T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BANKACILIK İŞLEMLERİNDE KONUM DESTEKLİ SAHTEKÂRLIK ÖNLEME SİSTEMİ

DOKTORA TEZİ

Betül EKİZOĞLU

Enstitü Anabilim Dalı	**:**	**ENDÜSTRİ MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. Ayhan DEMİRİZ**

Aralık 2016

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BANKACILIK İŞLEMLERİNDE KONUM DESTEKLİ SAHTEKÂRLIK ÖNLEME SİSTEMİ

DOKTORA TEZİ

Betül EKİZOĞLU

Enstitü Anabilim Dalı : ENDÜSTRİ MÜHENDİSLİĞİ

Bu tez 27/12/2016 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

Prof. Dr. **Orhan TORKUL** **Jüri Başkanı**	**Prof. Dr.** **Ayhan DEMİRİZ** **Üye**	**Prof. Dr.** **Cabir VURAL** **Üye**
Doç. Dr. **Bayram TOPAL** **Üye**	**Yrd. Doç. Dr.** **Seçkin ARI** **Üye**	

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Betül EKİZOĞLU

29.11.2016

ÖNSÖZ

Çalışmamın en başından en sonuna kadar tüm aşamalarında beni yönlendiren ve bana destek olan değerli tez danışmanım Prof. Dr. Ayhan Demiriz'e; yardımsever, anlayışlı, sabırlı, özverili ve samimi tutumlarından dolayı en içten saygı ve teşekkürlerimi sunarım. Lisans öğrenimim boyunca değerli tavsiyeleri ve verdikleri eğitim ile akademik gelişimim konusunda beni yüreklendiren ve üzerimde büyük emeği olan Öğr. Gör. Dr. Mustafa Dördüncü'ye ve Doç. Dr. Lale Özbakır'a; yüksek lisans öğrenimim boyunca yönlendirmeleri ile ufkumu genişleten Prof. Dr. Ahmet Fahri Özok ile Prof. Dr. Cengiz Güngör'e teşekkür ederim. Öte yandan doktora tez izleme jürisinde yer alan ve değerli görüşleri ile tezin gelişmesine katkı sağlayan Prof. Dr. Cabir Vural ile Doç. Dr. Bayram Topal'a teşekkürlerimi sunarım.

Öğrencilik yaşamım boyunca bana her konuda destek olan Erciyes, İstanbul Teknik ve Sakarya Üniversitesi Endüstri Mühendisliği bölümünde aynı sıraları paylaştığım değerli arkadaşlarıma teşekkür ederim. Ayrıca doktora çalışmaları boyunca maddi destek sağlayan TÜBİTAK Bilim İnsanı Destekleme Daire Başkanlığı'na (BİDEB), bu tez çalışmasının maddi açıdan desteklenmesine olanak sağlayan T.C. Bilim, Sanayi ve Teknoloji Bakanlığı San-Tez programına ve Sakarya Üniversitesi Bilimsel Araştırma Projeleri (BAP) Komisyon Başkanlığı'na (Proje No: 2014-01-02-002) teşekkür ederim.

Hayatımın her anında yanımda olduklarını hissettiren, sevgileriyle her zaman güç, güven ve iyimserlik kaynağı olan anne ve babama, biricik kardeşlerim Yasin ve Burak ile neşe kaynağım Ömer'e, hayat arkadaşım eşim Mehmet Fatih Bulut'a, İstanbul'daki kardeşim Ömer Faruk Baykal'a ve tüm dostlarıma yürekten teşekkür eder, sevgilerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

ACFE	: The Association of Certified Fraud Examiners
ATM	: Automated Teller Machines
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BKM	: Bankalar Arası Kart Merkezi
CIO	: Chef Information Officer
d	: Ardıl işlemler arası uzaklık (kilometre)
dak	: Dakika
e	: Entropi
EAST	: European ATM Security Team
FIS	: Fuzzy inference system
FFML	: Financial Fraud Management Language
EMV	: Europay, MasterCard, Visa
FBI	: Federal Bureau of Investigation
IVR	: Interactive voice response
KKB	: Kredi Kayıt Bürosu
km	: Kilometre
MASAK	: Mali Suçları Araştırma Kurulu
NFA	: National Fraud Authority
SEPA	: Single Euro Payments Area
t	: Ardıl işlemler arası geçen süre (dakika)
TBB	: Türkiye Bankalar Birliği
s	: Ardıl işlemler arası geçiş hızı (kilometre/dakika)
XML	: Extensible Markup Language

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Sahtekârlık (fraud) işlemleri, veri madenciliği, coğrafi bilgi sistemleri, lokasyon zekâsı

Sahtekârlık (fraud) işlemlerinin tespiti ulusal ve uluslararası ekonomiler için oldukça önemli bir görev haline gelmiştir. Bankalar ve diğer finansal kuruluşların gerçekleştirdikleri işlemlerin güvenilirliğini sağlaması başta ülke ekonomisi olmak üzere, finansal kuruluşun da itibar ve kârlılığını etkileyen temel faktörlerden birisidir. Sahtekârlık işlemlerinin tespit edilebilmesi ve önlenmesi amacıyla kamu ve özel finans kuruluşlarında bu kontrolleri yapmaktan sorumlu birimler oluşturulmuştur. Ancak sahtekârlık işlemlerini gerçekleştirmeye çalışan kişilerin, yakalanmamak amacıyla sürekli yöntem değiştirmeleri, bu tip işlemlerin tespit edilmesini zorlaştırmaktadır. Bu işlemlerin tespiti, işlem hacimlerinin yoğunluğu da dikkate alındığında teknoloji desteğini zorunlu kılmaktadır.

Sahtekârlık işlemlerinin tespiti için geliştirilmiş uygulamalar içerisinde özellikle kural tabanlı sistemlerin yaygınlığı dikkate değerdir. Bu sistemler; basit ve bileşik kurallar kullanan, doğrulanmış sahtekârlık veritabanları ve diğer önemli veri setlerinde karşılaştırma yapan ileri teknoloji veri eşleme sistemleri olabileceği gibi; şüpheli davranışları tespit edebilen ve bu bilgiyi doğru kanala yönlendiren veritabanları gibi basit sistemler de olabilmektedir. Bununla birlikte, sahtekârlık işlemlerinin tespitinde işlem konumlarının (lokasyonlarının) dikkate alınması üzerine geliştirilmiş bir modele rastlanmamıştır. Bu tez çalışmasında hedeflenen; bankacılık ürün ve hizmetlerine yönelik sahtekârlık işlemlerinin tespiti ve önlenmesi için finansal işlemlerin konum bilgisinin kullanılması ile daha iyi sonuçlar elde edilip edilemeyeceğinin incelenmesidir. Çalışma kapsamında coğrafi bilgi sistemlerinin yardımıyla ve veri madenciliği modelleri kullanılarak, konum ve zaman bilgisinin dahil edildiği senaryolar keşfedilmiştir.

LOCATION-AIDED FRAUD DETECTION IN BANKING OPERATIONS

SUMMARY

Keywords: Fraudulent Transactions, Data Mining, Geographical Information Systems, Location Intelligence

Fraud detection procedures for national and international economies have become quite important tasks. Ensuring the security of transactions carried out by banks and other financial institutions is one of the major factors affecting the reputation and profitability of such organizations. Public and private financial institutions establish organizational bodies responsible for carrying out controls for detecting and preventing fraudulent transactions. However, since people who perform fradulent transactions change their methods constantly in order not to get caught up, it gets more difficult to identify and detect this type of transactions. Detecting this type of transactions makes the support of technology compulsory, considering high volume and intensity of transactions.

Among the applications that has been developed for the detection of fraudulent transactions, the prevalence of the rule-based systems are particularly noteworthy. As these systems may use of simple and compound rules, advanced data mapping technologies that make comparison in validated fraud databases, and other important databases mapping systems, they may be simple database systems that can detect suspicious behavior and directs this information to the right. However, we have not come across any model that takes into account of transaction location. The aim of this thesis study is to study the worth of location information of financial transactions for detecting the fraudulent transactions. The scope of work is to discover scenarios to detect fraudulent transactions by the support of geographic information systems with location, and time information and the help of models built by using data mining.

BÖLÜM 1. GİRİŞ

1.1. Genel Bilgi ve Tarihçe

Bankacılıkta sahtekârlık riskleri banka yöneticilerinin, çalışanlarının, müşterilerinin veya üçüncü kişilerin iyi niyet kurallarına aykırı olarak suistimal, hile, dolandırıcılık gibi yöntemlerle bankaları ve müşterilerini zarara uğratmalarından kaynaklanan operasyonel risk türüdür. Günümüzde bankaların değişik alanlarda faaliyetlerini yoğunlaştırması ve elektronik bankacılık uygulamalarının yaygınlaşması, sahtekârlık risklerinin gerçekleşme olasılığını artırmıştır [1].

Bankacılık sektöründe parasal aktif ve pasiflerin bilanço içindeki payları yüksek olduğundan, diğer iş kollarına göre; bankaların aktiflerini, hizmet kanallarını ve müşterilerinin varlıklarını hedef alan finansal dolandırıcılık ve para aklama gibi suç girişimleri ve bunların sonucunda karşılaşılan kayıplar çok daha yüksek olabilmektedir [2]. Sahtekârlık, dolandırıcılık, kalpazanlık, hırsızlık, zimmet, para aklama olayları, bilgi işlem sistemleri ve elektronik bankacılık platformuna izinsiz girişler, çıkar çatışmaları, yasal yetki sınırlarının ve yükümlülüklerin ihlal edilmesi gibi operasyonel riskler; bankaların programlarındaki uygulama zayıflıklarından, etkin olmayan kontrol yöntemlerinden ve müşteri inceleme uygulamalarındaki başarısızlıktan kaynaklanmakta; bu durum diğer riskleri tetikleyebilmekte ve büyük miktarda kayıpların ortaya çıkmasına neden olabilmektedir [2].

Bankaların sektörde varlıklarını devam ettirebilmeleri, müşterileri için "güvenilir" algısını korumalarına bağlıdır. Herhangi bir sahtekârlık olayının yaşandığı bir banka olmak sektörde ciddi itibar ve müşteri kaybına yol açacaktır. Bu nedenle bankalar için etkin ve zamanında yapılacak işlem kontrolleri ile sahtekârlık işlemlerinin önlenmesi hayati önem taşımaktadır. Bankalar aracılığıyla yurt dışı para transferleri de yapıldığı

dikkate alındığında, yaşanacak bir kaybın ülke ekonomisi ve itibarı üzerinde de önemli olumsuz etkileri olacağı açıktır.

1.2. Kapsam ve Amaçlar

Yol açtığı finansal kayıplar ve itibar kayıpları ile sürekli değişen yapısı nedeniyle finansal sahtekârlıkların önlenmesi önemli bir araştırma konusudur. Bir önceki bölümde bahsedildiği gibi finansal sahtekârlık riskleri, bankacılık için yönetilmesi gereken önemli operasyonel riskler arasındadır. Bu tez çalışması kapsamında bankalar aracı kılınarak gerçekleştirilen sahtekârlık işlemlerinin önlenmesi ve tespit edilmesine katkı sağlayacak, bankacılık işlemlerinin konum bilgilerinin dikkate alındığı analitik bir model önerilecektir.

Yapılan literatür araştırmalarında finansal sahtekârlıkların birçok farklı sektörde ve bankacılık sektörü içerisinde de birçok farklı işlem tipi için ve farklı yöntemler kullanılarak gerçekleştirildiği görülmüştür. Bankalar ve diğer finansal kuruluşlar için sahtekârlık işlemlerinin yönetimi konusunda yapılan çalışmalar temelde ikiye ayrılabilir: 1) Sahtekârlık işlemlerinin henüz gerçekleşmeden belirlenerek önlenmesi ve 2) İşlemler gerçekleştikten sonra keşfedici analizler ile tespit edilmesi. Bankalardaki işlem hacimlerinin yoğunluğu, sahtekârlık işlemlerinin önlenmesi ve tespit edilmesi için yapılacak çalışmalarda veri madenciliği ve yapay öğrenme tekniklerinin kullanımını zorunlu kılmaktadır. Kredi kartları ile ve internet bankacılığı üzerinden gerçekleştirilen bankacılık işlemlerinde yapılan sahtekârlıkların tespiti için birçok çalışmanın yapılmış olduğu görülmektedir. Bu tez çalışmasında diğer çalışmalardan farklı olarak bankalar aracı kılınarak yapılan sahtekârlık işlemlerinin tespitinde işlem kanalı ve işlem tipi ayrımı olmaksızın bütüncül bir yaklaşımın sergilenmesi hedeflenmiştir. Bu tez çalışmasında temel olarak hedeflenen, bankacılıkta gerçekleştirilen sahtekârlık işlemlerinin tespit edilmesi için yapılan veri analizlerine işlemlerin "konum" bilgilerinin de dahil edilmesini sağlayacak bir analitik model geliştirilmesi ve sahtekârlıkların tespitinde konum bilgisinin anlamlı bir etkisinin olup olmadığının ölçülmesidir. Bu hedefe ulaşmak için aşağıda listelenen işlem adımları gerçekleştirilmiştir:

- Önerilen modelin geliştirilmesi ve test edilmesi için kullanılacak veri setinde yer alacak değişkenlerin tanımlanması,
- Türkiye'de faaliyet gösteren bir bankadan, müşteri hesaplarından yapılan bankacılık işlemlerini ve gerekli değişkenleri içeren gerçek veri kümesinin temin edilmesi,
- Sahtekârlık işlemlerinin tespitinde kullanılan, başarılı veri madenciliği tekniklerinin belirlenmesi,
- Sahtekârlık işlemlerinin tespitinde konum bilgisinin kullanılabilirliğinin analiz edilmesi,
- Konum bilgisi kullanılarak geliştirilmiş veri madenciliği tekniklerinin ve konum bilgisinin kullanım alanlarının belirlenmesi,
- Sahtekârlık işlemlerinin tespiti için konum bilgisinin dikkate alındığı yeni bir model kurulması,
- Kurulan model aracılığıyla sahtekârlık işlemlerinin tespit edilmesini sağlayacak dinamik iş kurallarının elde edilmesi,
- Kurulan modelin bulanık mantık ile yeniden modellenmesi, uzman bilgisinden yararlanılarak bulanık kuralların elde edilmesi,
- Mevcut iş kuralları, önerilen model ve önerilen modelin bulanık mantık ile çalıştırılması sonucu keşfedilen iş kuralları için performans karşılaştırması yapılması.

1.3. Çalışma Methodolojisi ve Çalışmanın Bilime Katkısı

Tez çalışması için izlenen yöntem aşağıdaki gibidir:

- İlk olarak çalışmada önerilen modelin kurulması ve test edilmesi için kullanılacak veri kaynakları ve bankacılık veri tabanı incelenerek gerekli analizler yapıldı.
- Konum destekli analizler yapılabilmesi için bankacılık veri tabanında mevcutta yer almayan konum bilgisinin işlemlerle ilişkili olarak veri tabanına eklenmesi sağlandı.

- Özellikle bankacılık sahtekârlıklarının tespit edilmesi ile ilgili literatürde yer alan çalışmalar araştırıldı, modelin kurulması ve test edilmesi çalışmaları için anlamlı olacak değişkenler tespit edildi.
- Farklı bankacılık kanallarından yapılan, farklı tiplerdeki işlemler için ortak bir değişken kümesi oluşturuldu; bankacılık veri tabanında dağıtık bir şekilde tutulan, müşteri hesaplarından tüm kanallardan yapılan ve tüm finansal işlemleri içeren, Kasım 2012 - Kasım 2014 dönemine ait veri kümesi oluşturuldu. Kredi kartı ve poslardan yapılan işlemler, çalışma kapsamı dışında bırakılmış ve veri kümesine dahil edilmemiştir. Veri kümesinde yer alan tüm işlemlerin sahtekârlık olmayan yani güvenli kabul edilen işlemler olduğu varsayılmıştır.
- Veri kümesinin uç değerlerden arındırılması için veri temizliği ve veri bütünlüğünü sağlayacak çalışmalar yapıldı.
- Bankacılık sahtekârlıklarının tespit edilmesi ve önlenmesi için yapılmış literatürdeki çalışmalar incelendi. Özellikle veri madenciliği tekniklerinin uygulandığı çalışmalar üzerinde duruldu.
- Konum bilgisinin dahil edildiği, coğrafi bilgi sistemlerinden faydalanılarak yapılan veri madenciliği uygulamaları incelenerek, sahtekârlık işlemlerinin tespitinde konum bilgisinin anlamlı sonuçlar üretebilecek şekilde kullanımı üzerine araştırmalar yapıldı.
- Müşteri hesaplarından yapılan sahtekârlık işlemlerinin tespit edilmesine yardımcı olması amacıyla, bankacılık işlemlerinin yapıldığı konum bilgisinin de dikkate alındığı bir model geliştirildi.
- Problemin çözümünde daha iyi sonuçlar verebileceği düşünülen bulanık mantık yaklaşımı uygulandı ve uzman bilgisinden faydalanılarak bulanık üyelik kuralları belirlendi.
- Konum bilgisinin dahil edildiği modelin ve bulanık mantık modelinin sonuçlarına bağlı olarak sahtekârlık tespiti için yeni, dinamik iş kuralları elde edildi.
- Bankadan elde edilmiş gerçek veri seti üzerinde hâlihazırda bankada uygulanmakta olan iş kuralları ve geliştirilen modeller ile elde edilen dinamik kurallar çalıştırılarak şüpheli işlemler tespit edildi. Mevcut durumun, klasik

yöntemle uygulanan modelin ve bulanık mantıkla uygulanan modelin performansları karşılaştırıldı.

- Yapılan çalışmalar neticesinde literatüre yeni bir yayın kazandırıldı [3].

1.4. İçerik

Bu çalışma toplamda yedi bölümden oluşmaktadır. Bölüm 2'de sahtekârlık işlemleriyle mücadelede problemin tanımı ve temel kavramlar; Bölüm 3'de sahtekârlık işlemlerinin tespiti için kullanılan teknikler; Bölüm 4'de sahtekârlık işlemlerinin tespiti için önerilen, işlemlerin konum bilgisinin dikkate alındığı modelin temelleri; Bölüm 5'de önerilen modelin banka veri seti üzerindeki uygulama çalışmaları; Bölüm 6'da önerilen modelin bulanık mantık ile uygulama sonuçları; Bölüm 7'de tüm çalışmalardan elde edilen sonuçların değerlendirmesi sunulacaktır.

BÖLÜM 2. PROBLEMİN TANIMI VE LİTERATÜR TARAMASI

Tez çalışmasında sıklıkla karşılaşılan finansal sahtekârlık terimi, İngilizce'deki "fraud" kelimesinin Türkçe karşılığı olarak kullanılmıştır. Fraud kelimesi Türkçe'de kullanılan yolsuzluk, dolandırıcılık, usulsüzlük, rüşvet, hile ve buna benzer birçok kelimeyi içine alan bir kavram olduğu için; bunların tamamını kapsayacak finansal sahtekârlık teriminin kullanılması tercih edilmiştir. Uluslararası Susitimal İnceleme Uzmanları Derneği (The Association of Certified Fraud Examiners (ACFE) Türkiye), fraud kelimesinin karşılığı olarak suistimal kelimesini kullanmaktadır [4]. Bu bölümde öncelikle finansal sahtekârlık tanımı yapılacak ve çeşitleri incelenecek, sahtekârlık faaliyetlerinin önlenmesi için izlenen yöntemler ile karşılaşılan zorluklardan bahsedilecektir.

2.1. Finansal Sahtekârlık Tanımı ve Çeşitleri

Finansal sahtekârlık için uluslararası arenada kabul görmüş genel bir tanım olmamasına rağmen The Association of Certified Fraud Examiners (ACFE) fraud kavramını, "kişinin işveren kuruluşa ait varlıkları kasti olarak kötüye kullanması ya da zimmetine geçirmesi yoluyla kişisel zenginliğe ulaşmak için mesleğini kullanması" olarak tanımlamaktadır [5]. Bu tanımın daha çok çalışanların kendi kurumlarına karşı gerçekleştirdiği sahtekârlık faaliyetlerine işaret ettiğine dikkat edilmelidir. Daha genel bir tanım üzerinden gitmek gerekirse Oxford İngilizce sözlükteki fraud kelimesinin anlamına bakılabilir. Buna göre fraud: "finansal veya şahsi kazanç elde etmek amacıyla haksız veya kanuna aykırı olarak gerçekleştirilen sahtekârlık" şeklinde tanımlanmıştır [6].

Fraud kavramının sahtekârlık işlemleri için genel bir kavram olarak kullanıldığı açıktır. Bununla birlikte, içeriği temelde aynı kalsa da birçok açıdan farklılık

gösterebilmektedir. Tablo 2.1.'de Federal Bureau of Investigation (FBI) tarafından finansal sahtekârlık için yapılan sınıflandırma sunulmuştur. Tabloya göre finansal sahtekârlık sınıflandırması iki seviyede yapılmıştır: birinci seviye sahtekârlık kategorilerini, ikinci seviye ise bu kategorilerde yapılan aktiviteleri içermektedir.

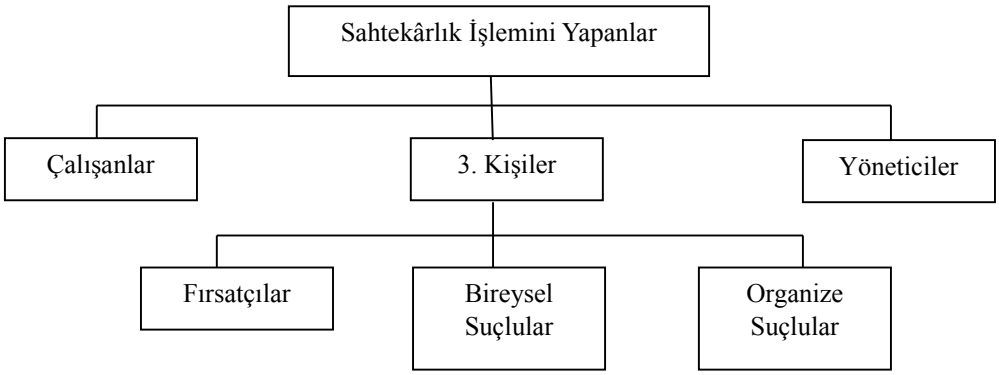
Tablo 2.1. FBI'a göre finansal sahtekârlık sınıflandırması [7]

Finansal Sahtekârlık Kategorileri	**Sahtekârlık Aktiviteleri**
Banka sahtekârlıkları	Mortgage sahtekârlıkları, kara para aklama, ...
Sigorta sahtekârlıkları	Sağlık sahtekârlıkları, sigorta sahtekârlıkları
Teminat ve emtia sahtekârlıkları	Teminat ve emtia sahtekârlıkları
Diğer finansal sahtekârlıklar	Kurumsal sahtekârlıklar, toplu pazarlama sahtekârlıkları

FBI'ın yaptığı sınıflandırmaya ek olarak sahtekârlık faaliyetleri bu faaliyetleri gerçekleştiren kişilere, faaliyetlere aracı kılınan kurumların sektörlerine veya faaliyetlerin yapılma şekline göre farklı başlıklar altında incelenebilir.

2.1.1. Sahtekârlık işlemini yapanlara göre sınıflandırma

Sahtekârlık faaliyetleri, bu faaliyetleri gerçekleştiren kişilerin aracı kılınan kuruma yakınlıklarına göre sınıflandırılabilir. Sahtekârlık faaliyetini gerçekleştiren kişiler bizzat o kurumun kendi çalışanları olabileceği gibi kurumu veya müşterilerini hedef alan üçüncü kişiler de olabilir. Müşteriler, tedarikçiler, üst düzey yöneticiler veya yatırımcılar sahtekârlık faaliyetinin öznesi olabilirler [8]. Aşağıdaki şekilde sahtekârlık işlemini yapan kişilere dair bir sınıflandırma gösterilmektedir.



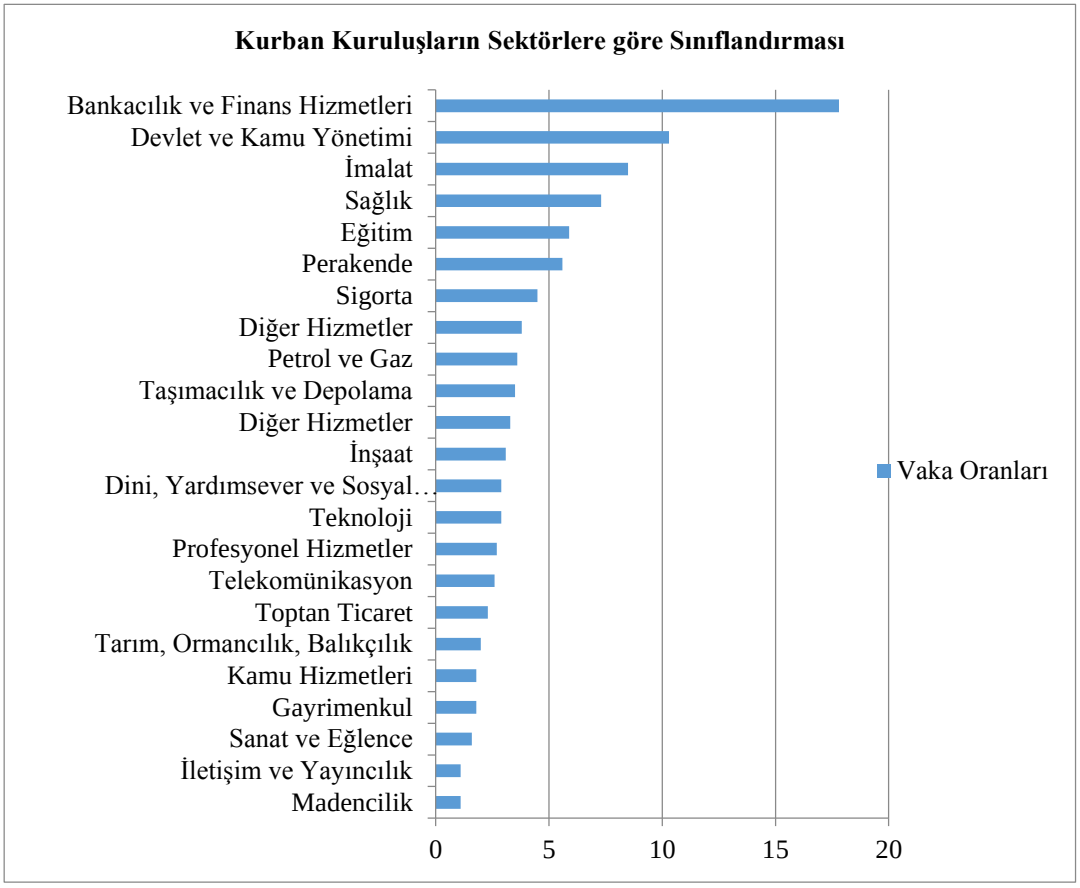
Şekil 2.1. Kurum içi ve kurum dışından sahtekârlık yapan kişilere dair hiyerarşi şeması [8]

Sahtekârlık faaliyetini gerçekleştiren kişilere göre saldırıların gerçekleşme şekli de değişeceği için alınacak önlemler de farklılaşmaktadır. Üst düzey yöneticiler şirketin gelir-gider göstergelerini, satış rakamlarını, faturalarını veya vergi ile ilgili evraklarını tahrif eden faaliyetlerde bulunabilecekken; bir müşterinin yapacağı sahtekârlık, ödememe niyetiyle borçlanmak, yanlış bilgi beyan etmek şeklinde olabilir [10]. Bununla birlikte aracı kılınan kuruma ve müşterilerine karşı ataklar gerçekleştiren bireyler veya çeteler, çeşitli yöntemlerle kurumların bilgi sistemlerine sızarak veya müşteri bilgilerini ele geçirerek haksız kazanç elde etmeye çalışmaktadırlar. Şekil 2.1.'de verilen şemada yer alan fırsatçılar, finansal bir zorlukla karşılaştıklarında veya bir fırsat gördüklerinde harekete geçen ve sürekli olarak bu işi yapmayan kişilerdir. Daha riskli olan kişiler ise bireysel veya organize olarak sürekli bir şekilde bu faaliyetleri gerçekleştiren kişilerdir [9]. Fırsatçılar toplamda daha çok ve göreceli olarak organize suç grupları daha az sayıda atak gerçekleştirse de bu atakların sebep olduğu maddi kayıplar açısından bireysel ve organize suç gruplarının ataklarının çok daha tehlikeli olduğu belirlenmiştir [11].

2.1.2. Sahtekârlık işlemi için aracı kılınan kuruma göre sınıflandırma

Sahtekârlık kavramı oldukça geniş bir kavram olduğu için iş dünyasındaki hemen hemen her sektörde bir türevine rastlamak mümkündür. Bununla birlikte, literatür taraması yapıldığında çalışmaların belli başlı sektörler için yoğunlaştığı görülmektedir. Sahtekârlık faaliyetlerinin yoğun, sebep olduğu kayıpların yüksek tutarda, sahtekârlık faaliyetlerine karşı kırılganlığın fazla veya çalışma yapılabilmesi

için gerekli olan veri ve diğer bileşenlerin ulaşılabilir olduğu sektörler daha çok çalışmanın yapıldığı sektörler olarak da yorumlanabilir. Şekil 2.2.'de ACFE tarafından 2014 yılı için yayınlanmış uluslararası raporda sunulan grafiğe yer verilmiştir. Bu grafik, yapılan araştırmaya katılan 1438 adet sahtekârlık faaliyetinden etkilendiği bilinen organizasyonun sektörlerine göre sınıflandırılmasıyla oluşmuştur. Grafikten görüleceği gibi sahtekârlık faaliyetlerinin en çok görüldüğü sektörler, bankacılık ve finans, kamu yönetimi, üretim ve sağlık sektörleridir.



