriler aynı zamanda algoritmaların standartlarını karşılamalıdır. Bazı algoritmalar, dolandırıcılık olaylarının fazla temsil edilmesiyle birlikte büyük miktarda etiketlenmiş veri gerektirir. Ancak sorun, bu tür verilerin gerçek sistemlerde bulunmamasıdır [34]. Direnç testleri için veri miktarı da mutlaka mevcut değildir [34]. Dezavantajları içermelerine rağmen, algılama algoritmalarının eksiksiz ve güvenilir bir şekilde incelenmesi için sentetik veriler üretilebilir. Bu nedenle bir sentetik veri üretecinin ana ilgi alanları şunlardır:

- Gerektiği kadar veri ve senaryo oluşturma yeteneği, örneğin algoritmaların özelliklerini test etmek için üretilen verilerin parametrelerinin kontrolü,
- Performans değerlendirmesini kolaylaştırmak için etiketlerin varlığı,
- Sistem kullanıcılarının gizliliğine saygı duyulması ve genel olarak veri gizliliği ile ilgili sorunların azaltılması,
- Henüz konuşlandırılmamış sistemler için veya çok az geri bildirim bulunan sistemler için algoritma değerlendirme imkânı.

5.2. Mevcut Çalışma

5.2.1. Sentetik veri kullanımı

Değerlendirme, eğitim ve test için sentetik verilerin kullanılması, gerçek verilerin kullanımına göre birçok avantaj sunar. Sentetik verilerin özellikleri, orijinal veri setlerinde bulunmayan çeşitli koşulları sağlayacak şekilde özelleştirilebilir. Emilie Lundin ve ark [34], sentetik verilerin kullanımı gerçek verilerle ilgili dezavantajları önler. [35] İçin Sentetik veriler için en az üç uygulama alanı vardır. Birinci Sahtekârlık Algılama Sistemini (FDS), belirli bir ortama eğitmek ve uyarlamaktır. Bazı Sahtekârlık Algılama Sistemini, normal olarak gerçek hizmet verilerinde bulunmayan birçok sahtekârlık örneği de dâhil olmak üzere, büyük miktarda eğitim verisi gerektirir. İkinci uygulama alanı, tespit oranı gibi performans parametreleri üzerindeki etkiyi incelemek için bilinen dolandırıcılık varyasyonlarını veya yeni dolandırıcılıkları sentetik verilere enjekte ederek bir FDS'nin özelliklerini test etmektir. Yanlış alarm hızı, saldırı olmadan normal kullanım olarak tanımlanan arka plandaki veriler değiştirilerek de test edilebilir. Üçüncü uygulama alanı, karşılaştırmalı analiz durumunda SDS'leri karşılaştırmaktır.

Bu çalışmanın amacı, bir sahtekârlık algılama sisteminin eğitimi ve testi için sentetik veri üretme ve kullanma fizibilitesini test etmektir. Sentetik veri üretimimiz [36]'da önerilen yönteme dayanmaktadır. Ancak bundan önce mevcut diğer sentetik veri jeneratörlerini göstereceğiz.

5.2.2. Mobil veri jeneratörleri

Bu alanda sahtekârlık tespitinin gerçek verilerin olmadığı gözlemlenebilir ve ayrıca sentetik veriler çok az kullanılır. O zamana kadar iki yapay veri üreticisinin varlığına dikkat ediyoruz. Her jeneratörün kendi amaçları vardır. Böylece Emilie Lundin Barse ve Erland Johnson'ın benzetimlik not edebiliriz. L Barse göre [37], talep üzerine bir video sisteminde sahtekârlığı tespit etme hedefi vardır. Bu jeneratör sistemi ve kullanıcı davranışını modellemektedir.

Çünkü mobil cihaz işlem sistemlerini hedef aldığı için diğerinde bağlamımızda biraz benzerlik var. Ancak vaka çalışmaları farklıdır. Edgar Alonso ve ark göre [38], para aklamanın tespit edilmesini hedeflerken, biz [19] 'da tanımlanan davranışsal sahtekârlığı araştırıyoruz.

Ek olarak, sentetik verilerin oluşturulması için başka bir yöntemin varlığını not edebiliriz. Bunlar bizim bağlamımızdan uzaktır. Çünkü dolandırıcılık tespitini hedeflemiyoruz. Ancak Jesk ve Coll, kredi kartı işlemleriyle ilgili veri oluşturmanıza olanak sağlayan bir jeneratör sunar. Jeneratörleri ödeme alanına en yakın olarak kabul edilebilir. Ancak çalışmamız için Java'da uygulanan MASON sürüm 19 adlı MABS araç setini kullanan Paysim benzetimliği benimsiyoruz. MASON, çoklu platform olduğu için seçildi. Diğer ajan çerçevelerine kıyasla paralel eştirme ve hızlı yürütme hızını destekler. Bu, özellikle PAYSIM gibi birçok çalışan ve maliyetli benzetim için önemlidir.

5.2.3. Paysim üreteci

PaySim tasarımı tarafından tanıtılan ODD modeline dayanıyordu (Grimm ve ark. 2006). ODD, 3 ana bölümden oluşur: Genel Bakış, Tasarım Kavramları ve Ayrıntılar.

Bu benzetimliğin amacı, mobil işlemler alanında yapılan ödemeleri simüle etmektir. Simülatör, mobil işlemler için sentetik veriler üretmek için nihayetinde

simülasyonlar gerçekleştirmelidir. Simülatör, Ericsson tarafından sağlanan birçok gerçek işlem verisine çok benzer sentetik veriler üretmelidir. Amaç, daha sonra dolandırıcılık tespiti hakkında daha fazla bilgi edinmek için bilimsel topluluk tarafından kullanılabilecek ve anında veri üretebilecek bir jeneratöre sahip olmaktır. Model, müşteri olan ana varlık tipine sahiptir. Her müşterinin günlük / yıllık işlem limiti, işlem limiti ve müşterinin maksimum bakiyesi gibi müşterinin yetkili davranışını tanımlayan bir görünüş vardır. Ayrıca, her müşteri için işlem sayısı, para çekme, transfer ve depozito sayısı depolanmaktadır. Her müşterinin işlemlerin esas alındığı bir temel para birimi vardır. Müşteri para yatırma, çekme ve transfer şeklinde işlem yapabilir. Her işlem için müşteride saklanır ve kaydedilir.