Şekil 2.2. Kurban kuruluşların sektörlerine göre sınıflandırması [5]

Literatürdeki çalışmalar incelendiğinde yoğun olarak bankacılık ve finansal işlemler, telekom ve sigortacılık sahtekârlıkları üzerinde çalışmalar yapıldığı görülmektedir. Bu tez çalışmasının konusu ve uygulama alanı da bankacılık sahtekârlıklarıdır.

Yufeng Kou, sahtekârlık işlemlerinin tespiti için uygulanan yöntemleri incelediği çalışmasında, sahtekârlık işlemlerini sınıflandırmış ve bu işlemlerle mücadele etmek

için kullanılan teknikleri incelemiştir [12]. Kou'nun yaptığı sınıflandırmada kredi kartı sahtekârlıkları, bilgi ağlarına sızma sahtekârlıkları ve telekom sahtekârlıkları yer almıştır. Michael H. Cahill, telekom sahtekârlıklarının tespitini samanlıkta iğne aramaya benzettiği çalışmasında, sahtekârlıklarla mücadele için bir model önermiş ve model için performans kriterleri tanımlamıştır [13]. Fawcett ve Provost ise telekom sahtekârlıklarının tespiti için kendi kendine öğrenen sistemler önermişlerdir [14]. Telekom sahtekârlıklarının modellenmesinde kullanılan veri kümesinin bireysel konuşma bilgilerinden (tarih/zaman bilgisi, arayan numara, aranan numara, konuşma süresi, arayan ve aranan numaraların konum bilgisi) ve hesap özet bilgilerinden (ödeme yöntemleri, aylık ortalama fatura bilgisi, konuşmalar arası ortalama süre, günlük ve haftalık konuşma özetleri) oluştuğu görülmektedir [9]. Birleşik Krallığa bağlı Ulusal Sahtekârlık Otoritesi'nin (National Fraud Authority, NFA) 2013 yılına ilişkin raporuna göre telekom sahtekârlıklarının Birleşik Krallık için yıllık 953 milyon İngiliz sterlini tutarında olduğu tahmin edilmektedir [15].

Sigortacılık sahtekârlıkları sigorta sürecinin pek çok farklı aşamasında görülebilir: (başvuru, uygunluk, derecelendirme, faturalandırma ve hak iddiaları gibi) ve müşteriler, sigorta acentaları, aracılar, sigorta şirketi çalışanları, sağlık hizmeti verenler gibi pekçok farklı kişi tarafından gerçekleştirilebilir [16]. Phua'nın yaptığı sınıflandırmaya göre sigortacılık sahtekârlıkları konut sigortaları, tarım sigortaları, otomobil sigortaları ve sağlık sigortaları olmak üzere dört temel başlıkta incelenebilecektir [9]. Birleşik Krallık'ta tüm sigortacılık sahtekârlıklarıyla mücadele etmek için 2006 yılında kâr amacı gütmeyen bir şirket olarak Sigortacılık Sahtekârlık Bürosu kurulmuştur [17].

Tez çalışmasının konusu olan bankacılık sahtekârlıkları ilerleyen bölümlerde daha detaylı bir şekilde anlatılacaktır. Bununla birlikte NFA tarafından 2013 yılına ilişkin yayınlanan rapora göre bankacılık ve sigortacılık sahtekârlıklarının Birleşik Krallık için tutar olarak dağılımını gösteren grafik Şekil 2.3.'de gösterilmiştir.

Kurban	Toplam sahtekârlık kayıpları	Sahtekârlık tipi	Sahtekârlık kayıpları	Tespit edilmiş kayıplar	Gizli kayıplar
		Sigorta sahtekârlığı	£2,1 milyar	£39 milyon	£2,1 milyar
		Mortgage sahtekârlığı	£1 milyar	£1 milyar	
		Plastik kart sahtekârlığı	£388 milyon	£388 milyon	Bilinmiyor
Finans ve sigortacılık hizmetleri	£5,4 milyar	Elektronik bankacılık sahtekârlığı	£40 milyon	£40 milyon	Bilinmiyor
		Çek sahtekârlığı	£35 milyon	£35 milyon	Bilinmiyor
		Telefon bankacılığı sahtekârlığı	£13 milyon	£13 milyon	Bilinmiyor
		Tahmin edilen diğer sahtekârlık	£1,8 milyar	Bilinmiyor	£1,8 milyar

Şekil 2.3. Sahtekârlık tiplerine göre yaşanan kayıpların tutarı [15]

2.2. Bankacılık Sahtekârlıkları

Bankacılıkta sahtekârlık işlemlerinin tespit edilmesi ve önlenebilmesi kritik bir görevdir. Bankalar gerek müşteri mağduriyetine izin vermemek ve müşterileri nezdindeki güvenilir algılarını korumak için gerekse de kamu kuruluşları tarafından birçok düzenlemeye uyma zorunlulukları nedeniyle sahtekârlık işlemlerinin tespit edilmesi ve önlenmesi konusunda oldukça hassastır. Bununla birlikte, internet şube, mobil şube ve çağrı merkezleri gibi farklı kanallar üzerinden yapılan bankacılık uygulamalarının hızla yaygınlaşması ile bankacılık; herkese açık, isimsiz, çok çeşitli, coğrafi kısıtlaması olmayan ve dijital bir işlev haline gelmiştir [11]. Bu ise hızla gelişen ve sürekli yeni ürünler geliştirip, farklı kanallardan müşterilerine hizmet sunmaya çalışan Türk bankacılık sistemini suistimallere açık hale getirmektedir.

Bankaların ürün çeşitliliğine bağlı olarak karşılaştıkları sahtekârlık işlemlerinin çeşitleri, yapıları ve önlenmeleri için alınması gereken önlemler de farklılaşmaktadır. Şekil 2.4.'de ACFE'nin 2014 raporunda yer alan bankacılık sahtekârlık çeşitleri ve toplam içindeki oranlarını gösteren grafiğe yer verilmiştir.

Sektör/Şema	Bankacılık ve Finansal Hizmetler	Devlet ve Kamu Yönetimi	İmalat	Sağlık	Eğitim	Perakende	Sigorta	Petrol ve Gaz	Taşımacılık ve Depolama	Diğer Hizmetler	İnşaat	Dinsel, Hayır ve Sosyal Hizmetleri
Vaka Sayısı	244	141	116	100	80	77	62	49	48	45	43	40
Faturalama	5.7 %	19.1%	22.4%	29 %	33.8%	10.4	17.7%	24.5%	33.3%	28.9%	34.9%	32.5%
Nakit Hırsızlık	13.1%	10.6%	6.0 %	12 %	6.3%	15.6%	6.5%	2.0 %	2.1%	11.1%	14.0%	7.5%
Kasa Bakiyesi	18.9%	12.1%	7.8%	16.0%	16.3%	22.1%	1.6%	2.0%	10.4%	11.1%	7.0%	12.5%
Çek Sahtekârlığı	5.7%	5.7%	7.8%	21.0%	10.0%	7.8%	4.8%	4.1%	20.8%	17.8%	27.9%	35.0%
Rüşvet	37.3%	36.2%	54.3%	37.0%	36.3%	22.1%	33.9%	57.1%	29.2%	35.6%	46.5%	30.0%
Masrafların Geri Ödenmesi	4.1%	12.8%	7.8%	23.0%	31.3%	3.9%	4.8%	14.3%	14.6%	17.8%	27.9%	32.5%
Finansal Rapor Sahtekârlığı	10.2%	5.0%	13.8%	8.0%	10.0%	6.5%	3.2%	12.2%	10.4%	6.7%	11.6%	7.5%
Gayri Nakdi	13.1%	17.7%	34.5%	12.0%	12.5%	33.8%	12.9%	16.3%	33.3%	17.8%	20.9%	15.0%
Maaş Bordrosu	5.3%	15.6%	8.6%	15.0%	16.3%	5.2%	8.1%	6.1%	16.7%	6.7%	18.6%	20.0%
Kayıtlı Avanslar	2.5%	0.7%	2.6%	3.0%	5.0%	13.0%	0.0%	0.0%	4.2%	6.7%	2.3%	2.5%
İzinsiz Kopyalama	5.7%	11.3%	4.3%	18.0%	20.0%	18.2%	22.6%	2.0%	6.3%	33.3%	7.0%	12.5%

Düşük Risk — Yüksek Risk

Şekil 2.4. Bankacılık sahtekârlıkları çeşitleri ve dağılımı [5]

Daha önce yapılmış çalışmalar incelendiğinde bankacılıkta sahtekârlık işlemlerinin tespiti için yapılan çalışmaların çoğunlukla kredi kartı işlemlerine yoğunlaştığı görülmektedir. Bununla birlikte ATM'den (Automated Teller Machines) yapılan işlemler ve internet bankacılığından yapılan işlemler de sahtekârlık araştırmalarının konusu olmuştur [19, 20, 21, 22]. Ancak bankacılık işlemleri bütüncül olarak ele alındığında bunların her biri sadece işlemlerin yapıldığı birer kanal olarak yerini almaktadır. Sahtekârlık işlemi gerçekleştirecek kişilerin ise hiçbir zaman tek bir kanaldan işlem yapmadığı, aksine farklı kanalları kullanarak farklı işlem kombinasyonları ile kendi başarılarını artırmaya çalıştıkları bilinen bir gerçektir. Edge ve Sampaio yaptıkları çalışmada sahtekârlık işlemleri için yönetim aracı geliştirmenin önemi üzerinde durmuş ve kanal kısıtı olmaksızın çalışacak, kural tabanlı bir sahtekârlık tespit aracı önermişlerdir [23]. Aşağıda bankacılık sahtekârlık işlemlerinden bazı temel olanları hakkında bilgi verilecektir.

2.2.1. ATM sahtekârlıkları

Müşterilere geniş bir finansal hizmet sunan ATM'ler, alternatif dağıtım kanalları içerisinde önemli bir yere sahiptir. ATM'ler aracılığıyla müşteriler banka hesaplarına ulaşıp bakiye sorgulama, nakit yatırma-çekme, fatura ödeme ve kontör yükleme gibi işlemler yapabilmektedir. İlk ATM 1967 yılında kullanılmaya başlandıktan sonra, sahtekârlık işlemlerini yapmak isteyenler ATM'lerin içindeki parayı almak için sürekli yeni yöntemler keşfetmeye çalışmışlardır. Tüketici Bankacılığı Araştırması'na göre, tüm dünyada 2,2 milyon ATM bulunmakta ve bu sayının 2016 yılında 3 milyona ulaşması beklenmektedir [21]. Günümüzde Türkiye'deki ATM'lerin sayısı ise 49 bin civarındadır [24]. ATM sayısı arttıkça güvenlik tehditlerinin sayı ve çeşitlilik olarak artacağı da açıktır.

ATM'lere karşı geliştirilmiş, bilinen güvenlik saldırılarını 4 gruba ayırmak mümkündür:

- Müşterilerin banka kartı bilgilerinin çalınması,
- Bilgisayar ve ağ saldırıları ile müşterilerin kart bilgilerinin çalınması,
- Bilgisayar ve ağ saldırıları ile ATM'lerdeki paranın çalınması [25]
- ATM'lere karşı gerçekleştirilen fiziksel ataklar [21].

ATM'ler hedef alınarak gerçekleştirilen farklı saldırı tipleri olsa da ATM sahtekârlıklarının çoğu iki adımlı bir girişimdir: ilk adımda müşterinin kart bilgileri alınırken, daha sonra ise bu bilgi kullanılır. Müşterinin kart bilgilerini almak için kullanıldığı bilinen ise birçok yöntem mevcuttur:

- ATM'lerin kart okuyucularına veya para çıkış yuvalarına genelde plastik veya ince metal bir bant yerleştirerek kartın müşteriye verilmesinin önlenmesi, ATM kart/para sıkıştırma (card/cash trapping/fishing) [26]
- ATM'ye yerleştirilmiş bir kart okuyucu aracılığıyla kart üzerindeki manyetik alandaki bilgilerin izinsiz kopyalanması (card skimming) [26]
- Oldukça ince plastik bir elektrik devre kartının ATM'ye yerleştirilmesi ile kart bilgilerinin kopyalanması ve kablosuz bir verici ile iletilmesi (shimming) [27]

- İnternet bankacılığında da görülen, müşterinin ATM cihazında yazdığı şifre bilgisini ATM'ye ulaştırmadan sahtekârların arayüzlerine alması (man in the middle attacks) [28]
- Kart şifreleme anahtarlarının tersine mühendislik faaliyetleri ile ele geçirilmesi (reverse engineering) [29]

Avrupa ATM Güvenlik Ekibi'nin (EAST: European ATM Security Team) 2014 yılı için hazırladığı üçüncü Avrupa Sahtekârlık Güncellemesi'nde, Avrupa Tek Ödeme Alanı'ndaki (SEPA: Single Euro Payments Area) 17 ve Avrupa Tek Ödeme Alanı'nda olmayan 2 ülke temsilcisinin verdiği bilgilere göre tüm dünyada ATM saldırılarının sayısının arttığı bildirilmiştir [21]. Bununla birlikte yine Europol ve EAST'in raporlarına göre, Avrupa Birliği'nde bankalar Europay, MasterCard ve Visa (EMV) ortamına geçtikleri için, 2008 yılından beri Avrupa içindeki yasal olmayan işlemler giderek azalmış, fakat Avrupa dışındaki sahtekârlık işlemlerinde belirgin bir artış yaşanmıştır. Bu tip olayların en çok yaşandığı ülkeler arasında Amerika Birleşik Devletleri en üst sırada yer alırken, Endonezya ve Tayland'ın ikinci ve üçüncü sıralarda geldiği belirtilmektedir [30, 22]. EMV uyumlu bir ATM, kart üzerindeki mikro çipler aracılığıyla kartın şifresini kontrol etmekte ve işlemin devam etmesine izin vermekte ya da vermemektedir. Üzerinde çip olmayan kartlar ise bu ATM'lerde kullanılamamaktadır.

2.2.2. Kredi kartı sahtekârlıkları

Yeni ödeme araçları içerisinde en önemlilerden olan kredi kartları günümüzde büyük ölçüde çekin yerini almıştır. İlk kez Amerika Birleşik Devletleri'nde (ABD) 1894 yılında Hotel Credit Letter Company tarafından kullanılan kredi kartı Avrupa'da da hızla gelişme göstermiştir [31]. Mal ve hizmet alımında, kartı veren kurumun belirlediği limit dâhilinde nakit ödemeksizin kredi imkânı sunması en önemli özelliğidir. Kısaca; "kredi kartını veren banka veya kuruluşun açtığı krediye istinaden kart sahibinin gereksinim duyduğu mal veya hizmeti o anda bir ödeme yapmadan satın almasına ve bedelini daha sonra herhangi ek bir mali külfet yüklenmeksizin ödeme

yapmasına imkân veren bir ödeme aracıdır.” [32]. Ancak kredi kartı kullanımının artması bu alanda çeşitli hilelerin de ortaya çıkmasına neden olmuştur.

Kredi kartı sahtekârlıkları pek çok farklı şekilde yapılabilmekle birlikte temel olarak kart bilgilerinin veya bizzat kartın kendisinin yasal olmayan yollarla kullanımı ile gerçekleştirilir. Kart hırsızlığı, sahte kart başvurusu, kopyalanmış kartlar, müşterinin eline ulaşmayan kartlar ve internet üzerinden kartla yapılan sahtekârlıklar temel kredi kartı sahtekârlıklarıdır. Çip ve pin uygulaması kart hırsızlığı, kopyalanmış kartlar ve müşteriye ulaşmayan kartlar ile yapılan sahtekârlıkları azaltırken; internet üzerinden yapılan sahtekârlıkların miktarını artırmıştır [33].

Kredi Kartı Hırsızlığı: Kredi kartının gerçek kartı taşıyanın elinden isteği dışında çıkmasının en sık rastlanan biçimi kredi kartı hırsızlığıdır. Kredi kartının yitirilmesi iki biçimde gerçekleşmektedir. Birincisi kartın henüz kart sahibine teslim edilmeden önce postada yitirilmesi, diğeri ise kart sahibinin elindeyken yitirilmesidir.

Bunların dışında kart hamilinin kartın kötüye kullanımı sonucunu doğuracak bir işlemden kazançlı çıkması hesabını yaparak, kaybetmediği veya çaldırmadığı halde kartını kullanıma kapattırması sonucu ortaya çıkan durumdur. Kart sahibinin bu durumdaki kazancı, kartını kapattırmadan önce yaptığı harcamaları kendi bilgisi dışında yapılmış gibi göstererek, bu tutarları ödemekten kaçınmasıdır. Özellikle yeni kredi kartları kanununda tüm bankalar için getirilen 24 saatlik kayıp-çalıntı kart sigortası, bu dolandırıcılık türünde gözle görülür bir artışın ortaya çıkmasına neden olmuştur [34].

Sahte Kart Kullanımı: Bu yöntemde sahte para gibi önce sahte kredi kartı da basılabilmektedir. Sahte kart yaratabilmenin birinci koşulu orjinal bir kart bilgisini ele geçirmekle başlar. Bu da iki türlü olabilmektedir: ya kart verisini kodlayıcı (encoder) ile kopyalayıp ele geçirerek ya da çöplerden, internet ortamından, kişilerin üzerlerinden kimlik bilgilerini çalarak mümkündür. Sahte kartların oluşturulmasında kullanılan yöntemlerden biri, geçerliliğini yitirmiş kartların manyetik bilgilerini silerek yerine geçerli bir kart verisinin yüklenmesi ya da white plastic diye tabir edilen,

üzerinde hiçbir görsel logo gibi emareler olmayan kartların manyetiklerine bu bilgilerin aktarılmasıdır [33, 35].

Kredi kartı sahtekârlıkları ile ilgili literatürde birçok çalışma bulunmaktadır. Dahl, 2006 ve Schindeler, 2006 kredi kartı sistemleri ile ilgili temel bilgi verdikleri bir çalışma yaparken; Hand ve Blunt (2001) da kredi kartı verisi ve karakteristiği hakkında detaylı bir çalışma yapmışlardır [36, 37, 38], [39].

Kredi kartı sahtekârlıklarıyla ilgili çalışmaların çoğunda yapay sinir ağları ve karar ağaçları gibi karmaşık gözetimli/denetimli algoritmalar kullanılmıştır. Stolfo ve diğerleri, (1999) bir sahtekârlık işleminin yasal kabul edilmesinin yani hatalı olarak işleme izin verilmesinin (Tip 1 hatası) maliyeti ile yasal olan bir işlemin sahtekârlık işlemi gibi kabul edilmesinin yani normal bir işlem için şüpheli olduğuna dair alarm üretilmesinin (Tip 2 hatası) maliyetini karşılaştırdıkları bir çalışma yapmışlardır [40]. Çalışmaya göre Tip 1 hatasının maliyeti, tip 2 hatasının maliyetinden yüksektir [39].

2.2.3. İnternet bankacılığında sahtekârlıklar

Kişilerin veya kurumların banka şubesine gelmeden, ev, ofis veya internete girilebilecek herhangi bir yerden, birkaç dakikada işlemlerini yapabilmeleri internet ve mobil bankacılığı cazip kılmaktadır. Bunun yanında gizliliğin olması, maliyetinin düşük olması gibi unsurlar kişileri internet ve mobil bankacılık kullanımına teşvik etmektedir. İnternet ve mobil bankacılıkta müşteriler, nakit para çekmek dışında her türlü yatırım, havale, fatura ödemesi ve tüketici kredisi başvurusu gibi işlemleri yapabilmektedir.

Sahtekârlık işlemleri yapmak isteyen kişiler için de internet ve mobil bankacılık cazip işlem kanalları olarak öne çıkmaktadır. Bu kanallardan yapılan işlemlerde banka çalışanları ile hiçbir irtibat bulunmadığı için sahtekârlar çok daha rahat hareket edebilmektedirler. İnternet ve mobil bankacılık kanallarındaki bilinen sahtekârlık yöntemleri aşağıda açıklanmaya çalışılacaktır.

Sahte Siteler ve Phishing Yöntemi: İnternet dolandırıcıları, özellikle banka ve finans kurumlarının sitelerinin görsel olarak benzerlerini hazırlayıp bu sitelere girilen bilgilerin kendilerine gönderilmesini sağlayabilmektedir. Sahte siteler arama motorlarındaki reklâm/destekleyici adreslerle ziyaretçi çekebildiği gibi, gerçek sitenin adresinin çok benzeri bir adrese yerleştirilerek, kullanıcıların yanlışlıkla gelmeleri de beklenebilmektedir. Ziyaretçileri sahte sitelere çekmek için en çok kullanılan yöntem "Phishing" yöntemidir [41].

"Phishing" terimi üç farklı kelimenin birleşmesinden ortaya çıkmaktadır. Password Harvesting'in (şifre toplama) baş harfleri ile fishing (balık tutma) kelimesinin birleşmesinden "phishing" kelimesi ortaya çıkmaktadır. Burada hesabın bulunduğu bankanın web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan bir internet dolandırıcılığı söz konusudur. Olta atıldığında en azından bir balık yakalanabileceği düşüncesinden esinlenerek uygulanmaktadır. Burada kullanıcı kandırılarak ona ait başta kredi kartı olmak üzere, şifre ve parolalar, hesap numaraları, kullanıcı kodları ve şifreleri gibi her türlü özel bilginin elde edilmesi hedeflenmektedir [35].

Tuş Kaydedici (Keylogger) ve Ekran Kaydedici (Screenlogger) Yöntemi: Keylogger bilgisayar kullanıcılarının internette dolaşırken, klavye kullanarak girdikleri bilgileri kaydeden ve bu bilgileri kötü niyetli kişilere gönderen yazılım iken; screenlogger keylogger ile aynı prensipte çalışan ve klavye tuşları yerine ekran görüntülerini kaydeden bir yazılım türüdür. Kullanıcının "fare" ile tıkladığı her ânın resmini çekerek kaydeden bu programlar sayesinde sanal dolandırıcılar sanal klavye kullanılarak girilen bilgileri de ele geçirebilmektedir [41].

Keylogger ve screenlogger yazılımları ya işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın yönetici haklarını kısmen veya tamamen saldırgana teslim etmekte olan truva atı (trojan) adlı yazılımlar aracılığıyla ya da kullanıcı tarafından bilinmeden bilgisayara yüklenebilmektedir.

Casus Yazılımlar ve Diğer Saldırı Türleri: Bir bilgisayarı ele geçirmek için en kolay yol bir dosyanın içine virüs programı saklamaktır. Saldırgan bu hedefine ulaşabilmek için öncelikli olarak güveni sağlamak isteyebilir. Bu amaçla kendi mail adresini aşina olunan bir mail adresi (resmî kurumlar, yakınlar vs.) gibi göstererek güvenilmesini sağlar. Saldırganlar, bunun dışında çok cazipmiş gibi görünebilen bir dosya veya link yollar. Bu dosya bilgisayara kopyalandığında (veya e-posta ekinden açıldığında) ve çalıştırıldığında, virüs bilgisayara bulaşmış olacaktır [42].

Salam tekniği, çok fazla sayıda banka hesabından, fark edilmeyecek kadar küçük meblağların belli bir hesaba transferi ile hukuka aykırı yarar sağlama yöntemidir. Transfer edilen meblağ o kadar küçüktür ki, hesabından para transfer edilen hesap sahipleri ile banka yöneticileri, yetkisiz hareketleri fark edemezler. Transfer edilen küçük meblağın çok sayıda hesaptan sağlanması nedeniyle, fail açısından çok büyük miktarda hukuka aykırı yarar sağlanmaktadır [43]. Bu işlemler için genellikle truva atı yazılımları kullanılmaktadır.

2.2.4. Sosyal mühendislik

Sosyal mühendislik yönteminde kişilerin dikkatsizliği ya da sosyal ilişkiler kullanılarak bilgi edinilmesi ön plana çıkmaktadır. Böylece internet bankacılığında gerekli olan şifre ve parolalara ulaşılması hedeflenmektedir. Sosyal mühendislik yöntemi çabuk sonuca götürmesi, hızlı ve basit olması nedeniyle saldırganlar tarafından sıklıkla kullanılmaktadır.

2.2.5. Çağrı merkezi aracılığıyla yapılan sahtekârlıklar

Çağrı merkezleri üzerinde amaçlanan sahtekârlıklar, sosyal mühendislik vakaları ile elde edilen bilgiler kullanılarak gerçekleştirilmektedir. Müşteri temsilcileri kendilerini arayan müşterileri yönetimlerinin düzenlediği müşteriyi tanımaya yönelik soru setleri ile karşılamakta ve işlem gerçekleştirmektedirler. Dolandırıcılar zaman içerisinde müşteri karşılama sorularının tamamını öğrenmiş olup, bu bilgilerden eksik olanları müşterinin bizzat kendisinden ya da şubelerden temin ettikleri görülmektedir. Bilgi

edinme hususunda sosyal mühendisler nüfus idareleri, vergi daireleri, mobil telefon operatörleri gibi her türlü kaynağı kullanabilmektedir.

Çağrı merkezleri sahtekârlar tarafından daha ziyade kart talepleri, kart teslim adresi değişiklikleri, ek kart talepleri gibi amaçlarla kullanılmakta olup geçerli kimlik doğrulamasını gerçekleştirdikten sonra sesli otomatik yanıtlama sistemleri (IVR, interactive voice response) üzerinden şifre temin edebilmekte, işlem onaylayabilmektedirler.

2.2.6. Şube kanalından yapılan sahtekârlıklar

Bankaların kurulduğu yıllardan itibaren, kredi, kart, hesap gibi birçok bankacılık ürünü için kötü niyetli kişiler tarafından düzenlenen sahte bilgi ve belgeler (kimlikler, sahte hesap cüzdanları, talimatlar vb) yoluyla bankalara sahte bireysel kredi ve kredi kartı başvuruları gerçekleştirilmekte, müşteri hesabına yönelik saldırılar düzenlenmektedir. Müşteri kimliğinin tespiti için nüfus cüzdanı, ehliyet, pasaport ve e-pasaport belgeleri geçerli kabul edilmektedir. Her belgenin kendine özgü güvenlik özellikleri bulunmasına karşın sahtecilik saldırılarının tamamiyle önüne geçildiği söylenemez. Kaybolan/çalınan kimlik belgelerini ele geçiren kötü niyetli kişiler bu kimliklerle:

- Şirket kurabilirler,
- Çapraz kimlik çıkarabilirler,
- Borç taahhütlerine girebilirler,
- Sahte fatura düzenleyerek yasa dışı gelir elde edebilirler,
- Cep telefonu hattı alıp tehdit, şantaj, terör gibi amaçla kullanabilirler,
- Yurtdışına çıkabilirler,
- İnternet bankacılığı başlatabilirler ve
- Evlenebilirler.

Bu durumda, gazeteye ilan vermek, emniyet makamlarına (pasaport şubesi/mahalli polis makamları, yurt dışı için konsolosluklar vb.) haber vermek, emniyet biriminden, "kaybolduğuna ya da çalındığına dair yazı veya tutanak" almak yeterli değildir. Mutlaka Vergi Dairesine bildirimde bulunulması gerekmektedir.

Herhangi bir sorgu yapılmadan, sadece müşterinin ibraz etmiş olduğu nüfus cüzdanı fotokopisine istinaden açılan mevduat hesabı; şube, banka veya üçüncü bir şahsın zararına yol açma riski taşımaktadır. Bankaların internet şubesi müşterilerinin kullanıcı kodları ve şifreleri ele geçiren dolandırıcılar, bu müşterilerin hesaplarından paravan olarak açılan hesaplara EFT ve havaleler yapmaktadır. Sadece kimlik ibrazı ile herhangi bir sorgulama yapılmadan açılan bu tür hesaplara yapılan transferler, genellikle aynı gün çekilerek müşteri zararına dönüşmektedir. Şubeler aracı kılınarak gerçekleştirilen sahtekârlık işlemlerinin önüne geçilmesi için aşağıdaki önlemlerin alınması önerilmektedir:

- Müşteri hesabının ilk hareketleri ilke olarak ve ihtiyaten şüpheli olarak kabul edilmeli ve bu hesap hareketleri için azami dikkat sarf edilmelidir. Internet, ATM, çağrı merkezi ve diğer alternatif dağıtım kanalları (şube dışı bankacılık) kullanılarak yapılan transferlerin amirden veya amir bankadan teyit edilmesi önerilmektedir.
- Şubeyle yeni çalışmaya başlayan bir müşteriye, aynı şubeden veya aynı bankadan sürekli gelen havale ve EFT'ler hangi kanaldan yapılmış olursa olsun şüpheli işlem olarak değerlendirilmelidir.
- Özellikle yurt dışında yaşayan veya hareketsiz hesapları olan müşterilerin müşteri kaydı altında yeni hesap açılışı yapılması ve bu hesaba mevcut diğer hesaplardan para aktarılması şüpheli olarak değerlendirilmelidir.
- Bireysel kredi/kredi kartı başvurularında sahte belge ihtimaline karşın önlem alınmalıdır.

2.3. Sahtekârlık İşlemlerinin Modellenmesindeki Zorluklar

Sahtekârlık işlemleri birçok farklı şekilde gerçekleşmekte ve yeni teknolojiler ile yeni ürünlerin hayatımıza girmesi yeni sahtekârlık yöntemlerinin geliştirilmesi için de fırsat sunmaktadır. Sahtekârlık işlemlerinden kaynaklanan tüm kayıpların hesaplanması pek mümkün gözükmemekle birlikte, bu konuda kamuoyunun bilgisine sunulmuş en güncel bilgi ACFE'nin 2014 yılı için yayınladığı raporda yer almaktadır. Araştırma sonuçlarına göre tipik bir kuruluş her yıl gelirlerinin %5'ini sahtekârlık işlemleri nedeniyle kaybetmekte iken bu veri 2013 dünya gayri safi hasılası ile

karşılaştırıldığında yıllık kayıp tutarının yaklaşık 3,7 trilyon dolar olduğu görülmektedir [5]. Böylesine büyük bir kaybı önlemek için çalışmalar yapılmasının gerekliliği açıkken, bu çalışmaların başarıyla sonuçlanması sahtekârlık işlemlerinin yapısından kaynaklanan birçok zorluğun aşılmasına bağlıdır.

2.3.1. Sahtekârlık işlemleri nadirdir

Sahtekârlık işlemleri genellikle nadiren gerçekleşir ve gizlice yapılmış olması ve nadiren gerçekleşmesi nedeniyle tespit edilmesi güçtür. Doğrudan bir bireye veya bir kuruma karşı yapılan sahtekârlık işlemlerinin, toplam işlemler içerisindeki oranı %0,1 düzeyinde bile olabilir. 1000 adet işlemin içerisine gizlenmiş olan 1 adet sahtekârlık işlemini tespit etmek için geliştirilecek model ise üzerinde detaylı bir çalışma yapılmasını gerektirecektir.

2.3.2. Sahtekârlık işlemlerinin yapısı sürekli değişir

Sahtekârlık işlemini yapan kişiler, sahtekârlıkları tespit etmek ve önlemek için geliştirilen yöntemlere ayak uydurmak ve kendi metotlarını ustalıkla güncellemek konusunda çok mahirdirler. Tespit ve önleme için geliştirilen metotların da sahtekârlık işlemlerini yapan kişilerin yeni stratejilerine adapte olması ve sürekli güncellenmesi gerekmektedir. [44]'de bu durum sürekli evrimleşen grip virüsüne karşına sürekli geliştirilmesi gereken grip aşısına benzetilmektedir.

2.3.3. Büyük veri kümelerine ihtiyaç vardır ve kaynaklar çok kısıtlıdır

Bankalar, telekom şirketleri veya e-ticaret şirketleri gibi sahtekârlık işlemlerinin başlıca hedefi olan kurumların günlük işlem hacimleri oldukça yoğun olmakla birlikte, bu işlemler arasında sahtekârlık işlemi olan ve büyük kayıplara yol açacak işlemlerin sayısı oldukça azdır. Sahtekârlık işlemlerinin tespit edilmesini sağlayacak modeller geliştirilirken bu modellerin test edilebilmesi ve tam zamanında gerekli kontrolleri yaparak önleyici aksiyonlara dönüşecek bilgi üretebilmesi için büyük veri kümelerine, hızlı ve verimli çalışan algoritmalara ihtiyaç duyulmaktadır.

Ayrıca sahtekârlık işlemleri ile ilgili veri kümelerine ve modellemeye dair teknik detaylara ulaşmak oldukça güçtür. Finansal kurumlar savunma stratejilerini veya maruz kaldıkları sahtekârlık işlemlerini güvenlik ve itibar koruma içgüdüleri nedeniyle paylaşmamaktadır. Bu anlamda sahtekârlık işlemlerini tespit ve önleme amaçlı analizler gerçekleştirilmesini sağlayacak veri temin edebilmek bu çalışmaların gerçekleştirilebilmesi için önemli bir adımdır [44]. Sahtekârlık işlemleriyle ilgili kamusal paylaşıma sunulmuş, en yaygın kullanıldığı bilinen iki farklı veri seti bulunmaktadır:

- İspanyol otomobil sigorta hasar taleplerine ait küçük bir veri seti
- KDD Cup 1999 Ağ saldırı tespiti veri seti [44].

2.3.4. Modelleme sırasında genelde sahtekârlık işlemleri bilinmiyordur

Sahtekârlık işlemleri yapılan analizler sonucunda tespit edilmiş olabileceği gibi birçoğu hiç farkedilmeden gerçekleşiyor da olabilir. Daha önce tespit edilmiş ve veri tabanında sahtekârlık işlemi olarak kaydedilmiş işlemlerin bulunduğu bir veri kümesi üzerinde çalışılarak model geliştiriliyorsa bu çalışmalara *gözetimli/denetimli (supervised)* ismi verilmektedir. Üzerinde çalışılan veri kümesinde sahtekârlık işlemleri belirtilmemişse bu çalışmalara da *gözetimsiz/denetimsiz (unsupervised)* ismi verilmektedir. Sahtekârlık işlemlerinin tespiti amacıyla geliştirilen model gözetimli veya gözetimsiz olsun üretilen sonuçların şüphe skorları ve sahtekârlık işlemi tahminleri olarak değerlendirilmesi gerektiği belirtilmektedir.

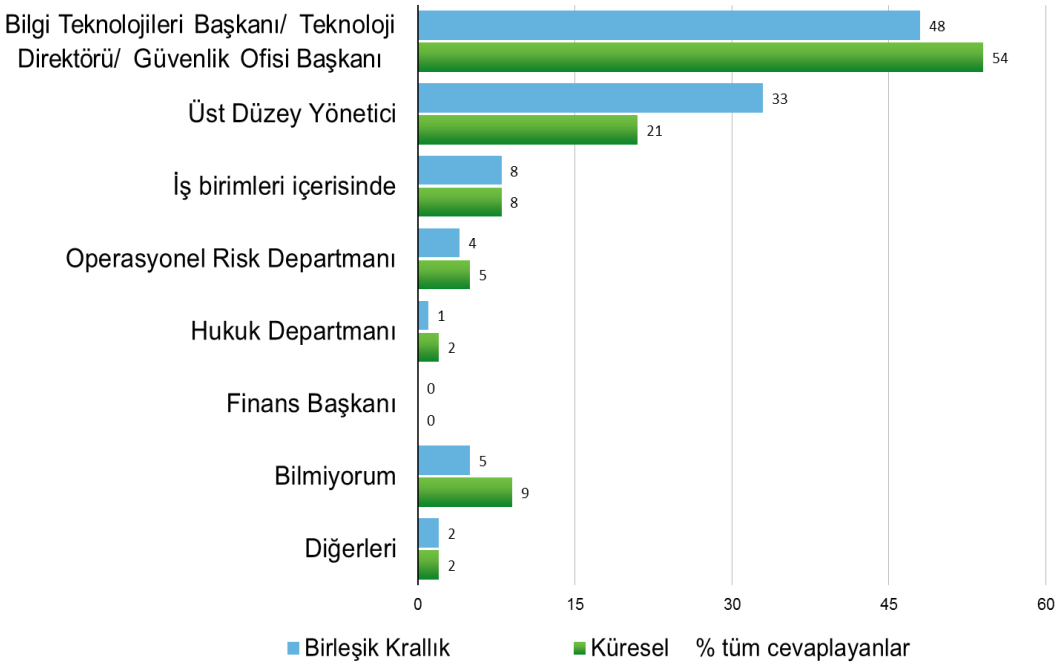
2.3.5. Sahtekârlık işlemlerinin yapısı karmaşıktır

İşlem verilerindeki karmaşıklığın yanısıra sahtekârlık işlemlerini meydana getiren olaylar silsilesi de karmaşık bir yapıya sahiptir. Sahtekârlık işlemini yapan kişilerin gizlenmek için özel olarak geliştirdikleri yöntemler karmaşıklığın temel sebebi olarak görülebilir. Sahtekârların geçtikleri yolu karartmak için karmaşıklaştırdıkları bu işlemlerin tespiti için model geliştirirken dikkate alınacak değişkenlerin seçimi, modelin yapısını etkileyen temel faktörlerden birisidir.

2.4. Kurumsal Sahtekârlık Önleme Stratejisi, Bileşenler ve Güçlükler

Teknolojideki gelişmelere paralel olarak müşterilere sunulan ürün ve hizmet çeşitleri ile kanallarının da hızla artış göstermesi nedeniyle finansal kuruluşlar için sahtekârlık işlemlerinin yönetimi yeniden düşünülmesi gereken konular arasında yerini almaktadır. Ürün çeşitliliğindeki artış ve farklı kanallardan hizmet verilmesi müşteri memnuniyetini artırdığı gibi sahtekârlar için de daha çok fırsat anlamına gelmektedir.

Kurumsal bir sahtekârlık önleme stratejisi geliştirilmek istendiğinde cevaplanması gereken en temel sorulardan biri, bu işlemlerin yönetiminden kurum içinde kimin sorumlu olacağıdır. Sahtekârlık işlemlerinin dağınık ve değişken yapısı nedeniyle bu sorunun cevabı kurumdan kuruma ve hatta ulusal düzeyde düşünüldüğünde ülkeler arasında bile farklılık göstermektedir. PriceWaterhouseCoopers'ın 2011 Global Economic Crime Survey isimli raporunda yer alan aşağıdaki grafikte görüleceği gibi, Birleşik Krallık'ta ankete katılan kişilerin %48'i, şaşırtıcı bir şekilde sahtekârlık işlemlerinin önlenmesi ve yönetilmesinden bilgi teknolojilerinden sorumlu başkanın (CIO) sorumlu olması gerektiği şeklinde cevap vermiştir.



Şekil 2.5. Anketi cevaplayanların siber suç risklerinin yönetiminden kimin sorumlu olduğuna ilişkin algısı [45]

Küçük boyutlu sahtekârlık işlemlerini tespit etmek ve önlemek göreceli olarak daha kolay ve daha az maliyetlidir. Bununla birlikte organize suç zincirlerinin yol açacağı kayıpları önleyebilmek için mümkün olduğunca erken aksiyon alınmalı ve kurumsal düzeyde bu tehditlerle mücadele edilmelidir. Kurumların ölçeğine veya bütçesine bakılmaksızın kurumsal bir sahtekârlık önleme stratejisi geliştirilmiş olması hem bugünün hem geleceğin tehditlerine karşı kurumu koruyacaktır. Kurumsal bir sahtekârlık önleme stratejisi gelişim ve uygulamasının sağlanmasının bağlı olduğu bileşenler aşağıda başlıklar halinde açıklanmaya çalışılacaktır.

2.4.1. Veri bütünlüğü

Kurumsal bir sahtekârlık önleme stratejisi geliştirebilmek için veri bütünlüğünün sağlanması hayati öneme sahiptir. Bankaların işlem verdiği birbirinden farklı işlem kanalları ve işlem türleri düşünüldüğünde, bu sistemlerin her biri için farklı bilgi sistemlerinin kullanıldığı gerçeği ve verilerin farklı veritabanlarında tutulma ihtimali karşımıza çıkmaktadır. Etkili bir sahtekârlık önleme stratejisi geliştirilebilmesi için birçok farklı kaynaktaki veriyi barındıran kurumsal bir sahtekârlık veritabanının bulunması önemlidir. Bu veri tipleri aşağıdaki gibi özetlenebilir:

- Tüm kanallardan ve tüm işlem tiplerinde müşterilerin gerçekleştirdiği işlemlere ait veri
- Müşteri hesap bilgilerini içeren veri
- Şube, ATM ve işlemlere ait konum bilgisini içeren veri
- İç sahtekârlıklara karşı insan kaynakları verisi

Anlık işlemlere dair sahtekârlık ölçümlerinin yapılabilmesi için bu verilerin tamamının hızlı bir şekilde entegre edilmesi ve yorumlanması gerekecektir. Veri bütünlüğünün sağlanması kurumsal sahtekârlık stratejisi geliştirmenin en önemli adımlarından biridir.

2.4.2. Sahtekârlık tespitine dair yöntem ve modeller

Sahtekârlıkları tespit etmek için yöntem ve model geliştiren kurumların etkili bir strateji geliştirebilmek için aşağıdaki yöntemlerin bir veya birkaçını birarada kullanmaları gerekmektedir:

- İş kuralları: Genel olarak tecrübeye veya izlenimlere dayalı, işlemlere skor atayan veya alarmlar üreten iş kuralları.
- Anomali tespiti: İşlemlerle ilgili normal veya beklenen davranışların tanımlanmış olduğu durumlarda, normalden veya beklenenden istatistiki olarak sapma olmasına göre alarm üreten yöntem.
- Tahmin edici modeller: Daha önce yaşanmış sahtekârlık işlemlerini baz alarak tüm işlemlere sahtekârlık skoru atayan ve bu skora göre alarm üreten sistemler.
- Sosyal ağ analizleri: İşleme taraf olan kişi veya hesabın, daha önce yaşanmış sahtekârlık olaylarına karışmış kişi veya hesaplarla ortak özelliklerinin derecesine göre alarm üreten yöntem.

Bu yöntemlerin nasıl konumlandırılacağı kurumsal sahtekârlık stratejisi geliştirmenin önemli bir adımıdır.

2.4.3. Alarm durumlarının yönetimi

Sahtekârlık işlemlerinin tespitine yönelik çalışmaların çıktısı genelde üretilen alarmlar olmaktadır. Anlık karar verilmesi gereken durumlarda (kredi kartı veya debit kart işlemleri gibi) bir alarm üretilmesinin yanısıra işlemler durdurulabilir ve gerçekleşmesine izin verilmeyebilir. Sadece alarm üretilen durumlarda ise bu alarmların yönetilme şekli kurumdan kuruma göre farklılık gösterebilmektedir. Herbir işlem kanalında oluşan alarmın takibini farklı bir ekip yapabileceği gibi bu ayrım işlem tiplerine göre de yapılabilir. Benzer şekilde bu alarmların takibinin yapılması için kullanılan ürün de farklılaşabilir. Örneğin kredi kartı ve pos işlemlerinde üretilen alarmları bir ekip yönetirken diğer bankacılık işlemlerinde oluşan alarmları farklı bir ekip takip ediyor olabilir. Bazı organizasyonlarda ise üretilen tüm alarmların takip

edildiği tek bir ürün konumlandırması ve paralel olarak bu alarmların tamamının takibinden sorumlu tek bir ekip de yer alabilir.

Alarm yönetimi sahtekârlık işlemlerinin önlenmesi için önemli bir adımdır. Alarm üretilen işlemlerin takibi, işlemin gerçekten sahtekârlık işlemi olup olmadığına karar verilmesi ve bu bilginin sistemlere işlenmesi gerek kurulan tahmin modellerinin geliştirilebilmesi gerekse de gizli sahtekârlık desenlerinin ortaya çıkartılabilmesi için önem taşımaktadır.

Olası müşteri mağduriyetlerinin erken tespit edilebilmesi veya önlenebilmesi için alarm üretilen işlemlerle ilgili hızlı aksiyon alınması gerekmektedir. Sahtekârlık işlemlerine dair alarm üreten sistemlerde, alarmlarla ilgili hızlı aksiyon alınmasını sağlamak amacıyla birçok dış sistemle entegrasyon yapılması da mümkündür. Kullanılan sistem, üretilen bir alarmla ilgili müşterilere veya çalışanlara bilgilendirici kısa mesajlar ve elektronik postalar gönderebilir veya otomatik olarak telefon görüşmeleri başlatabilir.

2.4.4. Sonuçların değerlendirilmesi

Kurumsal bir sahtekârlık önleme stratejisi geliştirmiş tüm kurumlarda hesaplanan temel ölçüt, *"önlenen kayıpların tutarı"* denilebilir [46]. Önlenen kayıpların tutarı genel olarak, henüz gerçekleşmeden tespit edilmiş ve müşteri mağduriyetine yol açmadan önlenmiş işlemlerin tutarı şeklinde tanımlanabilir. Ancak bu tanım, ilk sahtekârlık işleminin önlenmesiyle önüne geçilmiş diğer olası sahtekârlık işlemlerinin tutarlarını dikkate almaz. Daha kapsamlı bir ölçüm yapmak amacıyla sahtekârlık işlemi tespit edildiği andaki hesap bakiyesini yani gerçekleşebilecek en yüksek sahtekârlık işlemi tutarını kayıp tutar olarak kabul eden ölçümler de bulunmaktadır.

Aşağıdaki ölçeklerden biri veya birkaçı kurumlarda sahtekârlık tehdidinin boyutunu ölçmek için kullanılabilir. Bu ölçümlerin yapılabilmesi için kurum veritabanlarında ilgili verinin sağlıklı bir şekilde kayıt altında tutulması gerektiği açıktır.

- Sahtekârlık işlemleri nedeniyle kaybedilen tutarlar

- Sahtekârlık işlemlerinin yol açacağı önlenmiş kayıp tutarlar
- Önlenen ve gerçekleşen sahtekârlık işlemlerinin sayısı
- Ortalama kayıp tutarı (Kayıp tutarları toplamı/hesap, müşteri sayısı)
- Ortalama sahtekârlık işlemi sayısı (Toplam sahtekârlık işlemleri sayısı/hesap, müşteri sayısı) [46]

Sahtekârlık işlemlerinin tespiti ve olası kayıpların en aza indirilmesi için işletilen prosedürlerin ve üretilen sonuçların iyi bir şekilde değerlendirilmesi gerekmektedir. Kayıpları önlemek amacıyla çok fazla işlem durdurulduğunda veya ek güvenlik önlemleri getirildiğinde bu kez de yüksek ihtimalle müşteri şikâyetleri başlayacaktır. Müşteri şikâyetine ve kaybına neden olmayacak ve sahtekârlık işlemlerini de önleyecek kadar etkili bir strateji geliştirilmesi sahtekârlık işlemlerinin kurumsal düzeyde yönetiminin en önemli noktasıdır denilebilir.

2.4.5. Bütçeleme

Kurumsal bir sahtekârlık önleme stratejisi geliştirilmesi, çoğu zaman bu tip işlemleri önleyecek bir teknolojik ürünün kullanılmasına ihtiyaç duyulması ile birlikte gündeme gelmektedir. Böyle bir teknolojik ürünün kurumda konumlandırılması ise gerek ilk yatırım gerekse ihtiyaç duyulacak entegrasyon çalışmaları nedeniyle oldukça maliyetli ve uzun soluklu projelere dönüşmektedir. Birçok kurum kendi içerisinde projenin değerlenebilirliğini ölçmek amacıyla çeşitli ölçekler geliştirmiştir. Örneğin bir önceki bölümde bahsedilen ölçeklerden toplam kayıp tutarları dikkate alınarak, proje maliyeti üzerinden oransal ölçekler geliştirilebilmekte ve projenin yapılıp yapılmayacağına karar verilebilmektedir.

Bir sonraki bölümde finansal sahtekârlıklarla mücadele edebilmek için kullanılan veri madenciliği teknikleri ve piyasada yer alan ticari ürünler hakkında bilgi verilecek; finans sektöründeki sahtekârlıkla mücadele uygulamaları özetlenecektir.

BÖLÜM 3. SAHTEKÂRLIK İŞLEMLERİNİN TESPİTİNDE KULLANILAN TEKNİKLER

Finansal sahtekârlık olaylarının sayısındaki ve sebep olduğu kayıplardaki artış nedeniyle, kurumsal bir sahtekârlık önleme stratejisi geliştirmek ve bu amaçla teknolojik ürünlere yatırım yapmak tüm dünyadaki kuruluşlar açısından gecikmiş öncelikli bir iş olarak görülmektedir [47]. Sahtekârlık işlemlerinin gerçekleşme şekillerindeki çeşitlilik ve hızlı değişkenliğe sahip olması nedeniyle kurumlar da bu işlemlerle mücadele konusunda hızlı aksiyon alabilecekleri bir yapıya ihtiyaç duymaktalar.

Bir kurumda sahtekârlıkla mücadele amacıyla bir sistem kurulmasına karar verildiğinde cevaplanması gereken temel bazı sorular bulunmaktadır:

- Kurulacak sistem hangi ürün/kanallar için konumlandırılacaktır?
- Sistem birden fazla ürün ve kanal için kullanılacaksa, ürün ve kanallar için sistemin yönetimi nasıl yapılacaktır?
- Sistem sahtekârlık işlemlerini önlemek mi (henüz işlem gerçekleşmeden) yoksa tespit etmek (işlem gerçekleştikten sonra) amacıyla mı kullanılacaktır?
- Sistemin dinamik olması hedeflenmekte midir?
- Sistem kullanıcıları ve yöneticileri kimler olacaktır?
- Sistemin veri kaynakları, çalışma methodolojisi ve çıktıları neler olabilecektir?

Yukarıdaki soruların cevaplarına bağlı olarak kurulacak sistemin temel gereksinimleri ortaya çıkacaktır. Örneğin, kurulacak sistemle, sahtekârlık işlemlerinin henüz gerçekleşmeden önlenmesi isteniyorsa müşteri memnuniyetsizliğine yol açmayacak kadar hızlı bir sistemin kurulması gerektiği açıktır. Sistemin tamamını veya bir kısmını iş kullanıcıları kullanacaksa kullanıcı dostu ekranlara ihtiyaç duyulacaktır. Sistemin dinamik olması hedefleniyorsa güncellenmesi kolay, sürekli öğrenen ve kendini

güncelleyen yapılara sahip olması gerekecektir. Ürün ve kanallar arası veri paylaşımı, sistemin üretebileceği sonuçlar ve bunlar neticesinde alınabilecek aksiyonlar karar verilmesi gereken noktalardan bazılarıdır.

Uzman sistemler sahtekârlık işlemleriyle mücadelede kullanılan en eski tekniklerdendir. Bir grup uzmanın görüşleri ile oluşan kurallar bu sistemler aracılığıyla çalıştırılır ve sistem bu kuralların sonucuna göre bir karar verebilir. Uzman sistemlerin dezavantajı kişilerin yargılarına ve muhtemelen daha önce yaşanmış sahtekârlık olaylarına bağlı olmasıdır. Bu kurallar arasında çelişen kurallar olması da olasıdır [44]. Uzman sistemlerden daha ileri düzeyde olduğu söylenebilecek diğer sahtekârlık önleme sistemleri, kurallar arası çelişkileri önleyen otomatik kural optimizasyonu yapan kural motorları içeren sistemlerdir. Bu kural motorlarının bulanık mantık methodolojisi ile çalışması da mümkündür.

En güçlü sahtekârlık önleme sistemlerinin müşterilerin geçmiş finansal ve finansal olmayan verileri üzerinde çalışan analitik modelleri içeren sistemler olduğu söylenebilir. Birçok veri madenciliği tekniğinin tek başına veya birlikte kullanılabildiği modeller;

- Dinamik kural keşfi ve güncellemesi,
- Müşteriler veya işlemler için limit belirleme,
- Müşteriler ve işlemler arasındaki gizli kalmış ilişkileri ortaya çıkartabilme,
- Gizli kalmış sahtekârlık örüntülerinin keşfedilmesi gibi amaçlarla bu sistemlerin içerisine dahil edilmiştir.

Literatürdeki çalışmalar incelendiğinde sahtekârlık işlemlerinin tespit edilmesi ve önlenmesi için birçok veri madenciliği tekniği kullanılarak çalışma yapıldığı görülmekte olup, Bölüm 3.1.'de bu teknikler hakkında bilgi verilecektir.

3.1. Sahtekârlıkla Mücadelede Veri Madenciliği

Yıkıcı sonuçlarının önlenmesi için tespit edilmesi hayati öneme sahip olan finansal sahtekârlıkların tespit çalışmalarında yığınla veri arasında gizli kalmış gerçekleri gözler önüne sermesi nedeniyle veri madenciliği önemli bir rol oynamaktadır. Veri madenciliği birçok analiz ve modelleme tekniğini bir arada kullanarak veri içinde gizlenmiş örüntüleri ve ilişkileri ortaya çıkaran bir süreçtir. Bu desenlerin normal ve normal olmayan müşteri davranışları ile ilgili tahminlemede kullanılabileceği ise açıktır.

Veri madenciliğinde kullanılan modeller tahminleyici (predictive) ve tanımlayıcı (descriptive) olmak üzere iki kategoride toplanabilir [48]. Tahminleyici modellerin amacı sonuçları bilinen veriyi kullanarak bilinmeyen sonuçları tahmin etmek iken, tanımlayıcı modeller karar vermeye yardımcı olması amacıyla veride gizli olan desenleri ortaya çıkarmayı amaçlar [48]. Bununla birlikte kullanılan modellerin fonksiyonlarına göre sınıflandırılması da mümkündür. Ngai ve arkadaşları finansal sahtekârlıkların tespit edilmesinde kullanılan veri madenciliği tekniklerini inceledikleri çalışmalarında, veri madenciliği tekniklerini; sınıflandırma, kümeleme, tahminleme, anomali tespiti, regresyon ve görselleştirme olarak sınıflandırmıştır [16]. Han ve Kamber ise veri madenciliği modellerini;

- Sınıflandırma ve regresyon,
- Kümeleme,
- Birliktelik kuralları,
- Zaman serileri,
- Grafik madenciliği ve sosyal ağ analizi başlıkları altında incelemiştir [49].

Bu gruplandırmaya göre sınıflandırma ve regresyon modelleri ile zaman serileri modelleri tahminleyici; kümeleme, birliktelik kuralları ile grafik ve sosyal ağ analizleri ise tanımlayıcı tekniklere girmektedir. Tahminleyici metotlar geçmiş verideki durumlar tarafından yönlendirildiği için aynı zamanda *gözetimli/denetimli (supervised)* metotlar olarak da bilinir. Tanımlayıcı metotlar ise mevcut veri üzerinde çalıştığı ve geçmişin gözlemlerine sahip olmadığı için *gözetimsiz/denetimsiz*

(unsupervised) metotlar olarak da isimlendirilir. Herhangi bir amaçla bu metotlar birlikte veya ayrı ayrı kullanılabilmektedir. Tablo 3.1.'de gözetimli ve gözetimsiz yöntemlere ilişkin örnek kullanım amaçları sunulmuştur.

Tablo 3.1. Modelleme amacı ve öğrenme tekniğine göre veri madenciliği tekniklerinin kullanımı [50]

Modelleme Amacı	**Gözetimli Öğrenme**	**Gözetimsiz Öğrenme**
Tahminleme	ATM'de kullanılan nakit Hastane maliyetleri Sahtekârlık tespiti Kampanya analizleri	Uygulanabilir değil
Sınıflandırma	Segmentasyon Marka değiştirme Takipteki alacaklar Sahtekârlık tespiti Kampanya analizleri	Segmentasyon
Keşfedici	Segmentasyon Skor kart oluşturma Sahtekârlık tespiti Kampanya analizleri	Segmentasyon Profilleme
Benzerlik	Uygulanabilir değil	Çapraz satış / Yukarı satış Sepet analizi

Sahtekârlık işlemlerinin tespitinde kullanılan teknikler incelendiğinde gözetimli ve gözetimsiz tekniklerin ayrı ayrı kullanımları görüldüğü gibi bu tekniklerin kombinasyonlarının kullanıldığı da görülmektedir. Gözetimli tekniklerin kullanıldığı sahtekârlık tespit ve önleme çalışmalarında daha önce gerçekleşmiş normal ve normal olmayan (sahtekârlık) işlemlerin biliniyor olması gerekmektedir. Böylece kurulan model her yeni işlem için bir şüphe puanı üretebilecektir. Gözetimsiz tekniklerin kullanıldığı çalışmalarda ise daha önceki işlemlerin normal mi sahtekârlık işlemi mi olduğu bilinmemektedir. Phua ve diğerleri, sahtekârlık işlemlerinin tespit edilmesinde kullanılan veri madenciliği tekniklerini inceledikleri araştırmalarında, literatürdeki çalışmaları gözetimli, yarı gözetimli ve gözetimsiz olarak incelemişlerdir [9]. Sahtekârlık işlemlerinin tespitinde gözetimli tekniklerin kullanılmasıyla ilgili

eleştirilere bu çalışmada da yer verilmiştir. Farklı kaynaklarda değinilen bu eleştirilerin bazıları şöyle sıralanabilir:

- İşlemlerin normal mi sahtekârlık işlemi mi olduğuna dair etiketler (label) yanlış verilmiş olabilir [51].
- Etiketlenmiş veriyi elde etmek oldukça güç ve pahalı olabilir [52].
- Sahtekârlık işlemini yapan kişiler gizlenebilmek amacıyla sürekli yöntem değiştirdikleri için etiketlenmemiş veriyi kullanmak yeni sahtekârlık desenlerinin tespit edilmesinde daha faydalı olabilir [53].

Aşağıda sırasıyla temel veri madenciliği teknikleri ve sahtekârlık işlemlerinin tespitinde kullanılmış diğer teknikler hakkında bilgi verilecektir.

3.1.1. Sınıflandırma ve regresyon

Sınıflandırma ve regresyon veri içindeki önemli sınıfları belirleyen veya gelecekteki trendleri tahmin edebilecek modeller sunan iki önemli veri madenciliği tekniğidir. Sınıflandırma kategorik değerli veriyi tahmin ederken, regresyon kesikli olmayan sürekli verinin tahmini için kullanılır. Sınıflandırmada sınıfları bilinen öğrenme veri setine dayalı olarak kurulan modeller ile veri, daha önceden belirlenmiş gruplara ayrılır ve gelecekteki verinin hangi grupta yer alacağı tahmin edilir. Sınıflandırma ve regresyon modelleri arasında en çok kullanılan teknikler karar ağaçları, yapay sinir ağları, genetik algoritmalar, k-en yakın komşu, lojistik regresyon ve naive-Bayes teknikleridir [49].