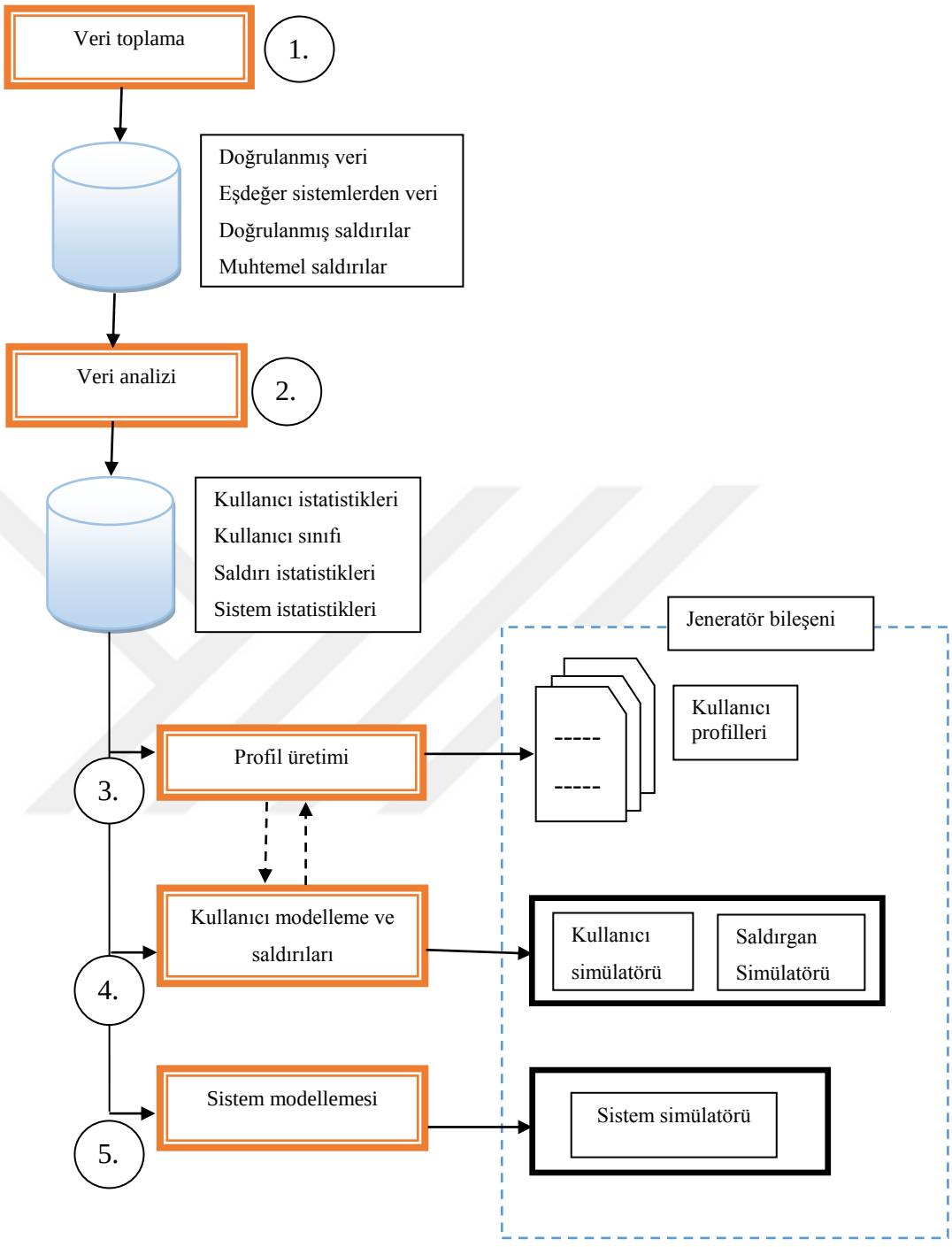
5.3. Model Ve Uygulama

Bir hatırlatıcı olarak mobil işlem sistemleri, sahiplerin satın alma veya transfer gibi çeşitli işlemleri gerçekleştirmelerini kolaylaştırma rolüne sahiptir. Bu tutucular, operatör tarafından verilen elektronik para m-para birimini kullanır. Bu para birimi dağıtıcılardan satın alınabilir veya değiştirilebilir. Böyle bir sistem teslim edilebilir ve MASSIF projesinde açıklanmaktadır.

5.3.1. Veri üretme yöntemi

Sentetik veriler Johnson ve ark [35], açıklanan yöntem ile üretildi. Veri oluşturma işlemini otomatikleştirmek için gereken ana bileşenler, kullanıcının sistemdeki kullanıcı davranışını ve kullanıcı profillerini, kullanıcı / saldırgan simülatörünü ve sistem simülatörünü belirtmesidir. Metodolojinin amacı bu bileşenlerin üretimine rehberlik etmektir. Başlangıç noktası, kullanıcının hedef sistemdeki beklenen davranışı hakkında bilgi toplamaktır. Metodoloji arka plan verilerinin ve saldırıların oluşturulmasını içerir. Bu nedenle olası saldırılar ve normal kullanımları hakkında bilgi sahibi olmak gereklidir. Bu veriler kullanıcıların ve sistemlerin modellenmesinde temel teşkil eder. Şekil 5.1.'de yöntem gösterilmektedir.

İlk adımda hedef sistemin beklenen davranışını temsil etmesi gereken verileri toplamaktır. Veriler, hedef sistemdeki otantik arka plan verilerini, benzer sistemlerdeki arka plan verilerini, otantik saldırıları ve diğer olası saldırı kümelerini içerebilir. İkinci adımda toplanan verileri analiz etmek ve kullanıcı sınıfları, kullanım istatistikleri, saldırı özellikleri ve sistem davranışı istatistikleri gibi önemli özellikleri tanımlamaktır. Üçüncü adımda önceki adımdaki bilgiler, öngörülen saldırıları tespit etmek amacıyla tutulacak parametreleri belirlemek ve parametre istatistikleriyle tutarlı kullanıcı ve saldırgan profilleri oluşturmak için kullanılır. Dördüncü adımda bir kullanıcı şablonu oluşturulur. Seçilen profil ayarlarını koruyacak kadar karmaşık olmalıdır. Saldırganlar da bu adımda modellenmiştir. Kullanıcı ve saldırgan simülatörleri modelleri uygular. Sistem beşinci adımda modellenmiştir ve bu model aynı tipteki kullanıcı eylemleri için hedef sisteme eşdeğer log verisi üretebilecek kadar doğru olmalıdır. Sistem simülatörü daha sonra bu modele göre uygulanır.



Şekil 5.1. Sentetik veri üretme yöntemi, [33]

Kullanıcı eylemleri oluşturmak için bir kullanıcı simülatörü yerine insanlar kullanmak ve bir sistem simülatörü yerine gerçek sistemin tümünü veya bir kısmını kullanmak mümkündür. Bu, bazı durumlarda örneğin sistemin veya kullanıcının davranışının çok karmaşık olması ve ayrıntılı olarak modellenmesi gerektiği

durumlarda tercih edilebilir. Deneylerimizde normal arka plan verileri üretmek için sahte davranış ve taklitleri taklit eden insanları kullandık.

5.3.2. Mobil para transferinde kullanıcı davranışı

Para işlem günlükleri, birden fazla oyuncu tarafından paralel olarak gerçekleştirilen eylemleri ve mantıksal davranışları ortaya çıkarabilir. Bunlar bizi çok ajanlı bir yaklaşım seçmeye zorluyor. Çok ajanlı sistemdeki temsilciler, mobil işlem servisine abone olan meşru kullanıcılar veya sisteme saldıran dolandırıcıların sistemdeki oyuncularıdır. Bu aktörlerin her birinin farklı rolleri vardır ve belirli eylemlerle ilişkilendirilir. Bu aktörler:

- Sahipler terminallerini transfer veya ödeme yapmak için kullanırlar.
- Tüccarlar mal ve hizmet sağlamak için e-para kabul eder.
- Aracı olarak da adlandırılan elektronik para dağıtıcıları, elektronik paranın satıcısıdır ve bu durumu taşıyıcıya veya tüccara ihraç eden operatörden dağıtımına izin verir.