Karar Ağaçları: Gözlemlerden yola çıkarak olası sonuçları tahmin etmeye çalışan tahminleyici karar destek araçlarıdır. Bu ağaçlar ID3 (Iterative Dichotomiser), CART (Classification and Regression Trees- Sınıflandırma ve Regresyon Ağaçları) ve C4.5 (ID3'ün bir sonraki versiyonu) gibi makine öğrenmesi temelli algoritmalar kullanılarak kurulabilir [54]. Tahminler yapraklarla, özelliklerin birleştiği noktalar ise dallarla gösterilir. Genellikle kredi kartı, otomobil sigortası ve kurumsal sahtekârlıkların tespitinde kullanılmıştır [49].

Yapay Sinir Ağları: Birbirine bağlı köşeleri kullanarak insan beyninin işleyişini taklit etmeye çalışan bir tekniktir. Yoğunlukla sınıflandırma ve kümeleme problemlerinde kullanılır. İnsan beyninin yapısına benzer olarak yapay sinir ağları da düğümlerden (akson) ve bu düğümleri birbirine bağlayan yönlü oklardan (dendrit) oluşur [55]. Özellikle kredi kartı, otomobil sigortası ve kurumsal sahtekârlıkların tespitinde kullanılmıştır [49].

Bayes Ağı: Bir dizi rasgele değişken ve onların koşullu bağımlılıklarını yönlü düz ağ grafiği olarak gösterir. Bu grafiklerde düğümler rasgele değişkenleri, oklar ise değişkenler arasında var olan koşullu bağımlılıkları gösterir. Değişkenler arasındaki koşullu olasılıkları gösteren bir de tablo oluşturulur [54]. Genellikle kredi kartı, otomobil sigortası ve kurumsal sahtekârlıkların tespitinde kullanılmıştır [49].

Lojistik modeller: Lojistik model binom regresyonu için kullanılan genelleştirilmiş lineer bir modeldir. Tahmin edilen değişken sayısal veya kategorik olabilir. Genel olarak otomobil sigortaları ve kurumsal sahtekârlık problemlerinin çözümünde kullanılmıştır.

3.1.2. Kümeleme

Kümeleme benzer veriyi biraraya toplayarak yeni kategoriler oluşturmak amacıyla veriyi kümelere böler. Kümeleme algoritmalarının temel amacı küme içi benzerliği en yüksek ve kümeler arası benzerliği en düşük tutmaktır. Belirlenen değişkenlere göre verinin kümelere bölünmesini amaçlayan kümeleme analizlerinde, kümeler önceden bilinmiyordur. Sınıflandırma analizlerinden farklı olarak önceden belirlenmiş sınıf kümeleri yoktur [56].

Kümeleme analizlerinde kullanılan birden fazla model bulunmakta olup, bu modeller temelde hiyerarşik ve hiyerarşik olmayan modeller olmak üzere ikiye ayrılmıştır. Hiyerarşik yöntemler, aşamalı olarak veri noktalarını birleştirip veya ayırıp kümeler oluşturmakta ve birden fazla kümeleme çözümü sunmaktayken; hiyerarşik olmayan yöntemler, önceden belirlenmiş küme sayısı kadar küme oluşturup tek bir çözüm

sunacak şekilde çalışmaktadır [57]. En kolay ve hızlı kullanım imkânı veren kümeleme modellerinden bir tanesi *k* küme sayısının önceden belirlendiği k-means algoritmasıdır. Algoritma sonucunda çok az üyeye sahip olan kümelerin oluşması halinde, bu kümelerdeki üyelerin anomali gösterdiği yani uç değer olarak değerlendirilebileceği belirtilmiştir [55]. Ayrıca, anomalilerin (uç değerlerin) tespit edilmesinin, sahtekârlık işlemlerinin tespit ve önlenmesinde çok kullanışlı bir yöntem olduğu bilinmektedir [54]. Bu yaklaşımla, kümeleme analizlerinin finansal işlemlerdeki uç değerlerin sahtekârlık belirtisi olarak tespit edilmesi amacıyla kullanılabileceği açıktır.

3.1.3. Anomali tespiti

Anomali (uç değer) tespiti kümeleme algoritmalarının bir alt koludur denilebilir. Bir anomali (uç değer), verinin geri kalan kısmıyla uyuşmayan bir veri objesidir. Bu uç değer bir gürültü nesnesi olabileceği gibi aykırı bir durumu da temsil ediyor olabilir. Anomali tespiti sahtekârlık işlemlerinin tespitinde oldukça sık kullanılan bir tekniktir.

Sahtekârlık işlemlerini tespit etme problemi, kesikli dizilerdeki anomali tespiti problemi gibi tanımlanabilir ve ilgili veri setleri de zamansal veya uzay-zamansal veri dizileri olarak sınıflandırılabilir [58, 59]. ATM sahtekârlıklarının tespit edilmesi için [60]'da ATM cihazları tarafından üretilen durum bilgisinin akışına bağlı olarak dizi tabanlı bir anomali tespit modeli önerilmiştir.

Bu tez çalışmasında, diğer çalışmalara benzer olarak sahtekârlık işlemlerinin tespitinde anomali tespiti modellerinin kullanılması önerilmekle birlikte diğer modellerden farklı olarak veri setine konum bilgisinin de dahil edildiği uzay-zamansal bir anomali tespiti modeli sunulmuştur [61].

3.1.4. Birliktelik kuralları ve dizi analizleri

Birliktelik kuralları sık tekrarlanan nesne birlikteliklerini inceleyerek veri içindeki ilişkileri ortaya çıkarır. Birliktelik kuralları şu soruları cevaplamaya çalışır: Hangi

nesneler birlikte satılmış? Güçlü ilişki içindeki nesneler aynı zamanda güçlü korelasyona sahip mi? Büyük veri setlerinde bu kuralları ve desenleri nasıl ortaya çıkarabiliriz? Birliktelik kuralları özellikle pazarlama çalışmalarında çok kullanılmaktadır.

Birliktelik kuralları modellerine zaman faktörünün eklenmesi ile dizi modelleri elde edilir. Dizi modellemede zaman içindeki birliktelikler incelenir ve gerçekleşme sıralarına göre olay dizileri elde edilir. Dolayısıyla bazen anormal ve beklenmeyen olayların tespit edilmesinde de dizi modelleri kullanılır [56].

3.1.5. Müşteri profilleme ve imza tabanlı sahtekârlık tespiti

Literatürde sahtekârlık işlemlerini müşterilere ait davranışsal profiller oluşturarak tespit etmeye çalışan yöntemler de mevcuttur [62]. Bu çalışmalarda temel olarak geçmiş işlemlere ait depolanan veri ile normal müşteri davranışlarına dair bir profil oluşturulur. Her yeni işlem kayıt altında tutulan bu davranışsal profil ile karşılaştırılarak normal davranıştan sapmalar hesaplanır. Oluşturulan normal davranış profilinin tek tek müşteriler için mi yoksa müşteri grupları için mi hesaplanacağı, profillerin her işlemle birlikte güncellenebiliyor olması ve yeni işlemin bu normal davranışa göre farklılığının değerlendirilmesi profil/imza tabanlı sahtekârlık tespiti çalışmalarının temel noktalarını oluşturmaktadır. ATM sahtekârlıklarının tespit edilmesi için yaptıkları çalışmada Klerx, Timo ATM üzerindeki davranışları profilleyerek sıra ve zaman tabanlı anomali tespiti yapılmasını önermişlerdir [63].

Bu tez çalışmasında diğer tüm parametrelere bağlı olarak müşteri profilleri oluşturulabileceği gibi şirketlerin müşterilerinin işlem yaptığı konum bilgisine göre de profiller oluşturulabileceğine dikkat çekilmektedir. Yukarıda anlatılan, sahtekârlık işlemlerinin tespit edilmesi amacıyla kullanılan veri madenciliği teknikleri, EK A'da sunulan tabloda özetlenmiştir.

3.2. Sahtekârlık İşlemlerinin Tespitinde Kullanılan Ticari Ürünler

Sahtekârlık işlemlerinin tespit edilmesine yönelik konumlandırılmış birçok ticari ürün bulunmaktadır. Bu ürünler uluslararası yazılım ürünlerinin sahtekârlık işlemlerinin tespit edilmesi amacıyla özelleştirilmiş ve ilgili fonksiyonların paketlenerek birarada toplandığı formları olabileceği gibi [64, 65, 66, 67]; sadece sahtekârlık işlemlerinin tespitine yoğunlaşmış firmaların ürünleri de olabilir [68, 69].

Ürünlerin çalışma prensibini belirleyen en temel nokta, ürünün gerçek zamanlı çalışmaya elverişli olup olmamasıdır denilebilir. Gerçek zamanlı çalışabilen bir ürünle sahtekârlık işlemleri henüz gerçekleşmeden önlenmesi mümkün olabilecektir. Bununla birlikte sahtekârlık işlemlerinin tespiti için statik kurallarla mı yoksa öğrenebilen dinamik kurallarla mı çalıştığı ayırt edici bir diğer özelliktir. Öğrenebilen bir ürün; sınıflandırma, kümeleme, sosyal ağ analizleri gibi istatistiksel veri modellerinin entegrasyonu zorunlu kılmaktadır. Ürünler için ayırt edici bir diğer özellik de ürünün işlem kanalı veya işlem/ürün tipinden bağımsız çalışıp çalışamaması olacaktır. Örneğin, sadece kredi kartı sahtekârlıkları için tasarlanmış bir ürün diğer kanal ve ürünlerdeki sahtekârlık işlemlerinin tespitinde kullanılamayabilir. Bu tip ürünlerde bulunan veya bulunması beklenen beş temel bileşenden söz edilebilir:

- İşlemler için sahtekârlık işlemi olup olmadığına dair değerlendirme yapacak Kural Motoru/Karar Destek Sistemi
- Belirlenmiş sahtekârlık işlem desenlerinin (iş kurallarının) sisteme entegre edileceği Senaryo Yönetim Aracı
- Sahtekârlık işlemi olup olmadığına dair kontrolü sonuçlanmış işlemlerle ilgili incelemelerin yapılacağı ve aksiyon alınabilecek Olay Yönetim Merkezi
- Geçmişe ve geleceği tahminlemeye dönük veri analizlerinin yapılabileceği Analitik Platform
- Gelişmiş raporlama ve izlemenin yapılabileceği rapor merkezi

Bu bileşenlere sahip bir ürünün ise sadece sahtekârlık işlemlerinin önlenmesinde değil müşteri ilişkileri yönetimi ve pazarlama gibi birçok farklı amaçla kullanılabileceği de açıktır. İş kuralları, karar destek sistemlerinin etkin kullanımları sonucunda firmaların süreçlerinde önemli yer almaktadırlar. Bir iş kuralı, kısa olarak bir işin bir yönünü veya

özelliğini kısa ve öz bir şekilde açıklayan ifadedir [70, 71]. Tarihsel olarak başlangıçta iş kuralları "EĞER-İSE" mantıksal ifadeleriyle geleneksel programlama dilleri ile bilgi teknolojileri tarafından uygulanmıştır. Bugünlerde ise iş kurallarının keşfi, uygulamaya konulması, güncellenmesi ve uygulamadan kaldırılması iş tarafındaki kullanıcılar tarafından gerçekleştirilmekte veya hız kazanmak için iş kullanıcılarının talep ettikleri bir özellik olmaktadır [72]. Kulanıcılar tarafından geliştirilen iş kurallarının birbirleri ile uyuşmazlıklarının olup olmadığı ve gerçekleşen işlemler detayında incelendiğinde anlamlı sonuçlar üretip üretmediği Rete algoritması ve bunun türevleri kulanılarak gerçekleştirilebilmektedir [73]. Modern bir iş kural motorunda Rete algoritmasının bir türevini bulabilmek mümkündür.

3.3. Sektör Uygulamalarının İncelenmesi

Sektörde yasal olmayan işlemlerin tespitine yönelik mevcut uygulamalar ve yazılım ürünleri, çoğunlukla geçmişte yaşanmış tecrübelerle elde edilen kurallara dayanmaktadır. Bu ise hızla gelişen ve sürekli yeni ürünler geliştirip, farklı kanallardan müşterilerine hizmet sunmaya çalışan Türk bankacılık sistemini suistimallere açık hale getirmektedir. Sahtekârlık önleme çalışmaları kapsamındaki banka uygulamaları incelendiğinde mevcut durumda iki farklı dezavantajlı durum öne çıkmaktadır:

- Farklı kanal ve ürünler için farklı firmaların sahtekârlık önleme çözümleri konumlandırılmakta ve bu çözümler arasında herhangi bir entegrasyon bulunmamakta veya
- Belirlenen senaryolar kod içerisine statik olarak yazılarak bankacılık uygulamalarına eklenmekte ve kontroller manuel takip edilmektedir.

Modern bir iş kuralı yönetim sisteminin en önemli faydası iş kurallarının uygulamalar içine kodlanması yerine bu kuralların kural motoru yardımıyla detay seviyede uygulama kodlarından bağımsız olarak uygulamalar içinde kullanılabilecek olmasıdır. Ayrıca iş kurallarının iş kullanıcıları tarafından senaryo yönetim sistemine girilmesi, herhangi bir iş kuralının bir uygulamada kullanılması firmaların bilişim sistemleri personelinden neredeyse bağımsız olarak gerçekleştirilebilir. Elbette böyle bir durum hem iş uygulamalarında kuralların kullanıma hazırlık süresini çok düşürecek hem de

bunun için bilişim sistemleri personeline duyulan ihtiyacı ortadan kaldıracaktır [70]. Sonuç olarak iş kullanıcıları diğer birimlerden bağımsız olarak yeni keşfedilen veya değiştirilen bir iş kuralını uygulamaya alma veya uygulamadan kaldırma işlemini çok hızlı şekilde gerçekleştirebileceklerdir.

Bankacılıkta kullanılmak üzere piyasada yer alan sahtekârlık önleme sistemi ürünleri incelendiğinde ise;

- Kredi kartı ve pos sahtekârlıklarının tespit edilmesinde faydalanıldığı görülen konum bilgisinin, diğer bankacılık işlemlerinde yapılan sahtekârlıkların tespitinde kullanılmadığı,
- Gerçek zamanlı işlem kontrollerinin istenen performansta sağlanamadığı veya ürün/kanal kapsamının yetersiz kaldığı,
- Uluslararası firmalar tarafından geliştirilmiş ve çok yüksek maliyetli olduğu,
- Herhangi bir değişiklik ihtiyacı durumunda firmaya bağlı kalınacak olduğu görülmüştür.

Farklı ülkelerde sahtekârlık işlemlerine dair ulusal düzeyde raporlamalar ve istatistiki veriler kamuoyuyla paylaşılmakla birlikte, birçok ülkede henüz bu düzeyde bir bilgi birikimi de bulunmamaktadır. ACFE'nin uluslarası düzeyde gerçekleştirdiği araştırmalar ve Birleşik Krallık'a ait Ulusal Sahtekârlık Otoritesi (National Fraud Authority, NFA) tarafından yayınlanan raporlar, sahtekârlık işlemlerinin boyutunu gözler önüne sermesi bakımından en önemli kaynakları oluşturmaktadır. Türkiye'de Emniyet Genel Müdürlüğü'ne bağlı Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı her türlü mali suçla mücadele için gerekli önlemleri almaya çalışırken, Maliye Bakanlığı'na bağlı olarak görev yapan Mali Suçları Araştırma Kurulu (MASAK) da kara para aklama faaliyetlerini önlemek amacıyla kurulmuştur. Bununla birlikte Bankacılık Düzenleme ve Denetleme Kurumu'nun (BDDK) Türkiye Bankalar Birliği (TBB) bünyesinde bir çalışma başlattığı da bilinmektedir. Bu çalışma neticesinde bankalar aracı kılınarak gerçekleştirilen dolandırıcılık işlemlerine karşın;

- Ulusal düzeyde oluşturulacak kurumsal bir yapının özellikleri ve çalışma prensiplerinin belirlenmesi

- Bankalar içerisinde dolandırıcılık işlemleri ile mücadele için oluşturulması gereken organizasyonel yapıya dair karar verilmesi
- Bankalar Arası Kart Merkezi (BKM) ve Kredi Kayıt Bürosu (KKB) ile bankalar tarafından dolandırıcılıkları önleme amacıyla yapılan çalışmaların komsolide edilmesi
- Bankalar, BKM ve KKB arasında dolandırıcılık önleme amacıyla bir bilgi paylaşım platformu oluşturulması hedeflendiği bilinmektedir.

Bu amaçla TBB'de sahtekârlıkla mücadele çalışma grupları oluşturulmuş ve tüm bankalardan bu çalışma gruplarına katılım sağlanarak ortak bir irade oluşturulması sağlanmıştır.

Sahtekârlıkla mücadele çalışmaları bu yönüyle incelendiğinde Edge ve Sampaio'nun 2008 yılında yaptıkları çalışmada, sektördeki kuruluşlar arasında sahtekârlık senaryolarının ve diğer gerekli bilgilerin iş birliği çerçevesinde paylaşılabileceği bir servis önerisi sundukları görülmektedir [74]. XML (Extensible Markup Language) servis mimarisinin kullanıldığı sistemde, senaryo tanımlarının ve dağıtımının Edge ve Sampaio (2012)'de detaylı olarak anlatılan dil ile (FFML: Financial Fraud Management Language) sağlanması planlanmıştır [23]. Sahtekârlık işlemleriyle etkin bir şekilde mücadele edilebilmesi için Samakovitis ve Kapetanakis ise finansal kuruluşlar ve düzenleyici kurumlar arasında kolektif bir zekâ oluşmasını sağlayacak bir altyapı önermiştir [75].

BÖLÜM 4. ÖNERİLEN YÖNTEM: KONUM DESTEKLİ SAHTEKÂRLIK TESPİTİ

Tez çalışmasında sahtekârlık işlemlerinin tespit edilmesi amacıyla geliştirilen modelde, entropi kavramı ve konum bilgisinin dahil edildiği veri madenciliği çalışmaları esas oluşturmaktadır. Bu bölümde müşterilerin bulundukları konumun işlem kararları üzerindeki etkisine dair bir giriş yapılacak, entropi kavramı ve kullanım alanları ile konum bilgisi destekli veri analizleri hakkında bilgi verilecek, sahtekârlık işlemlerinin tespiti için geliştirilen model tanıtılacaktır.

4.1. Risk ve Güvenlik Algısı ile Suç Korkusunun Finansal İşlem Kararı Üzerindeki Etkisi

Müşterilerin güven ve güvenlik algıları, tüm markalar için özellikle de müşterilerin kişisel bilgilerini ve paralarını yöneten bankalar için çok önemlidir. Bir ürün satın alan müşteri ile bankacılık gibi bir hizmet satın alan özellikle de fiziksel olarak şubeye gitmeden elektronik olarak hizmet satın alan müşterinin risk algısının farklı olacağı bilinmektedir [76].

Banka müşterilerinin güvenlik ve risk algılarının incelendiği birden fazla raporda, müşterilerin %70'inden fazlasının siber saldırılardan ve kişisel bilgilerini kaybetmekten endişe duyduğu görülmektedir. Endişeli müşterilerle ilgili bu kadar yüksek bir orana bağlı olarak, bir müşterinin elektronik olarak finansal bir işlem yapıp yapmama kararında güvenlik algısının önemli bir rol oynadığı söylenebilecektir [77].

Bankacılıkta alternatif dağıtım kanallarının ilk çıktığı zamanlarda, müşterilerin teknolojik bankacılığı tercih etme nedenleri ve karar verme süreçleri ile ilgili birçok çalışma yapılmıştır [78, 79, 80, 77, 81, 82]. Bu çalışmaların ortak sonuçlarına göre,

güven ve risk algısının elektronik bankacılığın adaptasyonunda temel lokomotif olduğu bulunmuştur. Elektronik bankacılıkta yapılan işlemlerde yaşanabilecek kayıplarla ilgili algılanan risk [83], geleneksel bankacılıktaki kayıplara göre daha yüksek olduğu için, müşterilerin internet bankacılığını kullanmamayı tercih etmeleri hizmetlere güvenmemesine bağlanmaktadır [84]. Kasada yaptığımız bir ödemenin şekline bile karar verirken güvenlik algısı ön plana çıkarken, güvenlik, tamamen sezgisel bir şekilde karar faktörlerimiz arasında yer alır [85].

"Risk algısı" kavramı ilk olarak, algılanan tehlike ve satın alma sırasında ve sonrasındaki algılanan tehlikeler olarak tanımlanmıştır [86]. Tek boyutlu bir kavram olmayan risk algısı, farklı araştırmacılar tarafından farklı şekillerde kategorize edilmiştir. Finansal, fiziksel, güvenlik, zaman, performans, psikolojik ve sosyal riskler tanımlanmış birkaç risk kategorisidir [76]. Sahtekârlık faaliyetleriyle ilgili risk algısı, genel olarak finansal ve güvenlik riskleri şeklinde tanımlanabilir. Finansal riskler, bir ürün veya hizmetin satın almasının sonucunda yaşanabilecek maddi kayıplardan ortaya çıkabilir [87]. Diğer taraftan, güvenlik riski müşterilerin kendi hesaplarından yaptıkları finansal işlemlerle veya kendi özel finansal bilgilerinin kendi izinleri olmaksızın çalınmasından duydukları kuşkuyla ilgilidir [88].

Risk algısıyla ilgili yapılan çalışmalarda, risk algısı üzerinde etkili olan faktörler yedi kategoride toplanmıştır: gönüllülük, kontrol edilebilirlik, doğal yollarla mı yoksa insan eliyle mi ortaya çıktığı, erteleme etkisi, tanıdıklık ve alışkanlık, fayda ve risk-fayda dağılımı, medya etkisi [89]. İnsanlar gönüllü olarak kabul ettikleri, başkalarındansa kendileri tarafından daha kontrol edilebilir olduğunu düşündükleri, kontrol özelliğinden dolayı da doğal yollarla gelişen olaylardaki riskleri daha çok tercih ederler [90]. Risk algısını etkileyen faktörlerden tanıdıklık ve alışkanlık, daha önceden o riskin alınmış olması veya etkilenen kişinin gerçekten o riskin farkında olduğu durumlarda geçerlidir [89]. Teknik olarak risk miktarı aynı seviyede kalsa bile, uzun süredir var olan bir riskin tanıdıklık etkisinden dolayı küçültülerek algınlandığı belirtilmiştir [91]. Tanıdıklık kişilerin korkularını kaybetmesine sebep olurken, bilinmeyen ve yeni riskler insanları daha çok alarm durumuna geçirmektedir. Kişilerin sahtekârlık işlemlerine maruz kalmayla ilgili korkuları da diğer faktörler gibi

tanıdıklık ve alışkanlık faktörleri ile ilişkilidir. Tek bir tanımı olmayan "suç korkusu", bazı insanlarda olan ve diğerlerinde olmayan bir özellik olmaktan çok, geçicidir ve şartlara göre ortaya çıkar [92]. Kişilerin deneyimlerine ve mekansal, sosyal ve anlık durumlara bağlıdır. Yapılan araştırmalarda, müşterilerin elektronik ödeme sistemlerini kullanma seviyeleri ve algılanan risk/güvenlik faktörleri arasındaki ilişkiler incelenmiş, müşterilerin bir ürün veya hizmetle ilgili belli koşullarda hissetiği duyguları tanımlamak üzere "koşullu katılım" kavramı geliştirilmiştir [93]. Koşullu katılım, ürüne veya duruma bağlı ve geçici olma durumudur. Tüm bunlardan yola çıkarak, finansal işlemlerle ilgili de aşağıdaki sorular sorulabilir:

- Müşterilerin finansal bir işlemi yapma veya yapmama kararı, bulundukları yere, zamana ve sosyal koşullara bağlı olabilir mi?
- Müşteriler tanıdık ve alışkın oldukları mekânların dışına çıktıklarında, finansal işlemlerinin durumu ne olmaktadır?
- Evden veya her zaman bulunduğu yerden uzakta bir yerde bulunmak, tanıdık veya alışkın olunmayan bir yerde bulunmak şeklinde değerlendirilebilir mi? Geçici bir durum olan bu koşullarda, müşteri daha az güvenli hissedip, suç korkusu hissi artabilir mi?
- Tanıdık ve alışkın olmayan bir yerde bulunmak, müşterinin finansal işlemlerinin sayısı, parasal büyüklüğü ve sıklığı üzerinde etkili bir faktör müdür?

Tez çalışmasında, müşterilerin kendi tanıdık ve alışkın oldukları her zamanki yerlerinden uzakta olduklarında, geçici bir durum içinde oldukları ve bu geçici durumun finansal işlem kararları üzerinde etkili olduğu varsayımı ile, sahtekârlık işlemlerinin tespit edilip önlenmesinde finansal işlemlerin konum bilgisinin kullanılmasının anlamlılığı ölçülmeye çalışılmıştır. Bu gibi geçici durumlarda, müşterilerin paraları ile ilgili büyük ve önemli kararlar vermeyeceği, çünkü seyahat halinde olmanın algılanan risk ve güvenliği etkileyeceği varsayılmıştır.

4.2. Entropi Kavramı

Düzensizliğin ölçüsü olarak kullanılan entropi terimi, termodinamikten gelir ve ilk defa Clausius tarafından 1850'lerde önerilmiştir [94]. Bilişim teorisine ise bu teorinin yaratıcısı kabul edilen Claude Elwood Shannon tarafından uyarlanmıştır [95]. Bilgi kuramında entropi bir rasgele değişkene bağlı belirsizliği ölçer. Rasgelelik arttıkça entropi değeri artar ve tam tersi olarak rasgelelik azaldıkça entropi değeri düşer. Shannon öz bilgi (self information) olarak adlandırdığı bir nicelikten bahseder. Eğer bir A olayının gerçekleşmesi olasılığı *P(A)* ise, A ile ilgili öz bilgi *i*(*A*) ile ifade edilir ve aşağıdaki formül ile bulunur;

$$i\,(A) = \log_x [1 / P(A)] = -\log_x P(A) \tag{4.1}$$

Bilginin birimi logaritmanın tabanına bağlıdır. Eğer taban 2 ise birim bit'tir, *e* ise birim nat'tır, 10 ise birim hartley'dir. Bu eşitlik bize, yüksek olasılığa sahip mesajların düşük bilgi içerdiğini, düşük olasılığa sahip mesajların ise yüksek bilgi içerdiğini gösterir. Örneğin; "İzmir'de 19 Mayıs günü kar yağacak" mesajı düşük olasılıklıdır, fakat "İzmir'de 19 Mayıs günü güneşli bir hava olacak" mesajına göre daha fazla bilgi vericidir.

Entropi, her sembolün veya semboller kümesinin öz bilgisinin ağırlıklı ortalamasıdır:

$$H = -\sum_{i=1} P(s_i)\, \log_2 P(s_i) \quad (i = 1, 2, ..., n) \tag{4.2}$$

Bu formülde yer alan *n,* kodlanacak mesajda yer alan her bir farklı sembolün sayısıdır. $P(s_i)$ ise *i*. sembolün mesajda bulunma olasılığıdır. Formülden anlaşıldığı gibi mesajın içerdiği bilgi fazlalaştıkça, entropi büyüyecektir [96].

İlişkisel (relative) entropi: Eğer sadece belirsizlik derecesi değil de aynı zamanda varsayılan *(q)* ve gözlenen *(p)* dağılımlar arasındaki değişimler de önemli ise Kullback-Leibler sapması olarak da bilinen ilişkisel entropi kullanılabilir [97]:

$$D_{KL}(p \parallel q) = \sum_{i=1} p(i) \log_a [p(i)/q(i)] \qquad (i = 1, 2, ..., n) \qquad (4.3)$$

Koşullu (conditional) entropi: *Y* değişkenini gözleyerek *X* değişkeni ile ilgili ne kadar belirsizliğin ortadan kaldırıldığı ölçülmek isteniyorsa koşullu entropi kullanılabilir [98]:

$$H_S(X \mid Y) = \sum_{i=1} \sum_{j=1} p(x_i, y_j) \log_a p(x_i|y_j) \qquad (i = 1, 2, ..., n), (j = 1, 2, ..., m) \qquad (4.4)$$

Lee ve Xiang yaptıkları çalışmada, denetim verisi üzerinde kullanılan anomali tespit modellerini değerlendirmek için entropi, koşullu entropi ve ilişkisel koşullu entropi kullanmışlardır [99]. Berezinski ve diğerleri de ağ üzerindeki kötü amaçlı yazılımları tespit etmek için entropi tabanlı bir anomali tespiti modeli önermişlerdir [100]. Zhou ve diğerleri ise çalışmalarında entropinin finans alanındaki uygulamaları ile ilgili bir literatür taraması sunmuşlardır. Ayrıca çalışmada entropi türleri olan Shannon Entropi, Tsallis Entropi, Kullback Cross Entropi, Tsallis Relative Entropi, Bulanık (Fuzzy) Entropi, Renyi Entropi ve Havrda-Charvat Entropi hakkında bilgi verilmiştir. Buna göre finans alanında entropinin;

- Portföy seçim,
- Varlık değerleme,
- Risk ölçümü,
- Opsiyon fiyatlama problemlerinin çözümünde kullanıldığı belirtilmiştir [101, 102].

4.3. Konum Destekli Veri Analizleri

Konum destekli veri analizlerinin en çok kullanım alanlarından biri, fotoğraf paylaşım sitelerindeki kullanıcılar tarafından yüklenen fotoğraflar hakkındaki veriyi analiz ederek çıkarımlar yapmaya çalışmaktır [103]. Zheng ve diğerlerinin yaptığı ve benzeri birçok çalışmada da belirtildiği gibi, bu tip fotoğraf verileri üzerindeki konum bilgisi ile aynı zamanda turistlerin gezi rotalarına dair hesaplamalar yapmak için de kullanılabilmektedir [104]. İklim [105] ve bulaşıcı hastalıkların yayılması [106] verilerinin kullanıldığı uzay-zamansal (spatio-temporal) analizlerin yanısıra, konum

bilgisi ile etiketlenmiş fotoğrafların analizi en yaygın yöntemlerden biridir. Bu tip analizler ile sosyal ağ sitelerindeki kullanıcıların seyahat desenleri [107], kullanıcılar tarafından izlenen rotalar [106] ve ilgi alanları ile ilgili anlamlı sonuçlar üretilebilmektedir. Bu analizlere benzer şekilde kullanıcıların konum tabanlı davranışsal analizlerinin yapılması da mümkündür. [107]'de ilgi alanlarını oluşturmak için yoğunluk tabanlı bir kümeleme algoritması ve sonrasında ilgi noktaları arasındaki ilişkilerin analizi için de birliktelik kuralları kullanılmıştır. Sahtekârlık işlemlerinin tespit edilmesi için konum bilgisinin kullanılmasına dair tek çalışma, Sarvar Patel'in çalışmasıdır [108]. Patel bu çalışmada, mobil iletişim ve kablosuz ağlar üzerindeki sahtekârlıkların tespit edilmesi için yasal olan görüşmelerin konumlarının takip edilmesini ve böylece yasal olmayan işlemlerin kolayca fark edilebileceğini önermektedir. Konum bilgisinin sürekli elde edilebilirliği ise çözülmesi gereken bir nokta olarak belirtilmiştir [108].

Europol ve EAST, Avrupa Birliği'nde bankacılık sektörü 2008'de Europay, MasterCard ve Visa (EMV)'ya geçtikten sonra Avrupa Birliği içindeki yasal olmayan işlemlerin sayısında ciddi bir düşüş olduğunu rapor etmiştir. Fakat bununla birlikte Avrupa Birliği dışındaki ülkelerdeki yasal olmayan işlemlerin sayısı da hızlı bir şekilde artmıştır. Amerika bu ülkelerin başında gelirken, Endonezya ve Tayland'da da yasal olmayan işlemler artmıştır. Bu durumla mücadele etmek için Europol ve Avrupa Merkez Bankası tarafından önerilen ve *GeoBlocking* ismi verilen, kartların çip ve pin doğrulaması yapılmayan bölgelerde kullanımını kısıtlayan bir yöntem geliştirilmiştir. Güvenlik açısından oldukça faydalı gözüken bu yöntem, kart sahipleri için EMV uyumlu olmayan bölgelere her seyahatleri öncesi kartlarını aktive etmeleri gerektiği anlamına gelmektedir [22].

Tez çalışmasında önerilen yaklaşım ise konum, zaman etiketlerine sahip ve tarihsel olarak sıraya dizilmiş müşteri bankacılık işlemleri üzerinde uzay-zamansal anomali tespiti ile sahtekârlık işlemlerinin tespit edilmeye çalışılmasıdır. Çalışma kapsamında özel bir banka aracılığıyla Türkiye'de gerçekleştirilen bankacılık işlemleri incelenmiş olup, [107] 'dekine benzer şekilde problemi iki boyutlu olarak ifade edebilmek için Türkiye haritası gridlere bölünmüştür. Bu işlemden sonra anomali tespiti, birliktelik

kuralları ve dizi analizleri gibi analizler yapılabilir hale gelmiştir. Böylece tüm Türkiye üzerindeki gridler arası ilişkiler, ilgi noktaları arasındaki zamansal ilişkiler ve böylece işlemler arasında şüpheli olabilecekler tespit edilebilmiştir.

Müşterilerin bankacılık işlemleri açısından davranışları harita üzerinde incelenmiş, mobilite hesaplamalarının yapılabilmesi amacıyla her müşteri için entropi değeri hesaplanmış ve mobilite ölçülerine göre müşteri sınıfları oluşturulmuştur. Daha sonra müşterilerin işlemleri tarihsel olarak sıraya dizilmiş ve bir önceki işlemden mevcut işleme yani bir önceki konumdan mevcut konuma geçişleri gösteren veri seti oluşturulmuştur. Her geçiş için hız değeri hesaplanmış ve bundan sonra müşteri sınıfları için şüpheli işlemlerin tespit edilebilmesini sağlayacak iş kurallarını verecek birçok anomali tespit tekniğinin kullanımına hazır hale gelmiştir.

4.4. Geliştirilen Model

Gözetimli, gözetimsiz ve davranışsal birçok modelin sahtekârlık işlemlerinin tespiti amacıyla kullanılabileceğinden önceki bölümlerde bahsedilmişti. Bu tez çalışmasında dikkat çekmek istediğimiz nokta ise diğer parametrelere bağlı olarak kullanıcı profilleme yapıldığı gibi, şirketlerin müşterilerini işlem yapma lokasyonlarına göre de gruplayabileceğidir. Ayrıca, diğer anomali tespit yöntemleri gibi, konum tabanlı anomali tespit yöntemleri de geliştirilebilecektir.

$N = \{n\}$ olmak üzere bir finansal işlemler kümesi verildiğini düşünelim. Bu kümedeki işlemlerin yapıldığı konum bilgisini de dahil ederek konum etiketli işlemler kümesini oluşturabiliriz. İşlemlerin konum bilgisinin elde edilmesini daha kolay sağladığı için öncelikle ATM'den yapılan işlemler dikkate alınabilir. ATM'den yapılan bir işlemin konumu ATM'nin enlem ve boylam değerleri ile elde edilebilir. Olasılıkları ve dolayısıyla entropi değerlerini hesaplamak için sürekli olan enlem ve boylam değerlerinin kesikli hale getirilmesi gerekmektedir. Bu amaçla ATM'lerin yer aldığı Türkiye haritası üzerindeki alan 19×57 ebatlarındaki gridlere bölünmüştür. Böylece finansal bir işlem (U_i, H_i, L_i, t_i, g_i) değişkenleri ile ifade edilebilmiştir;

- U_i i işleminin tekil işlem numarasını,
- H_i i işlemini yapan banka kart sahibi numarasını,
- L_i enlem ve boylam olarak i işleminin yapıldığı konum bilgisini,
- t_i i işleminin yapıldığı zaman bilgisini,
- g_i i işleminin yapıldığı konumun grid numarasını göstermektedir.

Bu değişkenlerden oluşan veri kümesi, kart sahibinin yaptığı işlemlerin ardışıklığına göre $<n_1,...,n_z>$ şeklinde yeniden organize edilebilir. Bir *i* işleminin konum bilgisi kartezyen koordinatlar (x_i, y_i) şeklinde gösterildiğinde ise, bir kart sahibinin işlemleri için $ST= (x_1, y_1, t_1, g_1),...,(x_z, y_z, t_z, g_z)$ uzay-zamansal işlem dizisi elde edilir.

4.4.1. Entropi ile banka müşterilerinin mobilitelerinin hesaplanması

Müşterilerin hesap hareketlerine, demografik bilgilerine ve diğer bazı hizmet kullanım bilgilerine göre gruplanmasının oldukça yaygın olduğu bilinmektedir. Dolayısıyla para transferlerinin, fatura ödemelerinin ve diğer finansal aktivitelerin büyüklüğü ve sıklığı gibi bazı desenlerin elde edilmesi için banka müşterilerinin hesap hareketlerinin kullanılması da doğaldır. Bununla birlikte, bu tez çalışmasında önerilen ise müşterilerin hareketlerine ilişkin bazı uzay-zamansal kurallar elde edebilmek için (finansal işlemlerin yerleri gibi) konum bilgisinin kullanılmasıdır. Bunu yapmanın kolay bir yolu ise müşterilerin mobilite derecelerine göre gruplanması olabilir. Mobilitesi yüksek müşteriler için evlerinden veya iş yerlerinden çok uzak yerlerde finansal işlem yapmaları şüpheli bir durum oluşturmazken, bulunduğu yeri nadiren değiştiren müşteriler için bu gibi durumlarda ilave doğrulayıcı önlemler alınması faydalı olabilecektir. İş bakış açısıyla bakıldığında da her müşteri için favori ATM, şube ve hatta şehir bilgisinin çıkarılması ve kullanılması yoluna gidilebilir. Buradaki temel düşünce, müşterilerin her zaman bulundukları rahat bölgelerin dışındayken nadiren yüksek tutarlı finansal işlem yapacağı savıdır.

Birliktelik kuralları ve dizi madenciliği ile elde edilecek sonuçlar farklı konumlarda ATM kullanımı ile ilgili anlamlı bilgiler verecek olsa da ATM kart sahiplerinin işlem sıralarına göre mobilite desenlerini analiz edebilmek için daha farklı istatistiklere

ihtiyaç duyulmaktadır. Olasılıksal bakış açısı ile, mobilite düzensizliğinin artması, yüksek entropili kart sahiplerinin coğrafi-mekansal olasılık dağılımına işaret etmektedir. Bu nedenle, aşağıda gösterildiği şekilde hesaplanan Bilgi Teorisi'ndeki [96] Shannon entropisi kulllanılacaktır;

$$e = -\sum p_i \times log\, p_i \qquad (i= 1, \ldots, k) \qquad (4.5)$$

Burada p_i, finansal bir işlemin *i* gridinde gerçekleşme olasılığını göstermektedir. p_i olasılığı, her bir kart sahibinin *i* gridinde gerçekleştirdiği finansal işlemlerin sayısının, o kart sahibinin tüm finansal işlemlerinin sayısına bölünmesiyle tahmin edilir. p_i değerlerinden sonra tüm kart sahipleri için entropi değerleri elde edilebilir. Böylece kart sahiplerinin entropi değerleri ışığında bazı desenler ortaya çıkacak ve müşteriler mobilite değerlerine göre gruplanabilecekir.

4.4.2. Konum bilgisi eklenmiş bankacılık işlemlerinin markov süreci olarak analizi

Müşteri hareket istatistiklerinin analizi için, müşterinin hareketleri Markov zincir modeli ışığında, ATM'lerde yapılan işlemlerin bir dizisi şeklinde ifade edilebilir. Markov zincir modeli uzay-zamansal hareketlerin ve sıra takip eden olayların analiz edilmesinde yaygın olarak kullanılır. Markov zincirlerindeki birinci dereceden bağlılık özelliği ile farklı gridlerde arka arkaya iki işlem yapmış müşterilerin istatistikleri hesaplanabilir. Tüm kart sahipleri için daha önce oluşturulmuş olan uzay-zamansal *ST* işlem dizisi ile $(L_{i-1}, L_i, d, t, s, e_h, C_h)$ geçiş (transition) veri kümesi oluşturulabilir;

- L_{i-1} ve L_i, *(i-1)* ve *i* işlemlerinin gerçekleştirildiği grid merkezinin veya ATM'nin koordinatlarını,
- *d*, *(i-1)* ve *i* işlemlerinin gerçekleştirildiği noktalar arasındaki uzaklığı kilometre (km) cinsinden,
- *t*, *(i-1)* ve *i* işlemlerinin gerçekleştirildiği zamanlar arasındaki süreyi dakika (dk) cinsinden,
- *s*, *(i-1)* ve *i* işlemleri arasındaki bu geçişin hızını,

- e_h, h kart sahibinin entropi değerini ve
- C_h, h kart sahibinin entropi değerinin ait olduğu müşteri grubunu göstermektedir.

İşlemlerin gerçekleştirildiği konumlar arasındaki öklit uzaklığı, doğrudan ATM'lerin koordinatlarının veya grid merkezlerinin koordinatlarının uzaklıkları dikkate alınarak hesaplanabilir. Hız hesaplamasının yapılması ile de hem konum hem de zaman bilgisi pratik bir şekilde ifade edilmiş olacaktır. Diğer bir deyişle, hız değişkeni mobilitenin önemli bir göstergesi olacak ve entropi ile birlikte dikkate alındığında kart sahiplerinin konumlarını değiştirme desenleri ile ilgili bilgi verecektir. D, T ve S değerleri aşağıdaki gibi hesaplanacaktır:

$$D = \{|(x_i,y_i)-(x_{i-1},y_{i-1})|\ \mathrm{Euc}\},\ i \in 2,...,z \tag{4.6}$$

$$T = \{t_i - t_{i-1}\},\qquad i \in 2,...,z \tag{4.7}$$

$$S = D/T \tag{4.8}$$

İstatistiksel bakış açısıyla, kart sahiplerinin hareketleri bağımsız stokastik rassal süreç olarak modellenmektedir. Stokastik sürecin durum uzayı, boş olmayan yani en az bir adet ATM içeren gridlerin kümesidir. Kart sahiplerinin hareketlerini temsil eden bu stokastik süreç, bir sonraki durum değerinin sadece mevcut durum değerine bağlı olup daha önceki durumların değerlerine bağlı olmamasıyla bir Markov zincir olarak kabul edilebilir. Markov zinciri modelinde, durum uzayındaki her bir hareket bir adım olarak isimlendirildiğinden, kart sahiplerinin her bir hareketi bir adımdır.

Her finansal işlem bir birim zaman adımından sonra gerçekleştiğinden, kart sahiplerinin işlemlerinden oluşan stokastik süreç, kararlı kesikli bir Markov zinciri olarak modellenmektedir. Böylece i gridinden j gridine geçiş olasılığı, j gridinde gerçekleşmiş ve bir önceki işlemi de i gridinde gerçekleşmiş işlemlerin sayısı ile tahmin edilebilir. Bu geçişlerin frekanslarının hesaplanmasıyla anomalilere işaret eden nadir geçişlere ulaşılabilecektir.

4.4.3. Kümeleme ve anomali tespiti ile şüpheli işlemlerin bulunması

Yukarıdaki Markov istatistiklerine ek olarak, geçiş anomalilerini farklı istatistiksel yöntemlerle keşfetmek de mümkündür. Muhtemelen en basit istatistiksel anomali tespit yöntemlerinden biri, grafiksel bir görsel sunan ve bireylerin görsel olarak anomalileri tespit etmesine imkân sağlayan kutu grafiği yöntemidir. Bizim veri setimizde, kart sahiplerine ait olan tüm entropi sınıfları için hız değerlerine göre kutu grafikleri oluşturulacaktır. Yaygın olarak kullanılan diğer bir anomali tespit yöntemi de 4σ limitlerini kullanarak, standart sapmanın 4 katından daha fazla bir sapma gösteren değerlerin anomali kabul edilmesidir. Bu yöntem de kart sahiplerinin entropi sınıflarına göre geçiş işlemlerinin hız değerleri *(s)* için uygulanabilir. Daha anlamlı sonuçlar üretmek için sıfıra eşit olan hız değerleri hariç tutulabilir.

Bu temel anomali tespit yöntemlerinin yanısıra, geçiş veri seti üzerinde kümeleme çalışması yapılması uç değerler gösteren geçişlerin yani şüpheli işlemlerin keşfedilmesi için iyi bir yöntem olabilir. Etiketlenmemiş veri seti altında gizlenmiş yapıyı keşfetmek, hipotezler geliştirmek ve anomalileri tespit etmek için kullanılan kümeleme, gözetimsiz bir makine öğrenmesi tekniğidir. Geçiş veri seti içerisindeki gözlemlerin ise Markov özelliğinden dolayı birbirinden bağımsız olduğu, yani mevcut durumun geçmiş ve gelecek diğer durumlardan bağımsız olduğu varsayılabilir. Bu varsayım ile geçiş veri seti gözetimsiz bir algoritma için, bir başka deyişle anomali tespiti amacıyla gruplanmak için çok uygun hale gelmektedir. Geçiş veri setindeki mobilite ölçümlerinin kümelenmesi için, gruplara ayırmaya dayalı olan ve veri setini k adet kümeye bölerek gruplar oluşturan k-means ve k-median kümeleme algoritmaları kullanılmıştır. Uygulanması, anlaşılması ve büyük veri setleri üzerindeki uygulama kolaylığı nedeniyle en yaygın kullanılan kümeleme algoritmaları k-means ve k-median'dır. k küme sayısı kullanıcı tarafından belirlenir ve her kümenin kütle merkezi ismi verilen kendine ait merkezi bir noktası vardır. Uzaklık d, hız s ve entropi e değerleri kümeleme algoritmamızın girdilerini oluşturmaktadır. Algoritma uygulanmadan önce veri seti eğitim ve test amaçlarıyla ikiye ayrılmıştır. Algortimalar uygulanıp geçiş kümeleri oluşturulduktan sonra, küme merkezleri ve kümelerin üye sayılarının incelenmesiyle aykırı kümeler tespit edilebilecektir. Böylece anormal

değerlere sahip olan işlemlere ulaşılabilecek ve konum tabanlı şüpheli işlem kuralları elde edilebilecektir. Sahip oldukları entropi değerlerine göre gruplanmış olan kart sahiplerinin her bir grubu için farklı kurallar uygulanabilecek, bankacılık işlemleri bu kuralların kontrollerinden geçirilerek sahtekârlık vakaları önlenebilecektir.

BÖLÜM 5. ÖNERİLEN YÖNTEMİN BİR TÜRK BANKASINDA UYGULANMASI

Müşterilerin ATM kullanımlarına ilişkin orta ölçekli bir Türk bankasından elde edilen gerçek bir veri seti üzerinde yapılan keşfedici analiz sonuçlarının sunulacağı bu bölümde, öncelikle veri seti tanıtılacak ve veri seti üzerinde yapılan ön hazırlık çalışmaları ile konum bilgisinin analizlere dahil edilmesi ile elde edilen sonuçlar anlatılacaktır.

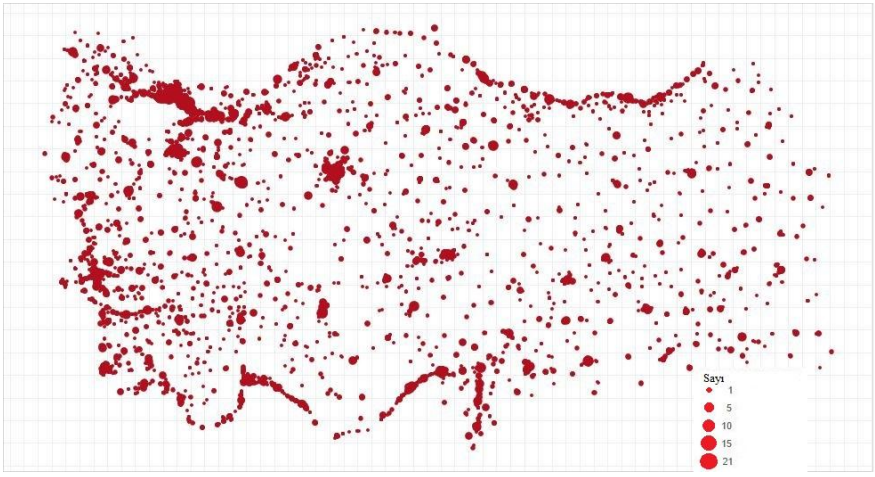
ATM sahtekârlıkları ile ilgili temel problem ATM kartlarının veya kart bilgilerinin suistimal edilmesi olduğu için, ATM kullanımlarındaki sahtekârlık tespiti problemi de büyük ölçüde kartın geçerliliğinin belirlenmesine dönüşmektedir. Bu tez çalışmasının temel amacı, bankacılıktaki ve özellikle de ATM'lerdeki finansal işlemlerin sahtekârlık işlemi olup olmadığının tespit edilmesinde işlemlerin konum bilgisinin dikkate alınmasının katkılarının incelenmesidir. Sahtekârlık işlemlerinin tespit edilmesi ve önlenmesi amacıyla hâlihazırda bankalarda kullanılmakta olan iş kuralları içerisine konum bilgisi ile ilgili kuralların eklenmesinin, sahtekârlık tespitindeki performansı artıracağı varsayılmıştır. Yapılan literatür ve piyasa araştırmalarında, özellikle bireysel bankacılık uygulamalarında sahtekârlık tespiti amacıyla işlemlerin konum bilgisinin dikkate alındığı bir çalışmaya rastlanmamıştır.

5.1. Veri Seti ve Hazırlık İşlemleri

Konum bilgisinin değerini ölçmek için, bankacılık hizmetlerinin kullanımında konuma bağlı bir desen olup olmadığının ve bu desenlerden iş kuralları elde edilip edilemeyeceğinin incelenmesi gerekmektedir. Bu amaca hizmet edecek en uygun tarihsel veriyi ise ATM işlemleri sunmaktadır. ATM'lerden nakit para yatırma çekme işlemlerinin yanı sıra para transferleri, fatura ve vergi ödemeleri, kontör yükleme gibi

birçok finansal işlem yapılmaktadır. Tez çalışmasında kullanılan veri seti, Türkiye'deki orta ölçekli bir bankanın müşterilerinin Kasım 2012 ve Kasım 2014 tarihleri arasında ATM'lerden yaptıkları finansal işlemleri içermektedir. Veri seti içerisinde 987.813 adet birbirinden farklı ATM kartından, Türkiye'deki tüm ATM'lerden yapılan 21.678.588 adet finansal işlem bulunmaktadır. İşlem bilgilerinin yorumlanabilmesi için ihtiyaç duyulan Türkiye'deki tüm bankalara ait olan ATM'lerin listesi ve konum bilgileri Bankalararası Kart Merkezi'nden (BKM) elde edilmiştir. ATM listesinin ve konum bilgilerinin finansal işlem veri seti ile birleştirilmesiyle birlikte işlemlerin konum bilgilerine ulaşmak mümkün olmuştur.

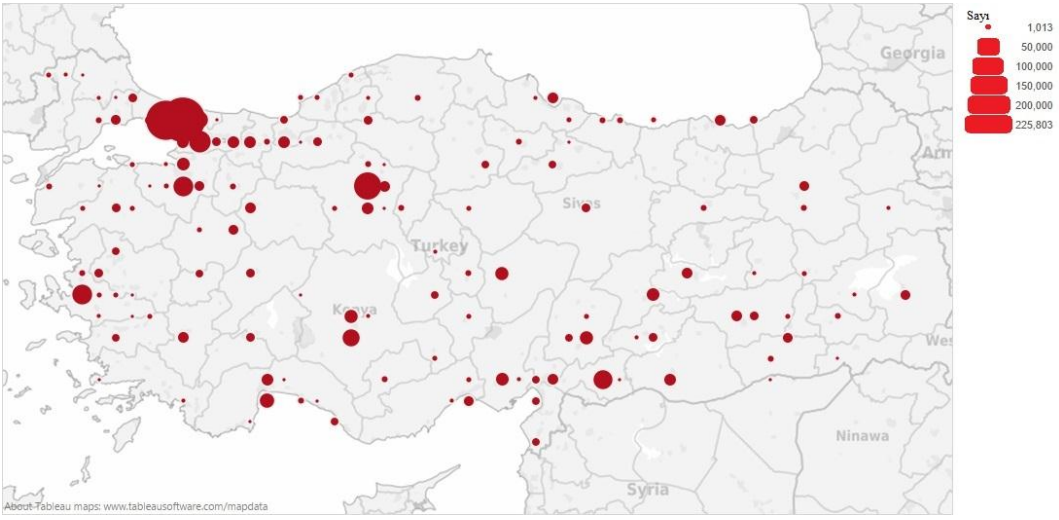
Türkiye'de yerleşik 42.000'den fazla ATM bulunmaktadır. Kuzey Kıbrıs Türk Cumhuriyeti'nde bulunan ATM'ler kapsam dışı bırakılmıştır. Aralık 2014 tarihi itibariyle güncel ATM verilerini içeren veri setinde yerleri değiştirilmiş veya kaldırılmış ATM'lerin bilgisi bulunmamakta, sadece aktif ATM'ler ve konum bilgileri yer almaktadır. Bazı genellemeler yapabilmek için, konum bilgisinin kesikli hale getirilmesi gerekmektedir. Böyle bir veriyi kesikli hale getirmenin yollarından birisi ise iki boyutlu uzaysal bir grid oluşturmaktır. Bu amaçla 0,33333◦×0,33333◦ çözünürlüğe sahip iki boyutlu uzaysal bir grid oluşturulmuştur. Böylece Türkiye haritası üzerindeki alanda 19×57= 1083 adet grid karesi elde edilmiştir. Bu karelerin 668 adedinde en az 1 adet ATM bulunmaktadır. ATM'lerden yapılan işlemler harita üzerine yerleştirildiğinde ise 660 farklı karede işlem yapılmış olduğu görülmüştür. Şekil 5.1.'de ATM'lerin grid karelere bölünmüş Türkiye haritası üzerindeki görünümü verilmektedir.



Şekil 5.1. Türkiye'deki ATM'lerin harita üzerinde görünümü

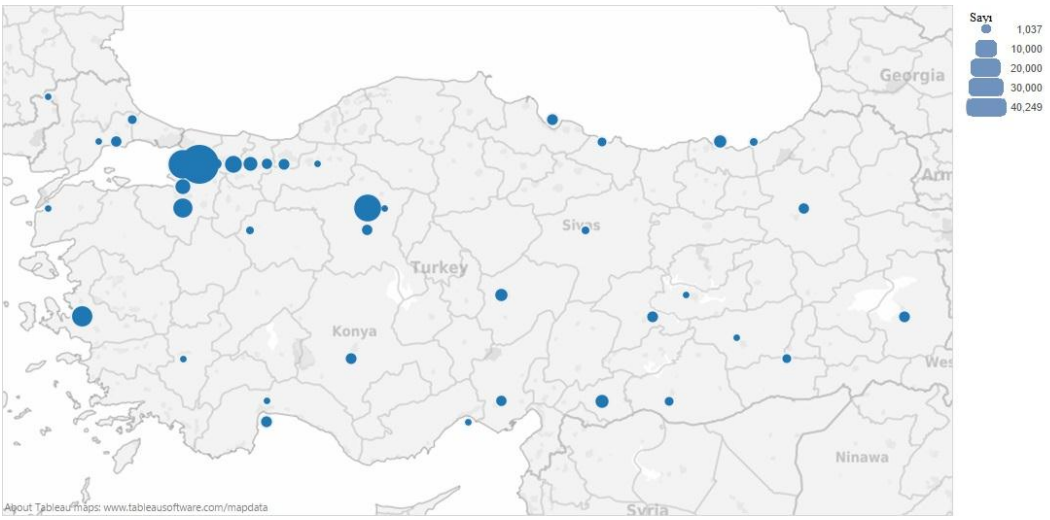
5.2. Bankacılık İşlemlerinin Konum Bilgisi ile Analizi

Finansal işlemler verisini yorumlamak için yapılabilecek çalışmalardan bir tanesi işlemlerin gerçekleştirildiği grid kareleri arasındaki birliktelik ilişkilerinin incelenmesidir. Birliktelik analizi yapılabilmesi için finansal işlemler verisi SAS Enterprise Miner aracılığıyla dikey formata dönüştürülmüştür. Finansal işlemler verisinde yer alan işlemlerin konum bilgisi ile grid koordinatları eşleştirilerek işlemlerin gerçekleştirildiği grid kareleri tespit edilmiştir. Bundan sonra birbiriyle ilişkili grid karelerinin bulunması için ATM işlemlerini içeren bu veri seti analiz edilebilecektir. Birliktelik analizi yapılırken bir grid karesinde birden fazla işlem yapılmışsa da sadece tek bir işlem hesaplamaya katılmış, tekrarlı ATM ziyaretleri dikkate alınmamıştır. Bu nedenle veri seti içerisinde bir ATM kartının bir grid karesinde sadece bir tek işlemi bulunabilecektir. Bunun sonucunda finansal işlemlerin bulunduğu veri setindeki kayıt sayısı 1.596.713'e düşmüştür. Eşik değeri 1000 olarak belirlendiğinde, yani en az 1000 farklı kart sahibi tarafından ziyaret edilmiş grid kareleri incelenmek istendiğinde, bu koşullara uyan 137 grid karenin bulunduğu görülmüştür. Şekil 5.2.'de gösterilen bu gridlerin sık kullanılan grid kareler olduğu söylenebilir. Şekilden anlaşılabileceği gibi, grid merkezleri ilgili gridde gerçekleşen işlem sayısı ile doğru orantılı olacak şekilde işaretlenmiştir.