İşlemleri alışkanlıklarıyla ilgili olduğu varsayımına dayanan meşru kullanıcılar için. Bu tekrarlayan ve oldukça sık bir işlem kümesi gerçekleştirmeleri gerektiğini gösterir. Bu varsayım işlemlerin normal veya anormal olarak sınıflandırıldığı anormallik saptama sahtekârlık saptama yöntemleri bağlamında da değerlendirilir. Genel olarak bu alanda normal işlemlerin kullanıcıların alışkanlıklarına karşılık geldiği ve sahtekârlıkların kaçınılmaz olarak normal işlemlerden farklı olduğu ve bu nedenle anormal işlemlerin bir alt kümesi olduğu düşünülmektedir.

5.3.3. Kullanıcı alışkanlıkları

Kokkinate göre [39], bir alışkanlık meşru işlemlerde bir denklik sınıfıdır. Başka bir şekilde bir alışkanlık, meşru bir işlem sırasında tekrar eden bir davranıştır [14]. Bu alışkanlık, normal bir dağıtımın iki işlemidir. Bunlar başlangıç tarihi, bitiş tarihi arasındaki zaman farkı ve normal dağılım izleyen bir miktar olan bir işlem türü ile

tanımlanır. Bu iki tarih, alışkanlığın yer aldığı süreyi belirler. Taşıyıcının C davranışının bir dizi alışkanlıktan oluştuğu hipotezini gösterir; buradaki Hi, bir işlem türü için alışkanlıktır [14].

5.3.4. Saldırılar

Saldırılardan bahsetmeden bu bölümü bitiremeyiz. Yukarıda listelendiği gibi birkaç tür saldırı vardır. Ancak yapılandırmamıza bağlı olarak, bir kişi bir mobil para müşterisinin telefonunu çalabilir veya kullanabilir ve işlem yapabilir. Veyahut hizmetin bir aktörü bile katır adında bir ortak ağı oluşturarak gayri meşru bir işlem yapabilir. Birçok sahtekâr, işlemleri yapmak için sisteme Truva atı virüs bulaştırabilir.

BÖLÜM 6. SINIFLANDIRMA ALGORITMALARININ UYARLANMASI

Algoritmalar çok sayıdadır ve özellikle mobil para transfer sistemindeki dolandırıcılık tespiti alanında birçok araştırma alanında uyarlanabilir. Bu çalışma için yalnızca denetimli otomatik öğrenme tarafından oluşturulan bir modelle sınıflandırma algoritmaları ile sınırlı olacağız.

Şimdiye kadar mobil para transferinde dolandırıcılık tespiti için sınıflandırma algoritmaları üzerine yapılan çalışmaların çoğu bankacılık ve telekomünikasyon alanındadır. Birkaç temel var ancak çoğu. Mobil para transferinde dolandırıcılık durumuyla ilgilenmiyor. Ancak PAYSIM simülatörü bu alanla ilgilenen bir veritabanı üretiyor.

Bu bölüm, sınıflandırma yöntemlerinin adaptasyonunu incelemeyi amaçlamaktadır. Metodolojiden başlıyoruz ve elde edilen sonuçlarla bitiriyoruz.

6.1. Metodoloji

Kullanılan yöntem ilk önce aşağıdaki şekilde sunulabilir: PAYSIM simülatöründen alınan veriler karşılaştırılacaktır. Daha sonra en iyi sonuçları veren olanı seçtik ve birkaç algoritmayı test edeceğiz ve en iyisi seçilecektir. Daha sonra en iyi sonuçları veren algoritmalar seçilir. Yeni bir veritabanında sahtekârlığı tespit etmek için seçilen algoritma ve en uygun parametreler kullanılarak çalışmaya devam edilir. Öte yandan bu yöntemi değerlendirme aşaması farklı veri setleri ve üç deneyin prosedürü gibi üç aşaması vardır.

6.2. Değerlendirme Kriterleri

Verilerin sınıflandırılmasında değerlendirme kıstasları dikkate alınarak çok önemlidir. Sahte işlemler geçmişte gerçekleşirken, tüm veritabanı girişlerini yasal işlemler olarak sınıflandıran bir algoritma düşünün. Bu durumda değerlendirme kıstas doğru sınıflandırma oranıysa, sonuç% 100 başarılı olmaz. Dolayısıyla dayandığımız değerlendirme kriterleri şunlardır: Doğru sınıflandırma oranı, Kappa katsayısı ve Matthews korelasyon katsayısı. Bu göstergeler, sınıfların dağılımı zayıf dengelendiğinde sınıflandırma algoritmalarının alaka düzeyini ölçmeyi mümkün kılmaktadır. Algoritmaların değerlendirilmesinde yürütme süresini de dikkate alacağız. Bunun için test ve öğrenme aşaması zamanları dikkate alınır.

Doğru sınıflandırma oranı, uygun şekilde etiketlenmiş işlemlerin yüzdesini ölçer. Bu değer %100'e ne kadar yakınsa, algoritmanın performansı o kadar iyi olur. Bu oran bir gösterge olarak tutulur.

Öğrenme ve test aşamalarının süresi algoritmaların performansını belirler. Seçim en düşük hesaplama sürelerine dayanır.

6.2.1. Matthews korelasyon katsayısı (MCC)

Matthews's korelasyon katsayısı (MCC), ikili (iki sınıf) sınıflandırmaların kalitesini ölçmek için makine öğrenmesinde kullanılır. Doğru ve yanlış, pozitifleri ve negatifli bir ölçü olarak kabul edilir. CC, esasen gözlenen ve öngörülen ikili sınıflandırmalar arasında bir korelasyon katsayısıdır. Berger ve ark göre[40], MCC karışıklık matrisini sentezlemenin bir yoludur. Bu satırların ve sütunların dikkate alınan farklı sınıfları temsil ettiği bir kare matristir. Matristeki her kutu, sütunda temsil edilen sınıf olarak sınıflandırılmış gerçek sınıfın (satırda gösterilen) örnek sayısına karşılık gelir. Bu matrisin köşegeni, doğru sınıflandırılmış örneklerin sayısına karşılık gelir. Sahte işlemlerin pozitif sınıfı temsil ettiği ve meşru işlemlerin negatif sınıfı temsil ettiği 2 sınıflı bir sınıflandırma probleminin karışıklık matrisi, Tablo 6.1.'de

gösterilmiştir. Matthews'un korelasyon katsayısı aşağıdaki eşitlik kullanılarak (Denklem 6,1) hesaplanmıştır.

$$\mathrm{MCC} = \frac{(\mathrm{VP}.\mathrm{VN})-(\mathrm{FP}.\mathrm{FN})}{\sqrt{(\mathrm{VP}+\mathrm{FP})(\mathrm{VP}+\mathrm{FN})(\mathrm{VN}+\mathrm{FP})(\mathrm{VN}+\mathrm{FN})}} \quad (6.1)$$

Sonuç, -1 ile 1 arasında bir değer döndürür. 1 katsayısı, kusursuz bir tahmini temsil eder.

Tablo 6.1. Sınıflandırma probleminin kafa karıştırıcı matrisi

		Tahmin	
		Pozitif	Negatif
Gerçek	Pozitif	(DP)	(YN)
	Negatif	(YP)	(DN)

Sıfır ise rastgeledir tahminden daha iyi değildir ve -1, tahmin ile gözlem arasındaki uyuşmazlığı belirtir.

6.2.2. Kappa katsayısı

Yargılamalar arasındaki anlaşma, aynı amaç ile ilgili iki veya daha fazla bilgi parçasının uygunluğu olarak tanımlanır. Bu nedenle anlaşma veya "uyumluluk" oranı Cohen'in Kappa katsayısı ile tahmin edilir [40]. Burada çalışmamızda meşru veya hileli olabilecek bir işlemin durumunu gözlemlemek için sınıflandırma algoritmaları arasındaki anlaşmanın derecesini değerlendirmek istiyoruz.

Nitel ve nitel olmayan değerlendirmeler arasında gözlenen anlaşma, "rastgele" bir bileşen ile "gerçek" bir anlaşma bileşeninin toplamından kaynaklanmaktadır. Kappa katsayısı K [41], eşleşen niteliksel kararlar arasındaki fiili anlaşmanın yoğunluğunu veya kalitesini ölçmeyi önermektedir. Çalışmamızda bir sınıflandırma algoritmasının rastgele bir karardan ne kadar farklı olduğunu ölçmek için Kappa kullanılmıştır. R

yargı modalarına sahip, istatistiksel olarak bağımsız iki gözlemci arasında r> 2 olan bir uzlaşma çalışması durumunda, Kappa katsayısı yazılır:

$$K = \frac{Po - Pe}{1 - Pe} \tag{6.2}$$

Po, incelenen sınıflandırma algoritmasının temel gerçeğe uygun olduğunu ve ***Pe***, rastgele bir fonksiyonun temel gerçeğe uygun olduğu ihtimalini temsil eder. Bu iki oran karışıklık matrisinden de hesaplanır. Po oranı aşağıdaki formülden kullanarak (Denklem 6.2) hesaplanmaktadır:

$$Po = \frac{DP+DN}{DP+DN+YP+YN} \tag{6.3}$$

Pe oranı gelince, aşağıdaki şekilde kullanarak (Denklem 6.3) hesaplanır:

$$Pe = \frac{(DN+YP)(DN+YN)+(DP+YN)(DP+YP)}{(DP+DN+YP+YN)2} \tag{6.4}$$

Kappa katsayısı, boyutsuz -1 ile +1 arasında olan gerçek bir sayıdır. Daha fazla Kappa 1'e yakındır ve sınıflandırma algoritması rastgele bir karar işlevi gibi görünmektedir. Ayrıca sınıflandırma algoritması verileri kötü bir şekilde sınıflandırırsa, Po 0'a yakındır ve Kappada 0'a çok yakındır, hatta negatiftir. Landis ve ark göre [42], farklı Kappa değerlerini yorumlamak için Tablo 6.2.'yi önermiştir.

Tablo 6.2. Landis ve ark tarafından önerilen anlaşma derecesi ve Kappa değeri.

Anlaşma	Kappa
Mükemmel	1 - 0,81
İyi	0,80 – 0,61
Ilımlı	0,60 – 0,21
Kötü	0,20 – 0,0
Çok kötü	< 0,0

6.3. Kullanılan Veri Setleri

PAYSIM simülatörünün yapılandırmasından bir aylık bir süre için bir veritabanı oluşturulmuştur. Bu veritabanı başlangıçta 1048576 adet işlem içermektedir. Bu işlemlerden 1047434 meşru işlem, 1142 işlem hırsızlık izlemektedir. Bu veritabanından sekiz yeni veritabanı oluşturuldu. Bu veritabanı aralarında en iyi temeli elde etmek için değişiklik testlerden geçecek ve sonunda sınıflandırma için uyarlanacaktır.

6.3.1. Veri formatı

Her şeyden önce, Tablo 6.3.'te temsil edilen verilerin formatı korunur ve yalnızca temel gerçeğin temsili değiştirilir. Başlangıçta temel gerçek iki sınıfla temsil edilir: Sınıf 0, meşru işlemi ve 1 hileli işlemi temsil eder. Bu ilk veritabanı DB_init ile gösterilir. Değişiklikten sonra sekiz sınıfa ayrıldık. Meşru sınıflar: L_DEP yatırma alışkanlıkları, L_DEBIT iletişim süresi alışkanlık alışkanlıkları, L_TRF meşru özel transferler, L_CASH_O olağan biçimde meşru para çekme işlemleri ve L_PAY ticari bir ödemeye karşılık gelen alışkanlıklar. Sahtekârlık işlemlerini temsil eden sınıflar şunlardır: F_CASH_T bir terminalin çalınmasının ardından gerçekleşen işlemleri, F_TRF_T_MULE, virüslü bir telefondan bir katıra doğru yapılan transferleri ve F_CASH_O_MULE bir katır tarafından gerçekleştirilen para çekme işlemlerini gerçekleştirir. Gerçekleştirilen ilk işlem için meşru olaylara karşılık gelen tüm sınıflar, 5 farklı sınıf içeren BD_5_CL veri kümesini elde etmek için tek bir sınıfta gruplandırılır. Ardından aynı sahtekârlığın iki fazına karşılık gelen iki sınıf birlikte gruplanır. Veri kümesi BD_2_CL böylece oluşturulur. Son olarak, BD_1_CL veri kümesinde işlemler başka bir değerlendirme yapılmadan normal veya sahte olarak tanımlanır.

Tablo 6.3. Brüt Format.

Adı	Anlam
ST_t	İşlemin adımı
T_t	Gerçekleştirilen işlem türü
M_t	İşlemin tutarı
N_e	Göndericinin adı
S_Exp_Av	İşlem öncesi Gönderici bakiyesi
S_Exp_Ap	İşlemden sonraki gönderici bakiyesi
N_d	Alıcının adı
S_Des_Av	İşlem öncesi alıcının bakiyesi
S_Des_Ap	İşlemden sonra alıcının bakiyesi

Temel gerçeğin temsili olan bu dört temelden verilerin formatı değiştirilir ve belirli bir süre boyunca farklı veri toplamalarına karşılık gelen bazı göstergeler eklenir. Orijinal formatın ve değiştirilmiş formatın farklı alanları sırasıyla Tablo 6.3.'te verilmiştir. Tablolardaki alanların görünüm sırası, kayıtlardaki sıralarına karşılık gelir. Toplu veriler, yalnızca geçerli işlemden önceki olayları dikkate alır. Böylece dört yeni veritabanı, BD_8_CL_M, BD_5_CL_M, BD_2_CL_M, BD_1_CL_M oluşturuldu.

Ham biçim yalnızca işlemi açıklar. Kilometre taşını, işlem türünü, işlemin alıcısını ve tutarını işlemden önceki ve sonraki ilgili bakiyelerini gösteren farklı alanlar içerir. Dolandırıcılık tespiti için sınıflandırma algoritmalarının performansı, girdi verileri toplanmış veriler içerdiğinde daha iyidir. Çalışmamızda bu öneri dikkate alınmamıştır.

Bu noktada, toplam sekiz veri seti vardır. Her birine temel bileşen analizi uygulanır [43]. Bu, bir olayı niteleyen farklı boyutların, yani yukarıda ayrıntılı biçimde verilen formatların alanlarını ilişkilendirmeyi amaçlar.

6.4. Deneyler

Veritabanı seçiminden sonra çeşitli deneyler için WEKA yazılımı (Bilgi Analizi için Waikato Ortamı) seçilir. Bu yazılım birkaç veri madenciliği algoritması ve makine öğrenmesi içeriyor. WEKA, geliştirme için bir algoritma kütüphanesine grafiksel bir ara yüze ve bunları yönetmenize izin veren çok gelişmiş özelliklere sahiptir.