Şekil 5.2. Sık kullanılan grid kareler

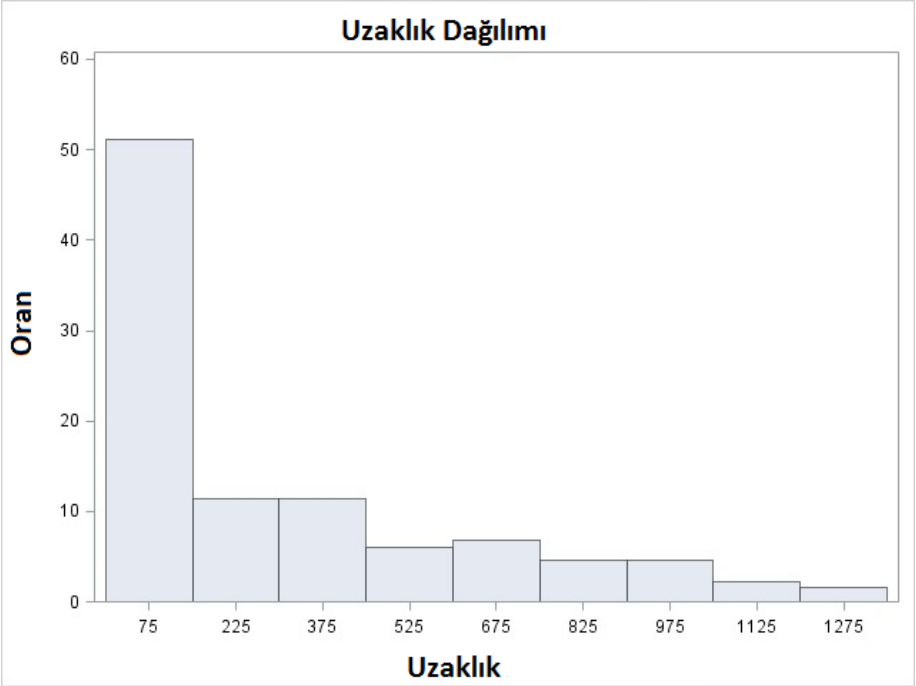
Grid karelerin birbirleri ile ilişkileri incelendiğinde ise, Türkiye'nin en büyük şehri olan İstanbul'un, diğer gridlerle en çok ilişkiye sahip olduğu tespit edilmiştir. Şekil 5.3.'de İstanbul ile ilişkili olan grid kareler gösterilmektedir. Benzer şekilde, gridlerin işaret büyüklüğü, İstanbul ile ilişkilerinin yoğunluğuyla orantılıdır. İstanbul içerisine 12 farklı grid bulunmakla birlikte, gösterimin daha belirgin olması açısından İstanbul içindeki tüm gridlerin ilişkili olduğu gridler şekilde yer almaktadır.



Şekil 5.3. İstanbul ile ilişkili olan grid kareler

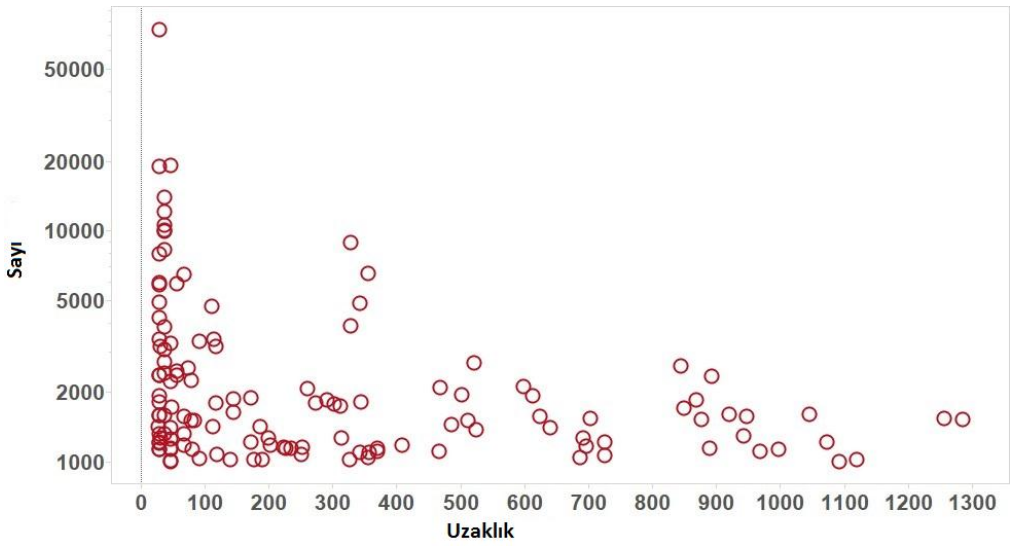
Türkiye'nin en doğusundaki illerin bulunduğu gridlerin bile İstanbul ile ilişkili olduğu görülmektedir. Bunda kuşkusuz İstanbul'un birçok ilden göç almış olmasının etkisi büyüktür denebilir. İstanbul dışında Ankara ve İzmir gibi büyük şehirlerin de Türkiye'de birçok şehirle ilişki içinde olduğu söylenebilir. Bununla birlikte, birbirine yakın olan küçük şehirlerin bile birbirleri ile ilişkisi bulunmaktadır.

İlişki analizlerine ek olarak, birbirleriyle ilişkili olan grid kareler arasındaki uzaklıkların hesaplanması da anlamlı sonuçlar doğurabilecektir. Bu değerlerin elde edilmesi amacıyla ikili ilişkiler dikkate alınmış ve SAS'ın GEODIST fonksiyonu kullanılarak grid karelerin birbirlerine uzaklıkları hesaplanmıştır. Buna göre 131 adet ikili ilişki içinde grid kare tespit edilmiş ve bunlar arasındaki uzaklıklar hesaplanarak Şekil 5.4.'deki histogramda sunulmuştur.



Şekil 5.4. İlişkili grid kareler arasındaki uzaklığın dağılımı

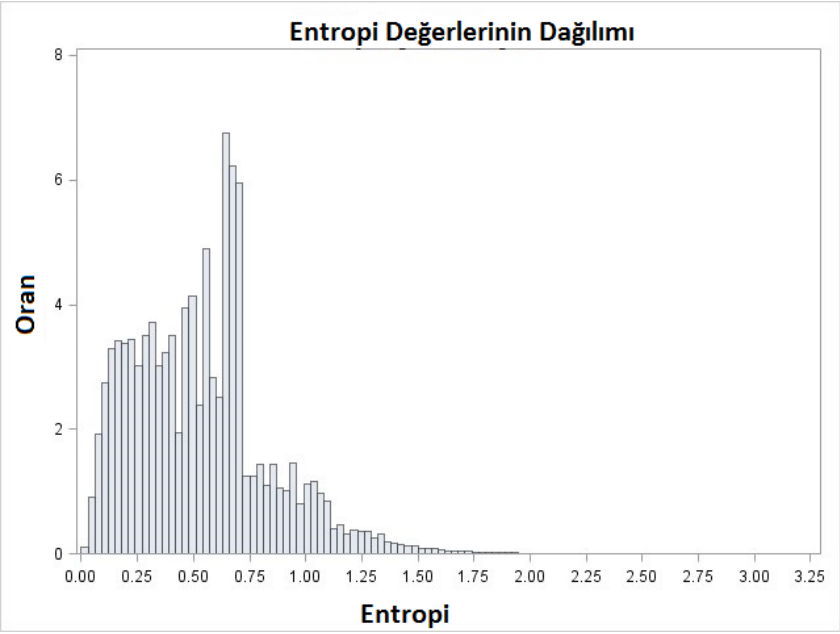
Histogramdan görüleceği gibi birbirine yakın grid kareler arasında daha çok ilişki bulunmuştur. Aslında ilişkili grid karelerin çoğunluğu arasındaki uzaklığın 75 kilometre veya daha küçük olduğu görülmektedir. Daha net görülmesi için ikili ilişkide olan grid karelerin ilişki sayılarının uzaklığa bağlı olarak sayıları Şekil 5.5.'de verilmiştir.



Şekil 5.5. İkili ilişkideki grid karelerin uzaklığa bağlı olarak sayısı

5.3. Geliştirilen Model ile Sahtekârlık Tespit Kurallarının Bulunması

Yukarıdaki bölümlerde anlatıldığı gibi, konum bilgisi dahil edilerek sahtekârlık işlemlerinin tespit edilmesini sağlayacak iş kurallarının bulunmasını amaçlayan çalışmamız birkaç adımdan oluşmaktadır. İlk etapta her müşteri için mobilite derecesini gösteren entropi değeri hesaplanmıştır. Her müşterinin farklı grid karelerde finansal işlemi olabilir. Bir işlemin *i* gridinde yapılmış olma ihtimali, p_i, bir müşterinin *i* gridinde yaptığı işlemlerin sayısının o müşterinin tüm gridlerde yaptığı işlemlerin sayısına bölünmesi ile hesaplanmıştır. Bu olasılık değerleri hesaplandıktan sonra SAS'ın TRANSPOSE prosedürü kullanılarak her müşteri (kart sahibi) için entropi değeri hesaplanabilmiştir. Veri seti içerisinde 987.813 adet kart sahibi bulunduğu belirtilmişti. Kart sahiplerinin tamamı için yapılan entropi hesaplamasından çıkan sonuçlara göre kart sahiplerinin %62,2'si her zaman işlem yaptıkları gridler dışında hiçbir gridde işlem yapmamıştır. Yani müşterilerin %62,2'si 0 entropi değerine sahiptir. Sadece İstanbul içerisinde 12 adet grid bulunduğu dikkate alınırsa, grid ebatlarının çok büyük olmadığı, ancak müşterilerin yaşam alanlarına yakın yerlerde kalmayı tercih ettiği görülmektedir. Şekil 5.6.'da 0'dan farklı olan entropi değerlerinin dağılımı görülmektedir.



Şekil 5.6. Sıfırdan farklı olan entropi değerlerinin dağılımı

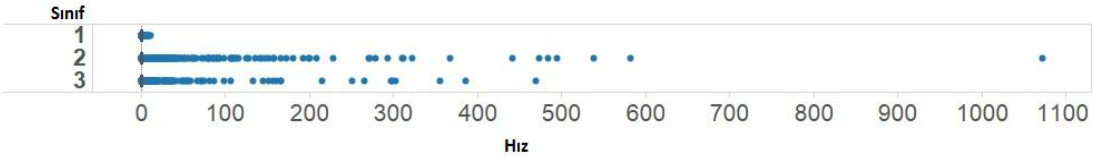
Entropi değeri müşterilerin mobilite derecelerini göstermesi bakımından önemli bir göstergedir. Temel olarak bu değerler bazı müşteri sınıfları oluşturmak için kullanılabilir. İlk grup kuşkusuz bulundukları gridi hiç değiştirmeyen, 0 entropi değerine sahip olan müşterilerden oluşmaktadır. Diğer gruplar için Şekil 5.6. analiz edilmiş, 0,75 değeri kesme noktası olarak kullanılarak iki farklı müşteri sınıfı daha oluşturulmuştur. Böylece, 0 entropi değerine sahip olan, 0 ile 0,75 arasında entropi değerine sahip olan ve 0,75'den büyük entropi değerine sahip olan müşteriler olmak üzere üç farklı müşteri sınıfı elde edilmiştir.

Entropi değerleri, orjinal finansal işlem veri setine işlemin gerçekleştiği grid bilgisinin eklenmesi ile oluşan veri seti kullanılarak hesaplanmıştır. Geçiş veri setinin elde edilmesi için, SAS'ın LAG fonksiyonu ile veya SQL kullanılarak nereden-nereye bilgisinin eklenmesi gerekmektedir. Bu adımdan sonra 20.690.775 kayıt içeren bir veri seti oluşmuştur. Nereden-nereye bilgisinin eklendiği bu veri setine bağlı olarak hesaplanabilecek uzaklık bilgisi için doğrudan ATM'lerin konumları dikkate alınabileceği gibi ATM'lerin bulunduğu gridlerin konumları da dikkate alınabilir. Uzaklık değerleri hesaplandıktan sonra, zaman bilgisi de dikkate alınarak hız bilgisi elde edilebilmiştir. Böylece uzaklık, hız ve müşterilerin entropi bilgisinin de eklenmesiyle yeni bir veri seti oluşturulmuştur. Tablo 5.1.'de bu veri setinde yer alan değişkenlere ait ortalama, standart sapma ve uç değer limitlerinin değerleri görülmektedir. Buradaki entropi değeri müşteri (kart sahibi) ile ilgili olup, geçişin (hareketin) bir göstergesi olmadığı için anomali tespitinde kullanılması uygun olmayacaktır.

Tablo 5.1. Özet istatistikler ve uç değer limitleri

Değişken	μ	σ	$\mu + 4\,\sigma$
Uzaklık (km)	46,75	151,57	653,03
Hız (km/dakika)	0,01	0,99	3,97
Entropi	0,37	0,39	1,93

Şekil 5.7.'de müşterilerin entropi sınıflarına ait hız değerlerinin grafiği verilmiştir. Uç değerler grafik üzerinde açık bir şekilde görülebilmektedir. Grafiğin anlamlı olabilmesi için 0 hız değerine sahip olan geçişler grafiğe dahil edilmemiştir.

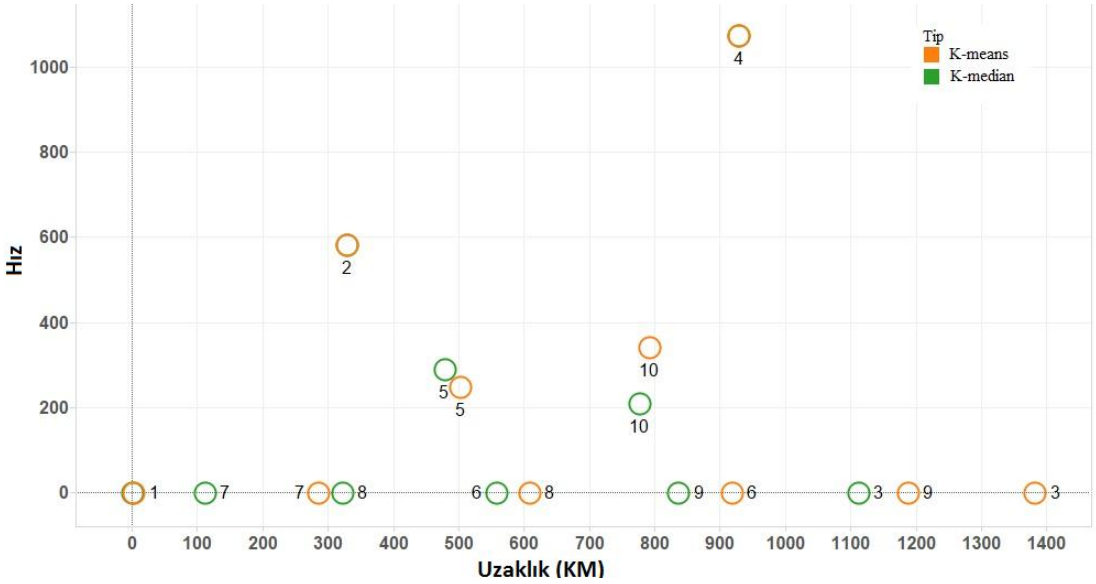


Şekil 5.7. Müşteri entropi sınıflarının hız değerleri

Geçiş veri seti üzerinde kurulacak SQL sorguları ile nereden-nereye bilgileri için frekans değerlerinin hesaplanmasıyla da uzak mesafelerdeki geçişlerin nadiren gerçekleştiği tespit edilmiştir. Frekans hesaplamaları sonucunda en sık hareketin 3.379.016 adet geçişle İstanbul içerisinde yer alan 865 numaralı gridde gerçekleştiği görülmüştür. Gridler arası tüm geçişler incelendiğinde 21.188 adet geçişin (grid kombinasyonunun) 2 veya daha düşük frekansa sahip olduğu görülmüştür. Tablo 5.1.'deki uç değer limitleri ile frekans değerleri birlikte değerlendirildiğinde, uzaklığı 653 km'den fazla ve frekansı 2 veya daha düşük olan 5.933 adet geçiş bulunmuştur. Şüpheli işlem değerlendirmesi için bu geçişlerin dikkate alınması anlamlı olsa bile daha ayırt edici kurallar bulunarak bu sayının düşürülmesi gerekecektir. Aksi takdirde çok fazla yanlış alarm durumu üretilmiş olacaktır.

5.4. Şüpheli İşlemlerin Bulunması için Gözetimsiz Yöntemlerin Kullanılması

Çalışmanın bu bölümünde SAS'ın FASTCLUS prosedürü kullanılarak uygulanan kümeleme algoritmalarının sonuçları paylaşılacaktır. Uygulama sonucunda ortaya çıkan kümelerin daha iyi değerlendirilmesi için veri seti ikiye ayrılmıştır: orjinal veri setinin yaklaşık %40'ından oluşan, kümeleri bulmak için kullanılan eğitim seti (training set) ve kümeleme sonuçlarını değerlendirmek için kullanılan, geri kalan veriden oluşturulan test seti. Eğitim veri seti üzerinde *k=10* belirlenerek k-means ve k-median kümeleme algoritmaları çalıştırılmıştır. Şekil 5.8.'de uzaklık ve hız değişkenlerine bağlı olarak küme merkezleri görülmektedir.



Şekil 5.8. Küme merkezleri

Şekilden görüldüğü gibi 2, 4, 5 ve 10 numaralı kümeler uç değerler barındırmaktadır. k-means kümeleme algoritmasına göre, bu kümelerde sırasıyla eğitim veri setinde 1, 1, 9 ve 3 adet; test veri setinde 3, 0, 9 ve 5 adet hareket bulunmaktadır. k-median kümeleme algoritmasına göre ise eğitim veri setinde bu kümelerde sırasıyla 1, 1, 8 ve 5 adet; test veri setinde 5 ve 10 numaralı kümelerde 11 ve 9 adet hareket yer almıştır. Noktaların büyük çoğunluğu 1 numaralı kümede toplanmıştır.

Müşterilerin sahip olduğu entropi değerlerine göre 3 sınıfa ayrıldığı hatırda tutularak, Tablo 5.1.'deki uzaklık ve hız değişkenleri için hesaplanmış uç değer limitleri de dikkate alındığında, eğitim ve test veri setlerinde sırasıyla 60 ve 119 adet uç değer olduğu görülmüştür. Tablo 5.2'de ve Tablo 5.3'de sırasıyla eğitim ve test veri setleri içerisinde 3 farklı müşteri sınıfının 10 farklı küme içindeki uç değere sahip hareketlerinin frekans değerleri sunulmuştur. Kümeleme algortimalarının sonuçlarına göre 2, 4, 5 ve 10 numaralı kümelerdeki hareketlerin şüpheli kabul edildiğine dikkat edilmelidir.

Tablo 5.2. Eğitim veri seti için frekans tablosu

	Küme	3	4	6	8	9	10	Toplam
Sınıf								
2 ($0 < e \leq 0{,}75$)		1	1	16	9	6	3	36
3 ($e > 0{,}75$)		3	0	11	5	5	0	24
Toplam								60

Tablo 5.3. Test veri seti için frekans tablosu

Küme	3	5	6	8	9	10	Toplam
Sınıf							
2 ($0 < e \leq 0{,}75$)	4	0	35	14	11	3	67
3 ($e > 0{,}75$)	4	1	23	10	12	2	52
Toplam							119

5.5. Geliştirilen Modelin Mevcut Uygulamalarla Entegrasyonu ve Performans Değerlemesi

Sahtekârlık işlemlerinin önlenmesi için kullanılan mevcut yöntemlere tamamlayıcı olması açısından geliştirdiğimiz yöntem, geleneksel bankacılık işlemlerindeki konum bilgisini dikkate almasıyla yeni bir yaklaşım olarak düşünülebilir [109]. Yaklaşımımızın performansının ölçülmesi ve kazanım sağlayıp sağlamadığının değerlendirilmesi için mevcutta sahtekârlık işlemlerinin önlenmesi amacıyla kullanılan sistemin performansı ile karşılaştırılması geçerli bir yöntem olacaktır. Performans bakış açısıyla değerlendirildiğinde tüm sahtekârlık önleme sistemlerinin temel amacı; yanlış alarm durumlar (false positive) ve hatalı bir şekilde onaylanan durumlar (false negative) en aza indirilirken, doğru alarm durumlarının (true positive) sayısının artırılması olarak özetlenebilir.

Çalışmamızın yapılabilmesi için veri sağladığımız bankada, mevcutta kural tabanlı çalışarak şüpheli görülen durumlar için alarm üreten bir sahtekârlık önleme sistemi kullanılmaktadır. Çalışmada kullanılan veri setinin ait olduğu Kasım 2012 ve Kasım

2014 dönemi için bankada ATM'lerden gerçekleşmiş bir sahtekârlık işlemi rapor edilmemiştir. Bununla birlikte mevcut sahtekârlık önleme sistemi, şüpheli gördüğü 506 adet bankacılık işlemi için alarm üretmiştir. Bu işlemlerin şüpheli olarak kontrol edildiği ve yapılan kontroller sonucu onaylanarak işlemin gerçekleşmesine izin verildiği bilinmektedir. Buna göre bu işlemler için gereksiz yere alarm (false positive) üretildiği açıktır. Mevcut sistemin şüpheli bulduğu 506 adet işlemi, tez çalışmasına esas teşkil eden veri seti ile eşleştirdiğimizde geçiş (transition) veri setinde 338 adet geçişe karşılık geldiği görülmüştür. Tanımladığımız uzaklık ve hız değişkenleri için belirlediğimiz istatistiksel uç değer limitleri dikkate alındığında, geçiş verisi içerisindeki bu 338 adet kaydın sadece 4 tanesinin uç değer limitlerini aştığı görülmüştür. Dolayısıyla, bankacılık işlemlerinin konum bilgisinin de dikkate alınarak oluşturulan geçiş (transition) bakış açısı ile uzaklık ve hız değişkenleri için belirlenen istatistiksel uç değer yaklaşımının yanlış alarm durumlarının sayısını anlamlı bir şekilde düşürdüğü gözlemlenmiştir denilebilir.

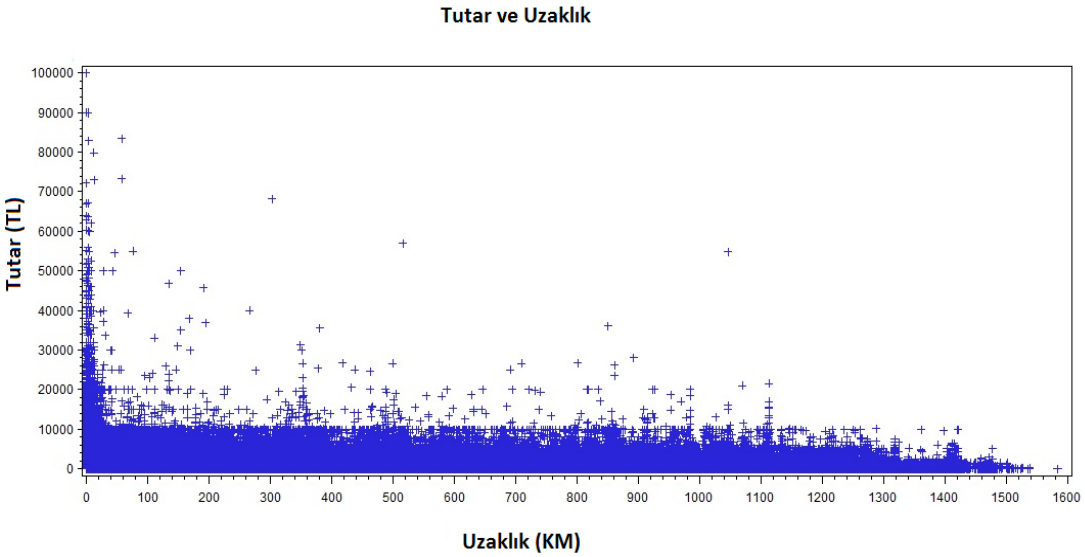
Sadece uzaklık değişkenine bağlı uç değer limitleri dikkate alındığında çok fazla sayıda işlemin şüpheli gibi gözüktüğü önceki bölümde belirtilmişti. Bunun nedeni yerleri değiştirilen ATM'ler ve bu değişiklik bilgisinin veri setine yansıtılamamış olması olabilir. Bununla birlikte, bu yaklaşım sonucunda bazı anlamlı iş kuralları da üretilebilecektir. Bunlardan ilki, entropi değeri 0'a eşit olan kesim, müşterilerin büyük çoğunluğunu oluşturmaktadır ve bu kişiler bulundukları gridi hiçbir zaman değiştirmemektedir. İlişkili gridler incelendiğinde ise en yüksek ilişkinin birbirine 75 km veya daha yakın mesafede bulunan gridler arasında bulunduğu görülmüştü. Dolayısıyla, 0 entropiye sahip olan müşteriler için, mevcut gridlerinden 75 km veya daha uzak bir mesafede işlem yapılmak istendiğinde alarm üretilmesi anlamlı olacaktır. İkinci kural 0'dan farklı entropiye sahip olan yani hareketli müşterilerle ilgili olarak geliştirilebilir. Bu müşterilerin hareketleri için uzaklık ve hız değişkenlerinin uç değer limitleri anlamlı olabilir. İstatistiksel uç değer limitlerine göre, entropi değerleri sınıflandırmasında ikinci veya üçüncü sınıfa giren müşterilerin kartları ile 653 km'den uzak bir mesafede ve 3,97 km/dak'dan daha yüksek bir hızla bir geçiş yapılmak isteniyorsa, bu geçişe sebep olan işlem şüpheli olabilir. Ayrıca geçiş kombinasyonları incelenerek nadiren gerçekleşmiş nereden-nereye (from-to)

durumları için de kurallar geliştirilebilir. Uzaklık için hesaplanan 653 km uç değer limitini aşan toplam 5.933 adet kombinasyon olduğu belirtilmişti. Bu sayı çok yüksek olduğu için, daha anlamlı sonuçlar elde edebilmek amacıyla bu limit 1000 km olarak düşünülebilir. Basit bir SQL sorgusu ile bu limiti aşan kombinasyonlar incelendiğinde ise bu şartlara uyan 1.973 adet grid kombinasyonu olduğu görülmektedir. Yapılan işlemin şüpheli olup olmadığını göstermesi bakımından bu da bir kural olarak düşünülebilir. Kümeleme algoritmalarının sonucunda ise daha az sayıda şüpheli işlem tespit edilmiş olup, bu işlemlerin şüpheli olma ihtimalleri yüksektir. Bulunan iş kurallarının özet gösterimi Tablo 5.4.'de sunulmuştur.

Tablo 5.4. Şüpheli işlem kuralları

Entropi Sınıfı	İş Kuralı
1 (e= 0)	D ≥ 75 km ise alarm üretilmeli (Birliktelik ilişkisi en yüksek olan gridlerin arasındaki mesafe < 75 km idi.)
2 (0 < e ≤ 0,75)	D ≥ 653 km ve S ≥ 3.97 km/dak ise alarm üretilmeli (İstatistiksel uç değer limitleri D= 653 km ve S= 3.97 km/dak idi.)
3 (e > 0,75)	Hareketli müşteriler için işlem tutarlarının dikkate alındığı analizler yapılabilir. Kümeleme algoritma sonuçları kullanılabilir.

Yukarıdaki kuralların finansal işlem bilgilerine bağlı olarak elde edildiği açıktır. Farklı kurallar bulunması için, gerçekleştirilmek istenen bir işlemin müşterinin favori (en çok işlem yaptığı) ATM'sine ve/veya şubesine olan uzaklığı da dikkate alınabilir. Ayrıca müşterinin ev ve/veya iş adresleri de aynı amaçla kullanılabilir. Anlamlı bir gösterge olması bakımından, mevcut veri seti ile hazırlanmış, yapılan işlemin finansal büyüklüğü ile işlemin favori ATM'ye olan uzaklığı arasındaki ilişkiyi gösteren grafik Şekil 5.9.'da sunulmuştur.



Şekil 5.9. İşlemin finansal büyüklüğünün uzaklığa bağlı değişimi

Grafik gösterimin daha net olması için işlem büyüklüğü 100.000 TL'den düşük olan işlemler grafiğe dahil edilmiştir. Grafikten açıkca görüldüğü gibi uzaklık arttıkça işlemin finansal büyüklüğü azalmaktadır. Bu ise konum bilgisinin kullanılmasının anlamlı sonuçlar doğuracağının açık bir göstergesidir.

5.6. Sonuçlar

Konum bilgisinin eklenmiş olduğu finansal işlem verisinin elde edilmesi ilk etapta ATM işlemlerinde daha hızlı olması nedeni ile tez çalışmasında konum bilgisinin anlamlılığı ATM'lerden yapılan işlemler üzerinde analiz edilmiştir. Benzer çalışma internet şube ve mobil şube aracılığıyla yapılan işlemler için konum bilgisinin elde edilmesi ve entegrasyonun sağlanmasıyla bu işlem kanalları için de yapılabilir. İnternet şubeden ve mobil şubeden yapılan işlemlerde konum bilgisi IP adresleri aracılığıyla elde edilebilecektir. İnternet şube, mobil şube, ATM, şube gibi tüm işlem kanalları için konum bilgisi alınarak veri konsolide edildiğinde, bir müşterinin yaptığı son işlem ile o anda yapılmak istenen işlemin konumları karşılaştırılabilecek, uzay-zamansal iş kuralları yardımıyla müşterinin o işlemi gerçekleştirme olasılığı değerlendirilebilecektir. Böylece işlem kanalından bağımsız olarak, müşteriyi daha iyi tanımaya yönelik, müşteri bazlı sahtekârlık önleme kontrolleri yapılabilecektir.