İlk deneyimiz en iyi veritabanını bulmaktır. Bunu yapmak için rastgele iki sınıflandırma algoritması seçilebilir. Böylece rasgele tatbikat bir PART Karar Tablosu ilk DB_8_CL veritabanından türetilmiş sekiz veri setine uygulanır. Bu algoritmaların kullanılması, hem birkaç yöntem üzerinde hem fikir birliği elde edilmesini hem de deneyin hesaplama ve performans sürelerini sınırlandırmayı mümkün kılar.

Her algoritma için yazılım tarafından önerilen varsayılan ayarları koruyoruz. Çapraz doğrulama yöntemi kullanılır. Bu veri kümesini birkaç kez burada on kez örneklemeyi içerir. Her örnek daha sonra öğrenme için kullanılan diğer örneklere karşı bir test temeli olarak kullanılır. Amaç bir veri kümesi üzerinde bir model öğrenmeyi daha güvenilir hale getirmektir. Tablo 6.2.'de tanımlanan kriterlere göre en iyi sonuçları temsil eden aşağıdaki deneyler için seçilir.

Daha iyi veriler elde ettikten sonra en iyi sınıflandırma algoritmalarını seçmek için ikinci deneyi yapmak için bunları kullanacağız. Bu algoritmalar yukarıda tanımlandığı gibi denetimli bir makine öğrenme modeline dayanmaktadır.

Bu çalışmalar için bölüm 3.5.'te listelenen farklı sınıflandırma yöntemlerini temsil eden algoritmalar dikkate alınmıştır. Bu algoritmalar sekizli bir sayıdır. Bayes ağı; saf bir Bayesian sınıflandırması, geniş bir kenar boşluğu ayırıcısı, k en yakın komşular yöntemi; K* algoritması; çoğunluk karar tablosu; PART tipi karar tablosu; bir karar ağacı C4.5 ve rastgele bir orman. Varsayılan ayarlar kullanılır. Tablo 6.2.'de tanımlanan kriterler bu algoritmaları değerlendirmeye ve en iyi performansı sunanları seçmeye izin verir.

Önceki deneyler WEKA yazılımının varsayılan ayarlarına dayanmaktadır. En verimli veri setlerini ve algoritmaları seçmeyi mümkün kıldılar.

6.5. Sonuçlar

Bu adım farklı deneylerin sonuçlarını gösterir.

6.5.1. Veri setlerinin seçiminde ilk denemenin sonucu

Sekiz veri setindeki testler için elde edilen sonuçlar ve bu iki algoritma için bu göstergelerin her biri için hesaplanan ortalama Tablo 6.4.'te ve 6.5.'te özetlenmiştir. Hatırlatma olarak bu testler Tablo 6.2.'de tanımlanan kriterlere dayanmaktadır.

Tablo 6.4. Sekiz veritabanı için rastgele ormanı yöntemine uygulanan göstergelerin sonuçları ve ortalaması

	Ortalama Değer				KAPPA Katsayısının Yorumlanması	
Veritabanlar	Başarı Oranı	Kappa	MCC	Zaman (saniye)	Kappa Değeri	Yorumlama
DB_8_CL	99,32%	0,00	0	5,62	0-0,20	Kötü
DB_5_CL	99,87	0	0	4,78	0-0,20	Kötü
DB_2_CL	99,97	0	0	2,83	0-0,20	Kötü
DB_1_CL	99,90	0	0	3,77	0-0,20	Kötü
DB_1_CL_M	99,70	0,98	0,99	35,9	0,81 – 1	Mükemmel
DB_2_CL_M	99,10	0,99	0,97	25,7	0,81 – 1	Mükemmel
DB_3_CL_M	96,90	0,96	0,93	3,45	0,81 – 1	Mükemmel
DB_4_CL_M	96,03	0,94	0,96	2,45	0,81 – 1	Mükemmel

Tablo 6.5. Sekiz Veritabanına ilişkin PART tipi karar tablosunda uygulanan göstergelerin sonuç ve ortalaması

	Ortalama Değer				KAPPA Katsayısının Yorumlanması	
Veritabanlar	Başarı Oranı	Kappa	MCC	Zaman (sn)	Kappa Değeri	Yorumlama
DB_8_CL	99,19%	0,3374	0,35	0,01	0,21 - 0.40	Ilımlı
DB_5_CL	99,79	0,159	0,18	0,01	0 - 0.20	Kötü
DB_2_CL	99,93	-0,0003	0	0,01	< 0	Çok kötü
DB_1_CL	99,85	-0,0007	0	0	< 0	Çok kötü

Tablo 6.5. (Devamı)

		Ortalama Değer			KAPPA Katsayısının Yorumlanması	
DB_1_CL_M	99,59	0,9936	0,9946	0,19	0,81 - 1	Mükemmel
DB_2_CL_M	99,88%	0,9982	1	0,11	0,81 - 1	Mükemmel
DB_3_CL_M	99,80%	0,9974	0,9978	0,33	0,81 - 1	Mükemmel
DB_4_CL_M	99,85%	0,9979	0,998	2,97	0,81 - 1	Mükemmel

6.5.2. Seçili veritabanları

Rastgele orman algoritması için DB_1_CL_M ve DB_2_CL_M veri setleri en iyi sınıflandırma performansını gösterir. Bu sonuçlar diğer veri setlerinden daha yüksek öğrenme süresi göstermektedir. Tablo 6.7.'te iki algoritmada elde edilen en iyi sonuçları gösteren bazları gruplandırmaktadır.

Veritabanının (DB_2_CL) en iyi başarı oranına sahip olduğu veya Kappa ve Matthews göstergelerinin kötü performans verdiği görülüyor. Bu doğru sınıflandırma oranının problemler için uygun bir kıstas olmadığını veya bir sınıfın yeterince temsil edilmediğini göstermektedir.

Tablo 6.6. Yukarıdaki elde edilen veritabanlarının sonuçları

	Ortalama Değer				
Veritabanlar	Başarı Oranı	Kappa	MCC	Zaman (sn)	Algoritmalar
DB_1_CL_M	99,70	0,98	0,99	35,9	
DB_2_CL_M	99,10	0,99	0,97	25,7	Rastgele orman
DB_3_CL_M	99,88%	0,9982	1	0,11	
DB_4_CL_M	99,85%	0,9979	0,998	2,97	PART tipi

Bu yüzden en iyi sınıflandırma performansını temsil eden DB_3_CL_M veri setlerini seçiyoruz. Bununla birlikte gerçekte kullanıcı davranışlarını vurgulamak için meşru davranışların parçalandığı açık değildir. DB_4_CL_M veritabanı denemelerin geri kalanı için de seçilmiştir. Bu iki veritabanın en iyi sınıflandırma algoritmalarını seçmek için kullanılacaktır.

6.5.3. En iyi algoritmaların seçimi

Daha önce seçilen iki veritabanı, sekiz sınıflandırma algoritmasına uygulanacaktır. Benzer şekilde, farklı göstergelerin sonuçları DB_3_CL_M veritabanı için Tablo 6.5.'te ve DB_4_CL_M veritabanı için Tablo 6.7.'de gösterilmiştir.

DB_3_CL_M veritabanı için elde edilen sonuçlara göre, K* algoritmasının zayıf performansı kaydedilmiştir. Bu algoritma, Kappa ve MCC katsayısı için 0.25'e eşit olan ve öngörülen değişkenler ile temel gerçek arasındaki toplam uyuşmazlığı gösteren zayıf bir anlaşmayı gösterir. Bayesian ağı için, saf Bayesian yöntemi rastgele tatbikat ve K-en yakın komşu yöntemi, Kappa ve MCC göstergeleri ile 0.81 ile 0.9 arasında neredeyse mükemmel bir anlaşmaya sahiptir. Son olarak, J48, PART ve Karar Tablosu algoritmaları, Kappa ve MCC göstergeleri ile 0.9 - 1 arasında değişen en iyi ve aynı performansı gösterir. Yüksek Kappa ve MCC oranlarıyla bu son üç algoritma seçilir.

Tablo 6.7. DB_3_CL_M veritabanına uygulanan sınıflandırma algoritmalarının karşılaştırılması.

Algoritmalar	Başarı Oranı	Kappa	MCC	Öğrenme (Sn)	Test (Sn)
Bayes Ağları	99,5	0,9925	0,994	0,05	0,02
Naif Bayes	91,5	0,8749	0,8753	0,01	0,06
K-en yakın komşular	98,82	0,9823	0,9838	0,1	1,78
K*	58,97	0,2473	0,25	0,1	193,76
Karar tablosu	99,88	0,9982	1	3,64	0,1
PART	99,79	0,9969	1	0,08	0,1
C4.5	99,88	0,9982	1	0,03	0,1
Rastgele Ormanı	99,1	0,98	0,97	0,4	0,1

DB_4_CL_M veritabanı genellikle DB_3_CL_M veritabanından daha uzun zamanlara sahiptir. DB_3_CL_M gibi K* da Kappa ve MCC'nin bir ölçüsü olarak 0.26 ile çok zayıf bir performansa sahip. Masal ile Bayesian Ağları, Naive Bayesian ve K'nin en yakın komşuları algoritmaları 1'e çok yakın göstergelere sahipler ve bu da iyi performanslarını kanıtlıyor.C4.5 algoritmalarına gelince, karar tablosu, PART hala Kappa, MCC ile 0.9 - 1 arasındaki en iyi performansları göstermektedir. Bu nedenle önceden elde edilen seçim korunur.

Tablo 6.8. DB_4_CL_M veritabanına uygulanan sınıflandırma algoritmalarının karşılaştırılması.

Algoritmalar	Başarı Oranı	Kappa	MCC	Öğrenme (Sn)	Test (Sn)
Bayes Ağları	99,71	0,9959	0,995	0,45	0,13
Naif Bayes	95,65	0,938	0,943	0,11	0,43
K-en yakın komşular	99,68	0,9954	0,9954	1	87,72
K*	62,2	0,3876	0,3975	0,03	904,36
Karar tablosu	99,72	1	1	120,722	0,01
PART	99,84	0,9977	1	1,63	0,03
C4.5	99,84	0,9978	1	0,73	0,01
Rastgele Ormanı	96,03	0,94	0,96	0,2	0,12

6.5.4. Onaylama

Seçimleri doğrulamak için seçilen algoritmalar karşılık gelen verileri iki meşru ve bir sahte sınıf içeren ilk DB_init veritabanına sınıflandırmak için kullanılır. Göstergeleri DB_3_CL_M ve DB_4_CL_M veritabanları ile elde edilenlerden daha düşüktür. Ancak öğrenme ve test süreleri aynı kalır. Algoritmaların aynı istatistiksel dağılımın başka bir temelini sınıflandırma kapasitesine sahip olduğunu söyleyebiliriz. Bu nedenle kafa karışıklıkları matrislerinde Tablo 6.9.'da, Tablo 6.10.'da ve Tablo 6.11.'de gösterilmektedir.

Aşağıdaki tablolarda PART tipi karar tablosunun yasal olarak sahte olarak tespit edilen en fazla işlem sayısına sahip olduğu görülmektedir. Karar tablosu yöntemine gelince en meşru yanlış sınıflandırılmış işlemleri ve sıfır sayıda yanlış sınıflandırılmış sahte işlemi gösterir. C4.5 ve PART yöntemleri aynı sayıda yanlış sınıflandırılmış sahte işlem gösteriyor.

Tablo 6.9. DB_init veritabanına uygulanan C4.5 yönteminin karışıklık matrisi.

		Tahmin	
		Normal işlem	Sahte işlem
Gerçek	Normal işlem	54974	3
	Sahte işlem	64	171

Tablo 6.10. DB_init veritabanına uygulanan karar tablosunun karışıklık matrisi

		Tahmin	
		Normal işlem	Sahte işlem
Gerçek	Normal işlem	54977	0
	Sahte işlem	106	129

Tablo 6.11. DB_init veritabanına uygulanan PART tipi karışıklık matrisi

		Tahmin	
		Normal işlem	Sahte işlem
Gerçek	Normal işlem	54974	3
	Sahte işlem	28	207

Sonlandırmak için iki veritabanını DB_3_CL_M ve DB_4_CL_M veritabanını, WEKA yazılımının varsayılan değeri olan % 66'lık yüzde oranını kullanarak yeniden gruplandırarak bir test uyguladım. Bu testler seçilen üç algoritma ile gerçekleştirilir. Bu testlerle elde edilen karışıklık matrisleri Tablo 6.13.'te, Tablo 6.14'te ve Tablo 6.15.'te gruplandırılmıştır.

Karışıklık matrisine göre sekiz sınıfın yazışmaları şöyle yapılır: a = L_PAY, b = F_TRF_T_MULE, c = F_CASH_O_MULE, d = L_DEBIT, e = L_CASH_O, f = L_TRF, g = L_DEP, h = F_CASH_O_T.

Tablo 6.12. Metot C4.5 ile ilgili karışıklık matrisi

	Tahmin								
	A	b	C	d	e	f	G	h	
Gerçek	9800	0	0	0	0	0	0	0	a = L_PAY
	0	29	0	0	0	6	0	0	b = F_TRF_T_MULE
	0	0	2	0	10	0	0	0	c = F_CASH_MULE
	0	0	0	253	0	0	0	0	d = L_DEBIT
	0	0	4	0	6107	0	0	0	e = L_CASH_O
	0	8	0	0	0	2079	0	0	f = L_TRF
	0	0	0	0	0	0	3847	0	g = L_DEP
	0	0	0	0	9	0	0	18	h = F_CASH_O_T

Tablo 6.13. Karar tablosu ile ilgili karışıklık matrisi

	Tahmin								
	a	b	C	d	e	f	G	h	
Gerçek	9800	0	0	0	0	0	0	0	a = L_PAY
	0	16	0	0	0	19	0	0	b = F_TRF_T_MULE
	0	0	0	0	12	0	0	0	c = F_CASH_MULE
	0	0	0	253	0	0	0	0	d = L_DEBIT
	0	0	0	0	6111	0	0	0	e = L_CASH_O
	0	0	0	0	0	2087	0	0	f = L_TRF
	0	0	0	0	0	0	3847	0	g = L_DEP
	0	0	0	0	9	0	0	18	h = F_CASH_O_T