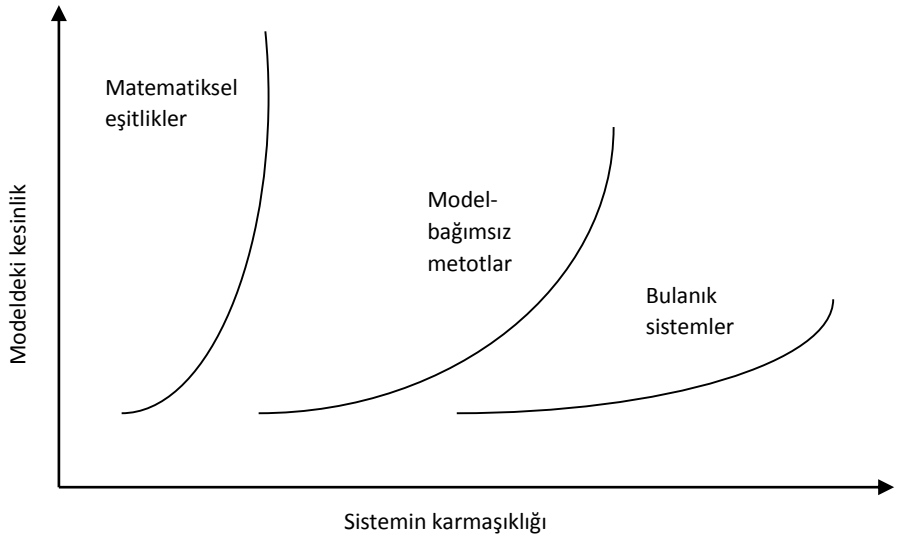
Örneğin; son işlemini internet şube aracılığıyla yapmış bir müşterinin yarım saat içerisinde son işlem konumuna 500 km uzalıkta bulunan bir ATM'den işlem yapması mümkün olmayacağı için bu işlem şüpheli olarak görülebilecektir. Hâlbuki zaman aralığı yarım saat değil de iki saat olursa bu işlemin mümkün olduğu görülebilecektir. Benzer şekilde, 0 entropiye sahip olan yani hiçbir zaman işlem yaptığı konumu değiştirmemiş bir müşterinin hesabından, kendisine çok uzak bir konumda işlem yapılmak istendiğinde şüphe oluşmalı ve ek doğrulayıcı kontroller için alarm üretilmelidir. Yukarıda detayları verilen yaklaşım ile elde edilen iş kuralları bir kural motoru aracılığıyla bankacılık sistemlerine dinamik bir şekilde entegre edilebilirse, mevcut sahtekârlık önleme kontrollerine müşteri alışkanlıklarıyla ilgili çok önemli bir değişken olan "işlem konumu" da dahil edilmiş olacak ve sahtekârlık önleme sisteminin performansı artacaktır.

BÖLÜM 6. ÖNERİLEN YÖNTEMİN BULANIK MANTIK İLE YENİDEN DEĞERLENDİRİLMESİ

Bölüm 4'de detayları sunulan ve Bölüm 5'de uygulama sonuçlarının paylaşıldığı, sahtekârlık işlemlerinin tespit edilmesi amacıyla geliştirilen modelin, bulanık mantık yaklaşımı ile entegre edilmesinin daha anlamlı sonuçlar üretebileceği düşünülmüştür. Bu bölümde hatırlatıcı olması bakımından bulanık mantık yaklaşımı ile ilgili temel bilgiler verilecek ve literatür araştırmamızda karşımıza çıkan, sahtekârlık işlemlerinin tespitinde bulanık mantıktan faydalanılmış çalışmalardan bahsedilecektir.

6.1. Kavram Olarak Bulanık Mantık

İnsan beyni gibi akıl yürütemeyen modern bilgisayarların ikili mantığı, gerçek dünyanın belirsizliğini modellemekte yetersiz kalmaktadır. Klasik mantıkla bulanık mantık arasındaki fark, sıfır ve bir dizilerine indirgenmiş kesin gerçekler ve doğru ya da yanlış olan önermeler ile serin hava ya da yüksek hız gibi belirsizlik veya değer yargıları içeren önermeler arasındaki fark gibidir [110]. Karmaşıklığı az olan, dolayısıyla belirsizliği de az olan sistemler için kapalı formdaki matematiksel ifadeler, sistemleri tam ve kesin olarak tanımlayacaktır. Karmaşıklığı biraz daha fazla olan ancak anlamlı verisine sahip olunan sistemler için, yapay sinir ağları gibi, model-bağımsız metotlar, eldeki veriden desenlerin öğrenilmesi yoluyla sistemle ilgili anlamlı sonuçlar verecektir. Sistemle ilgili çok az verinin bulunduğu, belirsizliğin ve karmaşıklığın yüksek olduğu sistemler için ise gözlemlenen girdi ve çıktı sonuçları arasında ilişki kurulmasına izin veren bulanık sonuç çıkarma, sistem davranışının anlaşılması için iyi bir yol sunabilir. Şekil 6.1.'de karmaşıklık, kesinlik ve modeller arasındaki ilişki grafik olarak sunulmuştur.

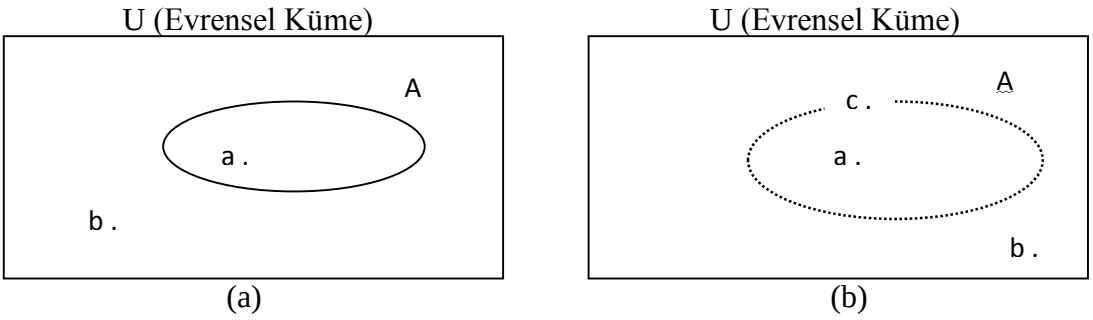


Şekil 6.1. Sistemin karmaşıklığı ve sistem modelindeki kesinlik arasındaki ilişki [111]

Yukarıdaki modellerin tamamı gerçek fiziksel dünyanın matematiksel özetlerini verir, ancak önemli olan nokta, problemdeki belirsizliğin karakteriyle uygun olan modeli seçebilmektir [111].

6.1.1. Klasik ve bulanık kümeler, bulanık sistem tasarımı

Klasik küme kuramında herhangi bir nesne bir kümeye ya aittir ya da değildir. Bu ilke bir nesnenin aynı anda hem birşey olması hem de o şey olmaması çelişkisini olanaksız kılmaktadır. Bulanık mantıkta ise, elemanlar bulanık bir kümeye ancak kısmen aittir ve kısmi üyelik nedeniyle aynı anda birden çok kümeye ait olabilirler. Şekil 6.2.'de klasik ve bulanık kümelerin sınırları görsel olarak sunulmuştur [110].



Şekil 6.2. (a) Klasik küme ve (b) Bulanık küme sınırları [111]

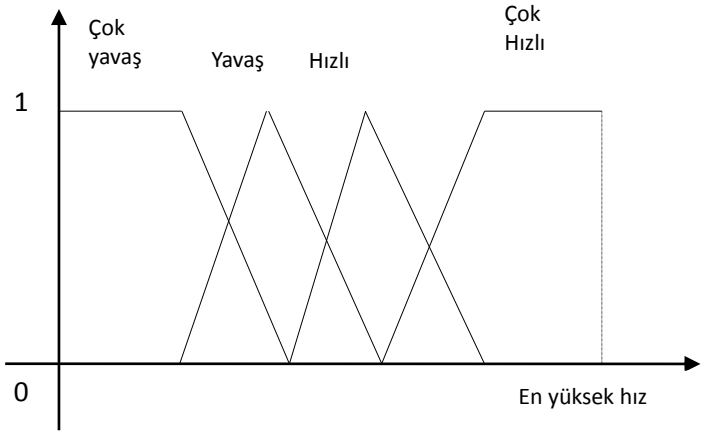
Bir bulanık *A* kümesi, *U* uzayında tanımlanan ve [0, 1] aralığında değerler alabilen $\mu_A(x)$ üyelik fonksiyonu ile gösterilen kümedir. Bu *A* kümesi;

$A = \{(x, \mu_A(x)) / x \in U\}$ şeklinde ifade edilir. (6.2)

Üyelik fonksiyonunun aldığı değerlere üyelik değerleri veya üyelik derecesi ismi verilmiştir. $\mu_A(x)$, *x*'in bu uzaya ne kadar üye olduğunun ölçüsüdür.

$$\mu_A(x) = \begin{cases} 1 \text{ ise, } x \text{ tamamen } A \text{ kümesinin üyesidir.} \\ (0, 1) \text{ ise, } x \text{ kısmen } A \text{ kümesinin üyesidir.} \\ 0 \text{ ise, } x \ A \text{ kümesinin üyesi değildir.} \end{cases} \quad (6.3)$$

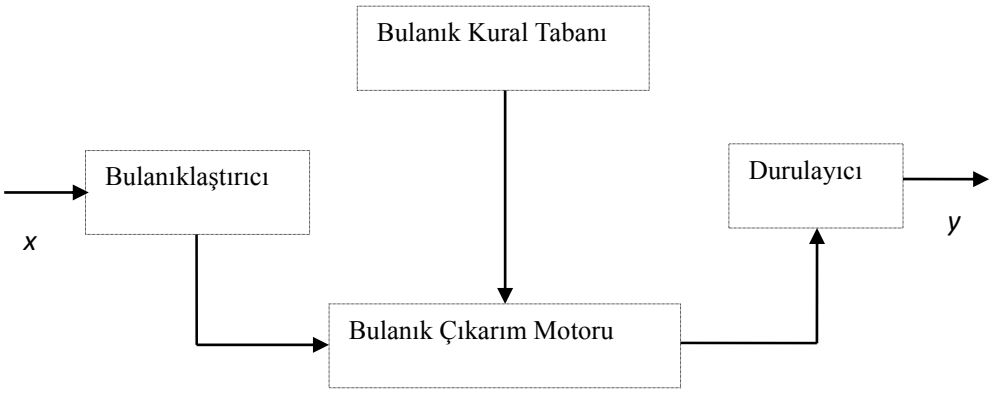
Bulanık sistemlerde kelimeler tanımlı oldukları uzayda bulanık kümelerle temsil edilirler. Örneğin bir arabanın hızının bulanık modeli çıkartılmak istendiğinde, ilk olarak arabanın ulaşabileceği en yüksek hız ile en düşük hız arasındaki değerler, yani değişkenin tanımlı olduğu uzay belirlenmelidir. Bu uzay belirlendikten sonra, çok yavaş, yavaş, hızlı, çok hızlı gibi sözsel değişkenler ve bu değişkenleri temsil edecek bulanık kümeler belirlenir. Şekil 6.3.'de bir arabanın hızına ait örnek bir bulanık küme görseli sunulmuştur.



Şekil 6.3. Sözsel değişken "arabanın hızı" için bulanık kümeler [110]

Klasik kümelerde gerçekleştirilen kesişim, birleşim, tümleme işlemlerinin benzerleri, bulanık kümeler de de gerçekleştirilir. Bu işlemlerin bulanık kümelerdeki gösterimi sırasıyla ve (V), veya (Λ), değil (~) işleçleri ile gerçekleştirilir. Bulanık mantık modellerinin geliştirilmesi için kullanılan MATLAB'de ise bu işlemler min, max ve üçgen gibi fonksiyonlar kullanılarak yapılabilmektedir [112, 113].

Bulanık mantıkla bir problemin çözümü için izlenecek modelleme adımları; girdi ve çıktıların bulanıklaştırılması, kuralların çıkartılması ve durulaştırmadır denilebilir. Bulanıklaştırma, girdi ve çıktıların bulanık küme gösterimi ile ifade edilebilmesi, üyelik fonksiyonları yardımı ile üyelik derecelerinin elde edilmesidir. Bulanıklaştırma için kullanılan Sigmodial *(S),* Pi *(π)*, Üçgensel, Yamuk gibi birçok üyelik fonksiyonu bulunurken, hangi üyelik fonksiyonunun kullanılacağına tecrübeye veya veri yapısına göre karar verilebilir. Bir sonraki adımda, uzmanların bilgi ve tecrübeleri eğer-ise şeklinde ifade edilerek bulanık kural tabanı oluşturulur. Son aşamada ise, sistemin sonuç olarak verdiği bulanık çıktı kümesi, durulaştırma yöntemlerinden biri kullanılarak sayısal, kesin ifadelere dönüştürülür. Buna göre bulanık bir sistem aşağıdaki grafik gösterim ile özetlenebilir [114].



Şekil 6.4. Temel bir bulanık sistem konfigürasyonu [110]

6.2. Sahtekârlık İşlemlerinin Tespitinde Bulanık Mantık

Sahtekârlık işlemlerinin tespitinde bulanık sistemlerden faydalanan az sayıda çalışma bulunmaktadır [115, 116, 117]. [116]'da yazarlar, şüpheli olan ve olmayan kredi kartı

işlemlerini sınıflandırabilmek için evrimsel bir bulanık sistem kullanmışlardır. Yaptıkları çalışma sonucunda, zor veri setlerinin sınıflandırılmasında bulanık mantık dönüşümünün kullanımının doğruluğu ve anlaşılabilirliği artırdığını göstermişlerdir. [117]'de Estevez ve diğerleri, sabit iletişim ağlarında kontör ödemelerindeki sahtekârlıkları önlemek için, sınıflama ve tahminleme modüllerinden oluşan proaktif bir sistem önermişlerdir. Bulanık kuralların uygulandığı sınıflandırma modülü, sahte abonelik, farklı bir sahtecilik, borcunu ödeyemez ve normal olmak üzere, daha önceki hareketlerine göre aboneleri dört farklı kategoriye ayırmıştır. Sahtekârlık tespitinde bulanık mantığın kullanıldığı diğer bir ilginç çalışmada da [115] veri madenciliği teknikleri ile birleştirilen bulanık mantık modeli ile elektronik bankacılıkta oltalama (phishing) sitelerinin bulanıklığının giderilmesine çalışılmıştır. [118]'de yazarlar kredi kartı sahtekârlıklarının tespit edilmesi için bulanık mantıktan faydalanmıştır. Çalışmada bulanık kurallar, bulanıklaştırma birimi, karar verme birimi ve durulayıcı birim olmak üzere dört bölüm vurgulanmıştır. [119] 'da yazarlar finansal raporlamada sahtekârlıkların tespit edilmesi için bulanık kümeleme uygulamasıyla sonuç elde etmeye çalışmışlardır. Çalışmada, bulanık kümelemenin veri setinde oluşturulan kümelere aidiyet yüzdesi şeklinde, her kümeye aidiyet oranını göstermesinin, finansal işlemlerden oluşan veri seti üyelerinin kısmi kategorizasyonuna izin verdiği vurgulanmıştır. Kümeleme yöntemlerinden biri olan bulanık c-means algoritması kümeleri, kümelere olan üyelikleri ve uç değerleri bulmak için kullanılabilecektir.

6.3. Önerilen Yöntemin Bulanık Mantık ile Yeniden Değerlendirilmesi

Bölüm 4'de detayları verilen ve Bölüm 5'de bir bankanın verileri üzerinden uygulama sonuçlarının paylaşıldığı yöntem, bulanık mantık bakış açısıyla yeniden yorumlanmıştır. Uç değerlerin, yani şüpheli işlemlerin bulunması için kullanılan kümeleme algoritması bulanık mantık ile uygulanmış, bulanık kurallar yardımı ile sahtekârlık işlemlerinin tespit edilmesine çalışılmıştır.

6.3.1. Bulanık kümeleme ve kural tabanlı analizler

Bir önceki bölümde anlatıldığı üzere, klasik kümeleme analizlerinde olduğu gibi bulanık kümeleme için de eğitim ve test veri kümeleri kullanılmıştır. Bulanık c-means kümeleme yöntemini uygulamanın bir yolu, MATLAB'in Fuzzy C-Means (fcm) fonksiyonunun kullanılmasıdır. Klasik kümeleme analizinde olduğu gibi Fuzzy C-Means uygulamasında da küme sayısı 10 olarak belirlenmiştir. Eğitim veri seti üzerinde fcm fonksiyonundaki standart seçenekler kullanılarak, sonuçları Tablo 6.1.'de verilen, üyelik değeri 0,95 veya daha yüksek olan bir kümeleme dağılımı elde edilmiştir. Test verisinin bulanık c-means algoritması sonucunda elde edilen kümelere klasik kümeleme yöntemi ile atanması sonucu oluşan üyelikler de Tablo 6.2.'de verilmiştir.

Tablo 6.1. Eğitim verisi için bulanık kümelerin üyelik ebatları (üyelik derecesi ≥ 0,95, eğitim verisi)

Küme	1	2	3	4	5
Üye sayısı	12.633	8.201	11.490	167.805	24.213
Küme	6	7	8	9	10
Üye sayısı	16.804	6.686.140	8.128	3.052	11.197

Tablo 6.2. Test verisi için klasik küme atamaları

Küme	1	2	3	4	5
Üye sayısı	81.682	44.245	65.649	905.752	135.546
Küme	6	7	8	9	10
Üye sayısı	77.519	10.996.164	39.046	20.198	53.613

Tablolarda görülen sonuçlar yorumlandığında, bulanık c-means kümeleme algoritmasının uç değerleri ortaya çıkarmadığı ve bu değerleri kümelere dağıttığı görülmektedir. Dolayısıyla k-means algoritmasının sonuçlarıyla kıyaslandığında, bulanık c-means algoritmasında her küme içerisinde daha fazla sayıda üye bulunduğu görülmektedir. Başka bir deyişle, bulanık c-means algoritması sonucunda az sayıdaki uç değerlerin yer aldığı kümeler oluşmamıştır. Sonuç olarak, bulanık c-means

algoritması ile elde edilen hiçbir kümenin uç değerlerden oluşan bir küme olduğu söylenememiştir.

Sahtekârlık işlemlerinin tespit edilmesi için bulanık kümeleme çalışmasına ek olarak, bulanık küme atamalarının üyelik derecelerinin kullanılacağı kural tabanlı bir bulanık sistem de uygulanabilecektir. MATLAB'deki fcm fonksiyonu sonucunda, eğitim veri seti için bu üyelik dereceleri elde edilmişti. Fakat test veri setindeki noktaların küme merkezlerine olan uzaklıklarının hesaplanması gerekmektedir. Herhangi bir *i* noktasının *j* kümesine üyelik derecesinin hesaplanması için aşağıdaki formül kullanılmıştır:

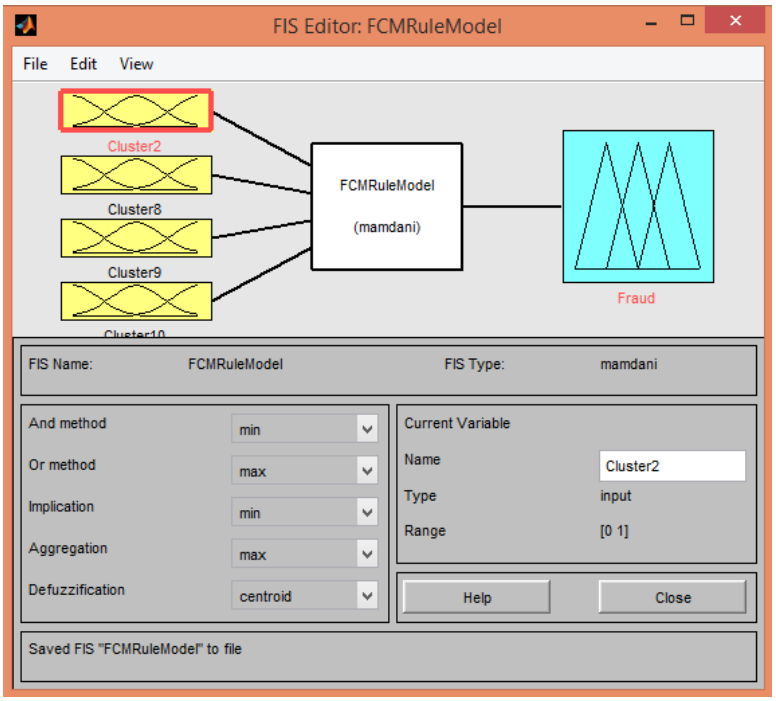
$$\mu_{ij} = \frac{1}{\Sigma_{k=1}^{N}\left(\frac{\| x_I - c_j \|}{\| x_I - c_k \|}\right)^{\frac{2}{m-1}}} \quad (6.1)$$

Burada x_I *i.* veri noktasının satır vektörünü, *N* kümelerin sayısını, c_j *j* kümesinin merkezini ve *m* bulanıklık indeksini göstermektedir. fcm fonksiyon hesaplamalarında MATLAB *m=2* kullanmaktadır. Buna göre hesaplanan küme merkezleri Tablo 6.3.'de verilmiştir.

Tablo 6.3. Bulanık c-means küme merkezleri

Küme	Uzaklık	Hız	Entropi
1	150,27	0,04	0,74
2	689,84	0,11	0,71
3	239,16	0,05	0,73
4	15,18	0,01	0,46
5	74,25	0,03	0,73
6	349,20	0,07	0,74
7	0,55	0,00	0,23
8	897,29	0,13	0,66
9	1158,20	0,16	0,71
10	504,11	0,09	0,72

Tablo 6.3.'de verilen bulanık c-means küme merkezleri düşünülerek; 2, 8, 9 ve 10 numaralı kümelere ait bulanık üyelik dereceleri, Şekil 6.5.'de verilen bulanık kural tabanlı modelin oluşturulmasında kullanılmıştır. Eşitlik 6.1. ile test verisindeki noktaların bulanık küme üyelik derecelerinin hesaplanmasından sonra, Şekil 6.5.'deki bulanık kural tabanlı model, test veri setindeki sahtekârlık vakalarının tespit edilmesinde kullanılabilecektir.



Şekil 6.5. FCM Bulanık kural modelinin özet gösterimi

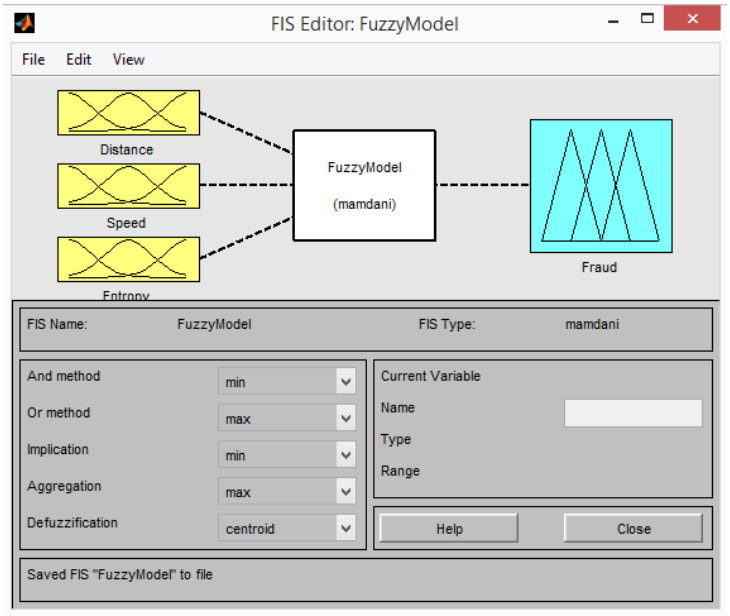
MATLAB içerisinde yer alan Fuzzy Logic Toolbox içinde bulanık bir sistem kurmak, kontrol etmek ve gözlemlemek için dinamik olarak birbirine bağlı, beş temel grafiksel kullanıcı arabirim vardır. Şekilde görülen Bulanık Karar Sistemi Editörü (Fuzzy inference system- FIS), sistemin giriş-çıkış değişkenlerinin sayısı ve isimleri gibi en temel işlemlerin yapıldığı editördür [110].

Bulanık modelin sonuçları değerlendirildiğinde, 0,9 eşik değerini aşan bulanık üyelik vakasının olmadığı gözlemlenmiştir. Fakat eşik değer 0,86'ya çekildiğinde, test veri setinde bu eşik değeri aşan 24.197 adet sahtekârlık üyelik derecesine sahip vaka olduğu görülmüştür. Algoritma sonuçlarına göre alarm üretilmesi gereken bu

işlemlerin sayısı çok yüksek olup, algoritmanın uygulanması çok verimli olmayacaktır.

6.3.2. Uç değerlerin bulunması için bulanık kural tabanlı sistemin uygulanması

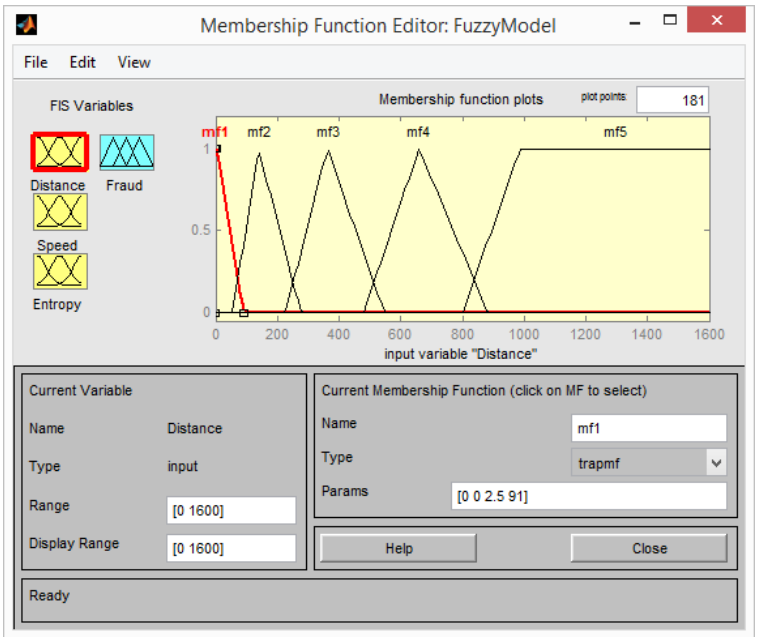
Sahtekârlık işlemlerinin tespit edilmesi amacıyla uzman bilgisinden faydalanılarak kural tabanlı bir bulanık model geliştirilmesi daha uygun olacaktır. Bulanık kural tabanlı sistemlerin endüstriyel birçok problemin çözümünde başarılı bir şekilde kullanıldığı bilinmektedir. Sahtekârlık işlemlerinin tespit edilmesi probleminde bulanık mantık ve kural tabanlı bulanık model kullanılmasının uygun olacağını düşünmemizin sebebi ise problemin karmaşık yapısı ve problemin çözümünde uzman bilgisinin yüksek önem arzetmesidir. Bu amaçla kurduğumuz bulanık kural tabanlı modelin gösterimi Şekil 6.6.'da verilmiştir. Bulanık modelin uygulaması için MATLAB'in Fuzzy Toolbox'ı kullanılmıştır. MATLAB'in sunduğu bu araçlar, bizim problemimizde olduğu gibi daha büyük veri setleri için bile bulanık kuralların rahatça yazılmasına imkan vermektedir.



Şekil 6.6. Bulanık modelin özet gösterimi

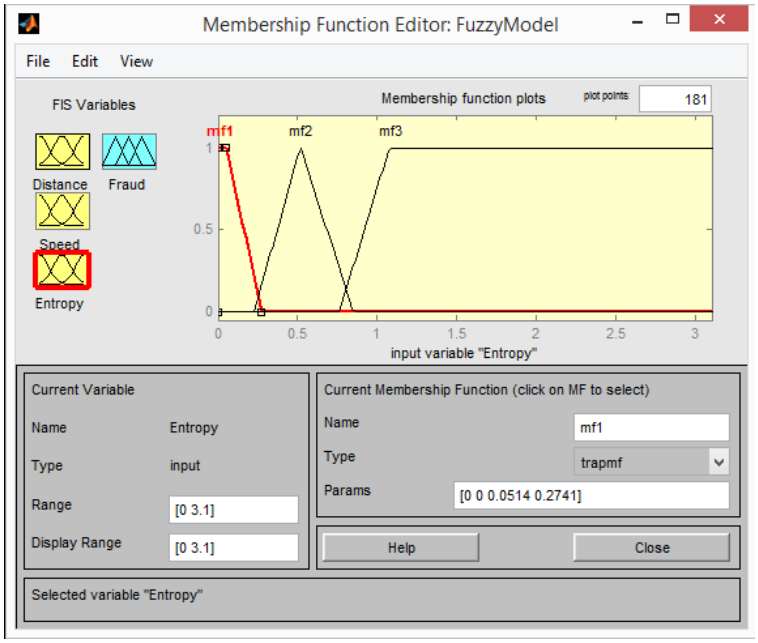
Şekilden görüldüğü gibi problemin çözümüne konu olan uzaklık, hız ve entropi değişkenleri yardımıyla işlemin fraud kümesine üyelik derecesi elde edilmeye

çalışılmıştır. Bu amaçla gerçekleştirilen bulanık kural tabanlı analizlerimizin ilk aşaması, üyelik fonksiyonunun belirlenmesidir. Bulanık c-means algoritması aracılığıyla bulanık üyelik fonksiyonlarının belirlenmesi için bir önceki bölümle benzer şekilde eğitim veri seti kullanılmıştır. MATLAB'de Üyelik Fonksiyonu Editörü (Membership Function Editor) kullanılarak Şekil 6.7. ve Şekil 6.8.'de görülen, analizlere temel teşkil eden üyelik fonksiyonları oluşturulmuştur.