Tablo 6.14. PART tipi karar tablosuyla ilgili karışıklık matrisi

	Tahmin								
	A	b	C	d	e	f	G	h	
Gerçek	9800	0	0	0	0	0	0	0	a = L_PAY
	0	28	0	0	0	7	0	0	b = F_TRF_T_MULE
	0	0	2	0	9	0	0	0	c = F_CASH_O_MULE
	0	0	0	253	0	0	0	0	d = L_DEBIT
	0	0	4	0	6107	0	0	0	e = L_CASH_O
	0	8	0	0	0	2079	0	0	f = L_TRF
	0	0	0	0	0	0	3847	0	g = L_DEP
	0	0	0	0	7	0	0	20	h = F_CASH_O_T

Tablolardan üç meşru işlem tipinin doğru bir şekilde sınıflandırıldığı düşünülebilir. Bunlar bir ticari ödemeye karşılık gelen L_PAY işlemleridir, L_DEBIT iletişim süresi alım işlemleri, Mevduat işlemlerini L_DEP. Bununla birlikte, meşru işlemlerin geri kalanı C4.5 algoritmaları için kötü bir şekilde sınıflandırılır ve PART, L_CASH_O'nun alışkanlık biçimindeki meşru geri çekilmeleri durumundadır. Meşru bireyler arasında L_TRF transferleri ve karar tablosu meşru bireyler arasında L_TRF transferlerini doğru şekilde sınıflandırır.

PART tipi yöntemi için başka bir telefondan 7 işlem meşru işlem olarak algılanır ve başka bir telefondan katırlığa halen yapılan 8 işlem meşru transfer olarak algılanır.

Katırlar tarafından toplam 13 işlem hilelidir. En önemlisi kötü sınıflandırmaların sayısı belirli meşru ve katırlar arasındaki para çekme işlemleri için karşılanmaktadır.

C4.5 algoritması, dolandırıcılık olarak algılanan 84 yasal işlemi ve 25 yanlış sınıflandırılmış dolandırıcılık işlemini görüntüler. Karar Tablosunda 9 yöntemde hileli işlemler meşru ve 21 Yanlış sınıflandırılmış hileli sınıflandırma sırada yer aldı. Karar tablosu, 16 sahte meşru işlem ve dolandırıcılık olarak tespit edilen 84 meşru işlem göstermektedir. En az yanlış meşru işlem içeren algoritma, PART tipidir. En az meşru yanlış sınıflandırılmış işlemi içeren algoritma ise karar tablosudur.

BÖLÜM 7. SONUÇ

Bu tez çalışmasında mobil para sahteciliğinin tespiti ve önlenmesi çalışılmıştır. Mobil para hizmetinin temel kullanım alanları; mal, hizmet alımı, yerel para ödemesi ve para transferidir. Bu işlemler güvenli ve zamanında yapılmalıdır. Operatör tarafından ya da finansal kurumlar tarafından yönetilen elektronik para kullanılarak gerçekleştirilirler. Mobil para hizmetlerinde donanımı olarak hizmet veren akıllı telefonların güvenliği önemlidir. Burada sunulan hizmetin ve hizmete kullanılan telefonun güvenliği irdelenmiştir.

Mobil ödeme sistemlerinde dolandırıcılık riski; mobil ödeme güvenliği mimarileri; mobil terminal güvenliği ve sınıflandırma algoritmaları ile ilgilidir. Mobil para operatörlerinin ticari başarısı dolandırıcılık riskinin önlenmesidir. Bu çalışmada mobil ödeme sistemlerinde dolandırıcılığı makine öğrenmesi yöntemleri ile tespiti ve önlemesi çalışılmıştır. Sahtekârlık tespiti alanında literatürde birçok çalışma yapılmıştır. Bu çalışmalarda mobil işlem hizmetlerinde sahtekârlık tespiti sınıflandırmasında makine öğrenmesi algoritmaları kullanılmıştır. Sahtekârlık önleme konusu çalışılmamıştır. Bu çalışmada mobil terminalleri güvenliği, mobil para transfer sistemindeki sahtekârlığı önlemek ve tespit etmek için makine öğrenmesi algoritmaları kullanılmıştır.

Kullanıcılar, dolandırıcılığı önlemek için alabilecekleri güvenlik önlemlerinin farkında olsalar da, hizmet sağlayıcının mobil para hizmetini güvence altına almasında büyük bir rolü vardır. Araştırmacılar, bu kullanıcı kategorisinin dolandırıcılıktan dolayı kendilerini suçlamadıklarına inanıyor, çünkü kullanıcılar hizmetin tamamen korunmasının servis sağlayıcısına bağlı olduğuna inanmaktadırlar.

Ayrıca kullanıcıların fatura ödemesi ve ek yayın süresi gibi hizmetlerden daha fazla faydalandığı, diğer hizmetlerden ise nadir olarak faydalandığı belirlenmiştir. Araştırmacılar, bu hizmetlerin kullanımının karmaşık yapısı nedeniyle olabileceğine inanmaktadırlar.

Mobil para transferinde yapılan öneriler aşağıdaki gibidir.

- PIN paylaşımı, tüketici dolandırıcılığının önde gelen nedenlerinden biridir. O yüzden hizmet sağlayıcılar, kullanıcıların parolalarını her üç ayda bir değiştirebilmeleri için parola değişikliği yapmalarını önerir. Daha sonra kişisel tanımlama sorularını cevaplayarak doğrulanmalıdır.
- Servis sağlayıcısı, mobil para kullanıcılarının mobil para hizmetinin güvenliğinin yalnızca mobil ağ operatörlerine bağlı olmadığını, aynı zamanda kullanıcıların da bir rol oynayabileceğini bilmelerini sağlamalıdır.

Bu çalışmada Paysim'den alınan veritabanları kullanarak, makine öğrenmesi algoritmalar ile testler yapılmıştır. Deneylerde ilk olarak sekiz adet veritabanından Rastgele orman algoritması ve PART tipi algoritma ile en iyi performansı veren veritabanı belirlendi. Daha sonra Bayes Ağları, Naif Bayes, K-en yakın komşular, K*, Karar tablosu, PART tipi, C4,5 ve Rastgele Ormanı makine öğrenmesi algoritmaları ile sahtekârlık tespiti sınıflandırması gerçekleştirilmiştir. Ancak, sonuçta 3 adet L_PAY bir satıcı ödemesine karşılık gelen işlemleri; L_DEBIT iletişim zamanının alım işlemleri ve L_DEP para yatırma işlemleri doğru sınıflandırılmıştır. Geri kalanı C4.5 ve PART tipi algoritmaları ile L_CASH_O meşru para çekme işlemleri; L_TRF meşru bireyler arasındaki işlemler yanlış sınıflandırılmıştır. C4.5 algoritma %0.85; PART tipi algoritma %0.86 ve Karar tablosu algoritma %0.81 F1 skoru olarak gösterilmiştir. En az meşru işlemi gösteren algoritma, PART tipi karar tablosudur ve en az meşru yanlış sınıflandırılmış işlemi gösteren algoritma karar tablosudur.

Bakış açısı olarak, sınıflandırma algoritmalarının adaptasyonu konusundaki çalışma, daha fazla veri temsili dikkate alınarak tamamlanabilir. Örneğin, standart veriler veya konum gibi ek bilgiler de dikkate alınabilir. Bu çalışma, daha fazla sınıflandırma algoritması veya diğer kategorilerin algoritmaları dikkate alınarak da

yapılabilir. Daha fazla işlem ve aktör içeren veriler kullanılabilir. Ek olarak, kullanıcıların alışkanlıkları zaman içinde değişebilir. İşlemlerin geçici yönü de dikkate alınabilir. Son olarak, bu çalışmada yapılan gözlemlerle karşılaştırmak için temel gerçeğe bağlı gerçek işlemlerin elde edilmesi ilginç olacaktır. Ayrıca, simülatör tarafından oluşturulan veri setleri, algoritmalar ve sahtekarlık algılama araçları üzerinde karşılaştırmalı çalışmalar yapmak için kullanılabilir.

KAYNAKLAR

[1] G. M. money, "State of the Industry Report on Mobile Money," GSMA Association, 2017.

[2] A. Z. Marina Solin, "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks," GSMA DISCUSSION PAPER, January 2010.

[3] G. M. Money, "Le point sur le secteur, Les services d'argent mobile," GSMA, London EC4N 8AF United Kingdom, 2015.

[4] C. S. E. C. WILLIAMSON, "L'argent mobile franchit les frontières : Nouveaux modèles de transferts en Afrique de l'Ouest," GSMA Mobile Money for the Unbanked, London, 2015.

[5] A. H. a. I. Mas, "Seeking Fertile Grounds for Mobile Money," Bill & Melinda Gate, January 2009.

[6] H. T. Renaud Kayanakis, Devenir opérateur mobile sans réseau, Editions d'Organisation, 2006.

[7] P. A. V. Jeroen P.J. de Jong, "Organizing Successful New Service," SCALES-paper, 6 6 2003.

[8] S. Miranda, "Systèmes d'information mobiquitaires la mobiquité. Introduction : de l'utilisateur au nuage," Ingénierie des Systèmes d'Information, vol. 16, 2011.

[9] I. K. Evgenia Novikova, "Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services," IFIP , vol. 16, p. 63–78, 2014.

[10] https://en.oxforddictionaries.com/definition/fraud., Erişim Tarihi: 9.11.2018.

[11] I. T. D. N. P. M. Matti Kurvinen, Warranty Fraud Management: Reducing Fraud and Other Excess Costs in Warranty and Service Operations, Hoboken, New Jersey: Wiley & SAS Business Series , 2016 .

[12] L. G. e. M. Joyce, "La prévention du risque de fraude dans l'argent mobile," GSMA, London , 2013.

[13] European Central Bank, The Payment System, 60311 Frankfurt am Main Germany: tom kokkola, 2010.

[14] R. G. M. A. B. H. M. P. P. U. Chrystel Gaber, "Analyse des comportements dans un système de transfert d'argent sur mobile," in HAL, france, sep 2013.

[15] J.-P. L. P. N. Laurent Condamin, Risk Quantification: Management, Diagnosis and Hedging (The Wiley Finance Series), West Sussex PO19 8SQ, England: Wiley, 2007.

[16] K. Julisch, "Risk-Based Payment Fraud Detection," IBM Research, Switzerland, 2010.

[17] R. G. M. A. B. H. M. P. P. U. Chrystel Gaber, "Analyse des comportements dans un système de transfert d'argent sur mobile," in hal, Mont-de-Marsan, 2013.

[18] T. F. A. F. PROVOST, "Adaptive Fraud Detection," Kluwer Academic, Netherlands, 1997.

[19] S. J. K. T. J. C. W. Siddhartha Bhattacharyya, "Data mining for credit card fraud: A comparative study," Elsevier B.V., p. 50:602–613, 2010.

[20] H. A. J. P. Linda Delamaire, "Credit card fraud and detection techniques," Banks and Bank systems, UK, 2009.

[21] G. Technology, "TEE System Architecture," GlobalPlatform, 2018.

[22] K. P. D. G. W. K. Linck, "Security Issues in Mobile Payment from the Customer Viewpoint," in European Conference on Information Systems, Schweden, 2006.

[23] P. K. S. S. e. R. T. Suresh Chari, "Security issues in m-commerce : A usage-based taxonomy. e-commerce agents," Springer, p. pages 264–282., 2001.

[24] p. preux, Fouille de données, Lille : Université de Lille 3, 2011.

[25] G. P.-S. a. P. S. Usama Fayyad, "From Data Mining to Knowledge Discovery in Databases," AI Magazine, vol. III, no. 17, pp. 5-15, 1996.

[26] E. F. Ian H. Witten, Data Mining: Practical Machine Learning Tools and Techniques, London: Morgan Kaufmann, 2005.

[27] T. Kohonen, "The self-organizing map," IEEE, vol. 78, no. 9, pp. 1464 - 1480, 1990.

[28] S. D. E. O. J. P. e. B. S.-k. Marti A. Hearst, "Support vector machines," Intelligent Systems and their Applications,, vol. 4, no. 13, pp. 18-28, 1998.

[29] J. R. Quinlan, programs for machine learning, San Mateo, Calif. : Morgan Kaufmann Publishers, 1993.

[30] L. Breiman, "Random forests," Berkeley, 2001.

[31] R. Kohavi, "The Power of Decision Tables," in European Conference on Machine Learning (ECML), 1995.

[32] E. F. e. I. H. Witten, "Generating accurate rule sets without global optimization," 1998.

[33] I. M. a. A. Ng'weno, "Three keys to M-PESA's success Branding, channel management and pricing," Bill & Melinda Gates Foundation, 2010.

[34] H. K. ¨. e. E. J. Emilie Lundin, "A synthetic fraud data generation methodology," in Springer, Berlin, 2002.

[35] H. K. E. J. Emilie Lundin Barse, "Synthesizing Test Data for Fraud Detection Systems," in In Computer Security Applications Conference, Las Vegas, 2003.

[36] E. A. L.-R. A. E. e. S. Axelsson, "A FINANCIAL MOBILE MONEY SIMULATOR FOR FRAUD DETECTION," IAAA, 2016.

[37] H. K. e. E. J. E.L. Barse, "Synthesizing test data for fraud detection systems," in In Computer Security Applications Conference, 2003.

[38] S. A. Edgar Alonso Lopez-Rojas, "Multi agent based simulation (mabs) of financial transactions for anti money laundering," in In Nordic Conference on Secure IT Systems. Blekinge Institute of Technology, Nordic, 2012.

[39] A. Kokkinaki, "On atypical database transactions : identification of probable frauds using machine learning for user profiling," IEEE, no. 97, p. 107–113, 1997.

[40] R. M. J.-P. B. I. BERGERI, "Pour Tout Savoir Ou Presque Sur Le Coefficient Kappa," Med Trop, no. 62, pp. 634-636, 2002.

[41] C. J., A coefficient of agreement for nominal scales, Educ. Psychol. Meas, 1996.

[42] J. R. L. e. G. G. Koch, The measurement of observer agreement for categorical data, biometrics, 1977.

[43] H. A. e. L. J. Williams, "Principal component analysis," Wiley Interdisciplinary Reviews, no. 4, p. 433–459, 2010.

ÖZGEÇMİŞ

Mayata NDIAYE, 15.04.1988'de Senegal'de doğdu. İlk, orta ve lise eğitimini Mbacke'de tamamladı. 2009 yılında Louis Baudin Lisesi'nden mezun oldu. 2010 yılında başladığı SUP'INFO Üniversitesi Bilgisayar Mühendisliği Bölümü'nü 2014 yılında bitirdi. 2016 yılında Sakarya Üniversitesi Bilgisayar ve Bilişim Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı ve halen devam etmekteyim.