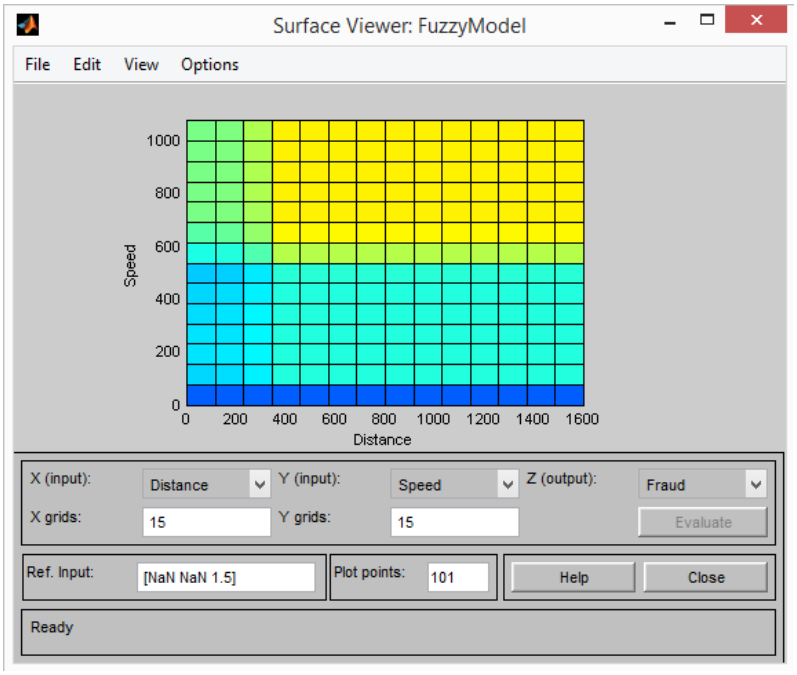
Şekil 6.7. Uzaklık değişkeni için üyelik fonksiyonu

Uzaklık değişkeni için bulanık c-means algoritması ile 5 adet küme oluşturulmuştur. Bu kümelerin sınırları, üyelik fonksiyonlarının alt ve üst sınırlarını belirlemiştir. Bu amaçla, "Uzaklık" bulanık üye değerleri için 0,35 üyelik değeri kullanılmıştır. Her bir bulanık kümenin pozisyonuna bağlı olarak üçgensel (triangular) veya yamuk (trapezoid) üyelik fonksiyonları kullanılmıştır.

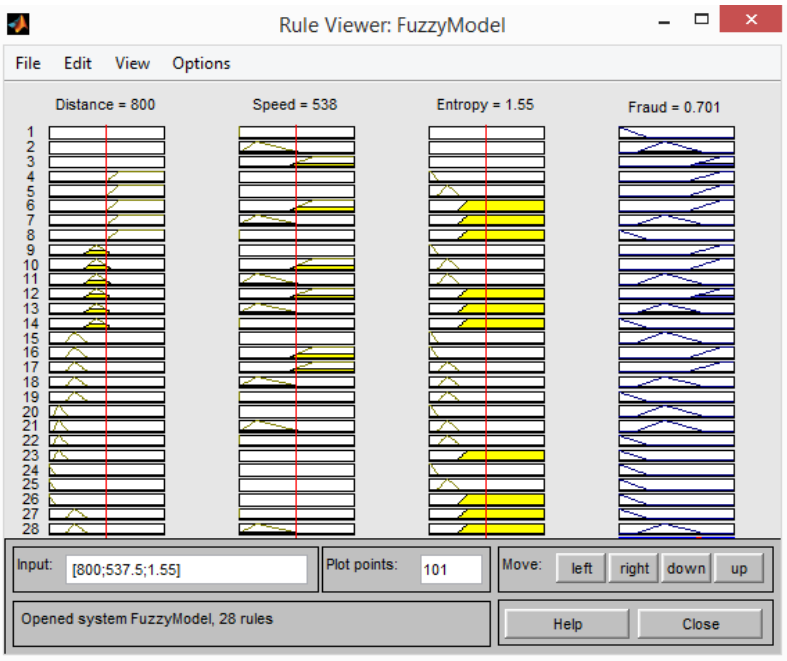


Şekil 6.8. Entropi değişkeni için üyelik fonksiyonu

Veri setimizdeki tüm değişkenler için üyelik fonksiyonları belirlendikten sonra, bu üyelik fonksiyonlarına bağlı olarak uzman görüşleri alınmış ve bulanık kurallar elde edilmiştir. Bu kurallar MATLAB'in Fuzzy Toolbox'ındaki Kural Editörü (Rule Editor) kullanılarak bulanık modele eklenebilir. Sahtekârlık işlemlerinin tespit edilmesi amacıyla uzman görüşlerine bağlı olarak oluşturulan 28 adet kural bulunmaktadır. Şekil 6.9. ve Şekil 6.10.'da bu kuralların grafik olarak özeti görülmektedir. Şekil 6.9. "Uzaklık" ve "Hız" değişkenleriyle ilgili ilişkiyi göstermektedir. Şekil 6.10. ise tüm kuralları özet olarak sunmaktadır.



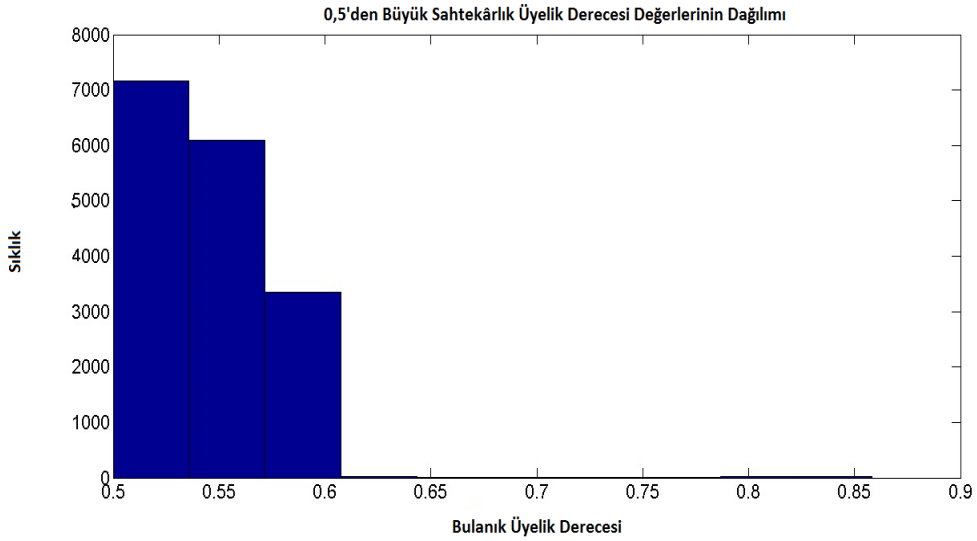
Şekil 6.9. Uzaklık ve hız değişkenleri için bulanık kuralların yüzey grafiği



Şekil 6.10. Kural görselinde bulanık kuralların grafik gösterimi

Bulanık kural tabanlı analizlerin son aşamasında, uç değerleri yani sahtekârlık işlemlerini tespit edebilmek için test veri seti ve bulanık kural seti kullanılmıştır. Bulanık kurallar test veri setinde uygulandıktan sonra, test setindeki tüm noktalar için sahtekârlık kümesine üyelik dereceleri de bulunmuştur. Şekil 6.11.'de sahtekârlık

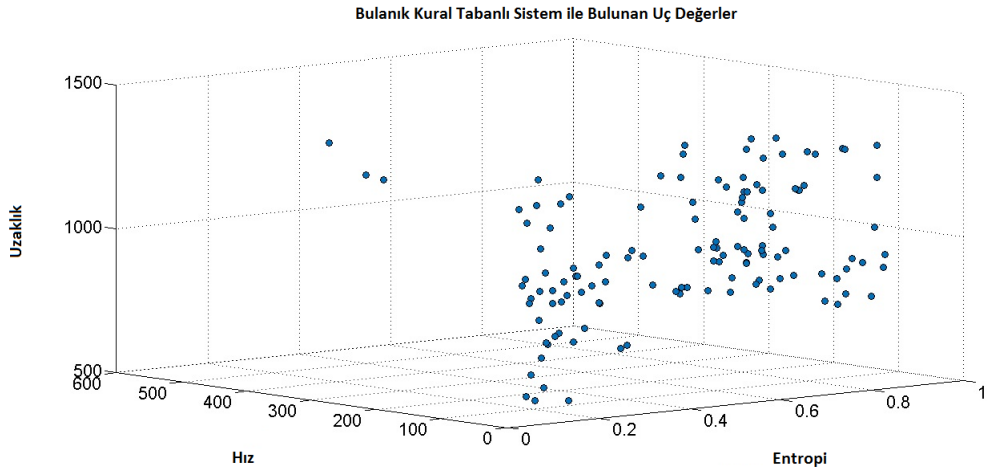
bulanık kümesine üyelik derecesi 0,5 veya daha yüksek olan noktaların sıklık grafiği verilmiştir. Bu sonuçlara göre, sahtekârlık bulanık kümesine üyelik derecesi 0,6 ve üzeri olan 127 adet uç değer bulunmuştur. Dolayısıyla, bulanık kural tabanlı sistemin çok fazla yanlış alarm üretmediği söylenebilir. Klasik yöntemlerle yapılan analizlerin sonuçlarıyla kıyaslandığında, 127 adet uç değerin yönetilebilirliğinin çok daha makul olduğu açıktır.



Şekil 6.11. Sahtekârlık bulanık kümesi için üyelik değerleri

6.3.3. Sonuçlar ve performans değerlendirmesi

Bulanık c-means kümeleme algoritması test veri seti üzerinde uygulandığında 2, 8, 9 ve 10 numaralı kümelerde 0,9 veya daha yüksek üyelik derecesinde üyesi bulunmadığı görülmüştür. Bununla birlikte, eşik değer biraz düşürüldüğünde, test verisi içindeki 24 binden fazla vaka şüpheli olarak bulunmuştur. Dolayısıyla, bulanık kümelemenin üyelik eşik değerlerine bağlı olarak çok sayıda yanlış alarm ürettiği söylenebilir. Ancak, aynı test veri seti üzerinde, bulanık kural tabanlı sistem sonucunda çok fazla yanlış alarm durumu oluşmadığından daha yönetilebilir sayıda uç değer tespit edildiği söylenebilir. Bu aslında bulanık kural tabanlı sistemin en çok istenen özelliğidir. Bulanık model tarafından bulunan 127 adet uç değer, yani 127 adet şüpheli işlem, Şekil 6.12.'de grafik görsel olarak sunulmuştur.



Şekil 6.12. Bulanık sistem tarafından bulunan şüpheli işlemlerin grafik gösterimi

Bulanık sistemin performans değerlemesi de klasik modelin performans değerlemesi ile benzer şekilde yapılabilir. Sahtekârlık önleme sistemlerinin temel amacının yanlış alarm durumlarını azaltmak ve doğru alarm durumlarını artırmak olduğu belirtilmişti. Çalışmaya esas teşkil eden veri setinin geçerli olduğu tarih aralığında, bankadaki mevcut sahtekârlık önleme sistemi tarafından üretilmiş 506 adet alarm durumu olduğu ve bu 506 adet işlemin geçiş veri setindeki 338 adet geçişle eşleştiği önceki bölümde paylaşılmıştı. Klasik yöntemle yapılan analizler sonucunda bu 338 adet geçişin sadece 4 tanesi şüpheli bulunmuştu. Bu bölümde detayları paylaşılmış olan bulanık kural tabanlı yaklaşım uygulandığında ise bu 338 adet geçişin sadece 1 tanesi için alarm üretilmesi gerektiği tespit edilmiştir. Şüpheli bulunan bu geçiş, 1.217 km mesafeye, 0,0715 km/dk hıza ve 0,5004 entropi değerine sahiptir. Üyelik derecesinin ise 0,5856 olduğu belirlenmiştir. Bu dikkate değer sonuç, bulanık kural tabanlı modelin yanlış alarm durumlarını belirgin bir şekilde azalttığını göstermektedir. Klasik yöntemle kıyaslandığında da bulanık modelin daha başarılı olduğu söylenebilir.

BÖLÜM 7. TARTIŞMA VE SONUÇ

Tüm dünyada banka müşterileri yeni teknolojilerin sunduğu imkânlarla, dünyanın neresinde olurlarsa olsunlar finansal işlemlerini yapabilmekten ötürü çok memnunlar [78]. İnternet ve mobil bankacılık aracılığıyla yapılan finansal işlemlerin sayısının ve büyüklüğünün her geçen gün arttığı bilinmektedir. Ancak bu teknolojilerin beraberinde getirdiği "anonimite", zamandan ve mekândan bağımsız olarak işlem yapabilme özgürlüğü, hesapların ve finansal değerlerin güvenliğinin sağlanması için yeni önlemler alınması gerekliliğini de doğurmaktadır.

Tez çalışmasında temel olarak hedeflenen, bankacılıkta gerçekleştirilen sahtekârlık işlemlerinin tespit edilmesi için yapılan veri analizlerine işlemlerin "konum" bilgilerinin de dahil edilmesini sağlayacak bir analitik model geliştirilmesi ve sahtekârlıkların tespitinde konum bilgisinin anlamlı bir etkisinin olup olmadığının ölçülmesidir. Sahtekârlık işlemlerinin tespit edilmesinde finansal işlemlerin konum bilgisinin etkisini ölçmek için, Türkiye'deki orta ölçekli bir bankanın müşterilerinin Türkiye'deki tüm ATM'lerde iki yıllık dönem içinde yaptıkları işlemler üzerinde analizler gerçekleştirilmiştir. Bu analizlerin neticesinde, sahtekârlık işlemlerine işaret eden iş kurallarının bulunması hedeflenmiştir. İşlemlerin konumu ve zamanı dikkate alındığından, bu kurallar uzay-zamansal bir yapıya sahip olup; sahtekârlık şüphesi uyandırması gereken işlemleri bulmanın en kolay yolu işlemin konumunun uzay-zamansal olarak uç değer olup olmadığının belirlenmesidir. İşlemin konumu bir uç değere işaret ediyorsa, işlem gerçekleşmeden önce ek doğrulama kontrolleri ile önlemler alınabilecektir. Müşterilerin mobilite desenleri de bu tür uzay-zamansal kuralların bulunmasında anlamlı bir bilgi kaynağı olacaktır. En temelde, bazı müşteriler hiçbir zaman işlem yaptıkları konumu değiştirmezken, bu müşterilerin hesaplarından her zamanki bu konumlarına çok uzak mesafede bir işlem yapılmak istendiğinde şüphe uyanması gerekecektir.

Tez çalışmasında sadece ATM'lerden yapılan işlemlere ait verinin kullanılmasının nedeni, ATM'lerden yapılan işlemlerin konum bilgisine erişimin daha kolay ve hızlı olmasıdır. Bununla birlikte, bütüncül ve müşteri odaklı bir sahtekârlık önleme sistemi için işlem kanalından bağımsız olarak değerlendirmeler yapılması gerektiği açıktır. Şubelerden yapılan işlemlerin konum bilgisinin elde edilmesinde ATM'lere benzer şekilde bir zorluk bulunmamaktadır. İnternet şubesi ve mobil şubeden yapılan işlemlerin konum bilgileri de IP adreslerinden elde edilebilecektir. Müşterilerle ilgili daha fazla bilgi sahibi olmak adına, müşterinin sosyal medya hesaplarındaki bilgilere erişim ve buradan konum doğrulaması yaptırmak da mümkün olabilecektir. Böylece, herhangi bir anda herhangi bir işlem kanalından yapılmak istenen bir işlem için, anlık olarak bir önceki işlemin konumu ile arasındaki mesafe hesaplanabilecek ve Bölüm 5 ve Bölüm 6'da elde edilen iş kuralları çalıştırılabilecektir. Örneğin, internet veya mobil şubeden işlem yapmış bir müşterinin, 45 dakika sonra 500 km uzaklıktaki bir ATM'den işlem yapması teknik olarak mümkün olamayacağı ve şüpheli görülmesi gerektiği halde, iki işlem arasında geçen sürenin 2 saat olması halinde böyle bir şüphe oluşmayabilecektir.

Bölüm 5 ve Bölüm 6'da elde edilen iş kurallarının, bir karar destek sistemi veya bir iş kuralları yönetim sistemine kolayca entegre edilebileceği açıktır. Kuralların sonuçlarına bağlı olarak sistemler alarm üretip ek doğrulama kontrollerini devreye sokabilecek veya işlemlerin devamına izin verebilecektir. Sahtekârlık işlemlerinin tespit edilip önlenmesi için konum bilgisinden faydalanılarak elde edilen bu iş kuralları, mevcut bilgi ve tecrübelerden çıkarılmış iş kurallarına ilave edilecek, tamamlayıcı kurallardır. Böylece amaçlanan, sahtekârlık önleme sistemlerinin performansının artırılarak, yanlış alarm durumlarının ve gözden kaçırılan sahtekârlık işlemlerinin azaltılmasıdır.

Uygulama sonuçlarının paylaşıldığı Bölüm 5 ve Bölüm 6'da elde edilen bulgular bir bütün olarak değerlendirildiğinde, sahtekârlık işlemlerinin tespit edilmesinde işlemlerin konum bilgisinin dikkate alınmasının, yanlış alarm durumlarının sayısını dramatik bir şekilde azaltarak sistem performansını büyük ölçüde artırdığı söylenebilir. Elde edilen bulgular aşağıda maddeler halinde sıralanmıştır;

- Entropi hesaplamalarına göre, banka müşterileri 3 farklı sınıfta değerlendirilebilir: tamamen hareketsiz müşteriler, ara sıra yer değiştiren müşteriler ve çok hareketli müşteriler.
- Müşterilerin %62'si tamamen hareketsiz müşteriler sınıfına girmiş olup, her zaman aynı yerde (komşulukta) işlem yapmışlardır.
- İşlem konumları dikkate alındığında, birbiri ile en yüksek ilişkiye sahip yani birbirleri arasında en yüksek geçişe sahip gridlerin uzaklıklarının 75 km veya daha az olduğu bulunmuştur.
- Hareketsiz (sıfır mobiliteye sahip) müşteriler için 75 km uzaklık, bir sınır olarak kabul edilebilecektir.
- Geçiş verisi üzerinden hesaplanan mesafe ve hız değişkenlerine ait istatistiksel uç değer limitleri oluşturulmuştur. Buna göre, 653 km mesafe değişkeni için, 3,97 km/dak da hız değişkeni için uç değer limitleri olarak belirlenmiştir.
- Orta hareketli ve hareketli müşteriler için istatistiksel uç değer limitleri anlamlı kontrol noktaları olabilecektir.
- Kümeleme algoritmaları ile de uç değer taşıyan işlemlerin tespit edilebileceği, bu algoritmaların istatistiksel uç değer limitleri ile elde edilen sonuçlara göre daha az sayıda şüpheli işlem ürettiği görülmüştür.
- Bankacılık sistemindeki mevcut sahtekârlık önleme sisteminin 506 adet işlem için yanlış alarm ürettiği bu veri setinde, konum bilgisi ile elde edilen iş kuralları da dikkate alındığında sadece 4 adet işlem için alarm üretileceği görülmüştür.
- Müşterilerin her zaman bulundukları yerden uzaklaştıkça finansal işlem kararlarının etkilenip etkilenmediğinin görülmesi amacıyla mesafe-parasal büyüklük ilişkisi incelenmiş; mesafe arttıkça işlemlerin parasal büyüklüğünün azaldığı gözlenmiştir.
- Problemin çözümü için önerilen yöntem, bulanık mantık yaklaşımı ile yeniden yorumlanmış; bulanık kümeleme ile sahtekârlık işlemlerinin tespitinde anlamlı sonuçlar elde edilememiştir.
- Uzman görüşlerinden faydalanılarak uzaklık, hız ve entropi bulanık kümelerine üyelik derecelerine bağlı olarak, sahtekârlık bulanık kümesine üyelikleri bulmak amacıyla 28 adet bulanık iş kuralı elde edilmiştir.

- Bulanık kuralların uygulanması sonucu 127 adet işlem şüpheli olarak değerlendirilmiştir. Klasik yöntemin sonuçlarıyla kıyaslandığında yanlış alarm sayılarında oldukça azalma sağlandığı söylenebilir.
- Bankacılık sistemindeki mevcut sahtekârlık önleme sisteminin 506 adet işlem için yanlış alarm ürettiği veri setinde, bulanık kuralların uygulanması sonucu sadece 1 adet işlem şüpheli bulunmuştur. Bu dikkate değer sonuç, bulanık kural tabanlı modelin yanlış alarm durumlarını belirgin bir şekilde azalttığını göstermektedir. Klasik yöntemle kıyaslandığında da bulanık modelin daha başarılı olduğu söylenebilir.

KAYNAKLAR

[1] Ziya Tunç Aloğlu, Bankacılık Sektörünün Karşılaştığı Riskler ve Bankacılık Krizleri Üzerindeki Etkileri, Uzman Yeterlilik Tezi, Türkiye Cumhuriyeti Merkez Bankası Bankacılık ve Finansal Kuruluşlar Genel Müdürlüğü, Mart 2008.

[2] Alparslan Çakır, Bankacilikta Operasyonel Risklerin Etkin Yönetiminde Risk Bazli Müşteri Tani İlkelerinin Önemi, Türkiye Bankalar Birliği, Nisan 2006.

[3] Demiriz A., Ekizoğlu B. 2016, "Fuzzy Rule-Based Analysis of Spatio-Temporal ATM Usage Data for Fraud Detection and Prevention", Journal of Intelligent & Fuzzy Systems xx (20xx) xxx, DOI: 10.3233/JIFS-169012, IOS Press.

[4] Gökhan Yılmaz, Suistimali Önlemede 10 Yöntem, 06.06.2014, http://www.usiud.org/index.php?ktg=nav&syf=makale&mode=0&mid=202.

[5] Report To The Nations On Occupational Fraud And Abuse, 2014 Global Fraud Study, https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

[6] Oxford Concise English Dictionary, Tenth edition, Publisher, 1999, page 562.

[7] FBI, Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Year, Department of Justice, United States, 2007, http://www.fbi.gov/publications/financial/fcs_report2007/financial_crime_2007.html.

[8] Albrecht, W.S., C.C. Albrecht, C.O. Albrecht and M.F. Zimbelman, 2009. Fraud Examination. South -Wester Cengage Learning, Mason, Ohio.

[9] Phua C., Lee V., Smith K., Gayler R., A Comprehensive Survey of Data Mining-based Fraud Detection Research, 2010.

[10] Sheela Thiruvadi and Sandip C. Patel, Survey of Data-mining techniques used in Fraud Detection and Prevention, Information Technology Journal 10 (4): 710-716, 2011.

[11] Moti Romi, Using Business Analytics for Detecting Fraud in Banking Sector, SAS Turkey, 2014.

[12] Kou Y., Lu C. T., Sinvongwattana S., Huang Y. P., Survey of Fraud Detection Techniques, Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23, 2004.

[13] Cahill H. M., Lambert D., Pinheiro J. C., Sun D. X., Detecting Fraud in the Real World, Handbook of massive data sets, Pages 911-929, Kluwer Academic Publishers Norwell, MA, USA ©2002, ISBN:1-4020-0489-3.

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

[15] Annual Fraud Indicator, June 2013, National Fraud Authority, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf.

[16] Ngai E. W. T., Hu Y., Wong Y. H., Chen Y., Sun X., The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature, Decision Support Systems Volume 50, Issue 3, February 2011, Pages 559–569.

[17] https://www.insurancefraudbureau.org, Erişim Tarihi: 25.11.2014.

[18] Tzenga, Shiang-Feng, Hwangb, Min-Shiang, & Chen, Hsing-Bai. 2005. A secure on-line software transaction scheme. Computer Standards & Interfaces, 27: 303-312.

[19] Yan Sun, An Investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China, Doctoral Thesis, May 2010.

[20] Aijaz Ahmed Shaikh & Syed Mir Muhammad Shah, Auto Teller Machine (ATM) Fraud Case Study of a Commercial Bank in Pakistan, International Journal of Business and Management; Vol. 7, No. 22; 2012, ISSN 1833-3850 E-ISSN 1833-8119, Published by Canadian Center of Science and Education.

[21] ENISA. Atm crime: Overview of the european situation and golden rules on how to avoid it. Technical report, European Network and Information Security Agency, September 2009.
https://www.enisa.europa.eu/publications/archive/atmcrime.

[22] Europol, Situation Report, "Payment Card Fraud in the European Union", Perspective of Law Enforcement Agencies, 2012.
https://www.europol.europa.eu/content/situation-report-payment-cardfraud-european-union.

[23] Michael E. Edge, Pedro R. Falcone Sampaio, The Design of FFML: A rule-based policy modelling lanugage for proactive fraud management in financial data streams, Expert Systems with Applications: An International Journal, Volume 39 Issue 11, September, 2012, Pages 9966-9985, Pergamon Press, Inc.

[24] Bankalar Arası Kart Merkezi, Pos, Atm, Kart Sayıları, http://bkm.com.tr/pos-atm-kart-sayilari/, Erişim Tarihi: 12.10.2016.

[25] Carbanak Apt The Great Bank Robbery, Version 2.0, February, 2015, http://krebsonsecurity.com/wpcontent/uploads/2015/02/Carbanak_APT_eng.pdf.

[26] http://www.access-cash.com/atm-glossary.php, Erişim Tarihi: 30.11.2015.

[27] European banks see new ATM skimming attacks, http://www.computerworld.com/article/2514560/security0/european-banks-see-new-atm-skimming-attacks.html, 25.11.2015

[28] Murat Kaya, İstanbul Bilişim Suçlarla Mücadele Şube Müdürlüğü, şifrematik cihazıyla internet üzerinden işlem yapan banka müşterilerini dolandıran ve kredi kartı kopyalayarak dolandırıcılık yapan bir şebekeye operasyon düzenledi, 14.12.2012, http://www.muratkaya.com.tr/2012/12/, Erişim Tarihi: 02.09.2016.

[29] Erkut Beydağlı, Manyetik Şeritli Kartlar ve CHIP&PIN Uygulaması, TÜBİTAK BİLGEM, 05.07.2009, http://www.bilgiguvenligi.gov.tr/donanim-guvenligi/manyetik-seritli-kartlar-ve-chip-pin-uygulamasi-3.html.

[30] European ATM Security Team (EAST), "European Fraud Update 32014" https://www.european-atm-security.eu/east-publishes-europeanfraud-update-3-2014/.

[31] Ali İhsan Karacan, Bankacılık ve Kriz, İstanbul: Finans Dünyası Yayınları, 1996, s. 13.

[32] M. Fedai Çavuş, "Bireysel Finansmanın Temininde Kredi Kartları: Türkiye'de Kredi Kartı Kullanımı Üzerine Bir Araştırma, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Yıl. 2006, Sayı. 15, s. 174.

[33] "Kredi Kartı Dolandırıcılığında 10 Yöntem", http://www.ntvmsnbc.com/news/195214.asp, 07.06.2008., Erişim Tarihi: 30.10.2015.

[34] Rıdvan Yıldız, Kredi Kartı ve Banka Kartlarının Üçüncü Kişiler Tarafından Haksız Kullanımı, 15.09.2014, http://webunya.com/kredi-karti-ve-banka-kartlarinin-ucuncu-kisiler-tarafindan-haksiz-kullanimi, Erişim Tarihi: 02.05.2013.

[35] Aydın S., Yılmazer Y., Yolsuzluk ve Mali Suçlar, Adalet Yayınevi, 2014 Mayıs, Ankara, ISBN/Ref: 9786051463858.

[36] Dahl, J. 2006 Card Fraud. In Credit Union Magazine.

[37] Schindeler, S. 2006 Fighting Card Fraud in the USA. In Credit Control, House of Words Ltd.

[38] Hand, D. J., Blunt G. 2001 Prospecting gems in credit card data. IMA Journal of Management Mathematics, 12.

[39] Yusuf Şahin, Intelligent Ways Of Detecting Fraud, Ph.D. Thesis, İstanbul, 2013, Marmara Üniversitesi, Fen Bilimleri Enstitüsü.

[40] Lee W., Stolfo S. J., Mok K. W., A data mining framework for building intrusion detection models, Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium.

[41] Bankacılıkta Dolandırıcılık Eylemleri: Tespit/Önleme Yöntemleri, Türkiye Bankalar Birliği Yayını, 2007, s. 9.

[42] Savaş Kavcı, Banka Dışı Kişilerce Yapılan Bankalara Yönelik Hileler, Yüksek Lisans Tezi, İstanbul, 2009.

[43] Kabay M. E., "Salami Fraud, http://www.networkworld.com/newsletters/sec/2002/01467137.html. Erişim Tarihi: 05.05.2013.

[44] Robert Nisbet, John Elder, Gary Miner, Chapter 17, Fraud Detection, Handbook of Statistical Analysis and Data Mining Applications, pages 347-361, Academic Press, Boston, 2009.

[45] PriceWaterhouseCoopers (2011) Global Economic Crime Survey – UK Report. Available at: http://www.pwc.co.uk/eng/publications/global-economic-crime-survey-2011-uk-report.html.

[46] Protecting the Enterprise: Enterprise Fraud Strategy, Vision and Reality, Fraud Management Institute, June 2010. http://www.sas.com/resources/asset/enterprise-fraud-strategy-summary.pdf.

[47] Transactional Fraud Detection: A Modular Approach, Addressing the next generation of financial crimes, IBM. https://www.ibm.com/services/multimedia/Transactional_fraud_detection.pdf., Erişim Tarihi: 06.05.2013.

[48] Zhong, Ning, Zhou, Lizhu, Methodologies for Knowledge Discovery and Data Mining, Third Pacific-Asia Conference, PAKDD'99, Beijing, China, April 26-28, 1999, Proceedings.

[49] Han J., Kamber M., Data Mining: Concepts and Techniques, 2nd ed., The Morgan Kaufmann Series in Data Management Systems, Jim Gray, Series Editor Morgan Kaufmann Publishers, March 2006. ISBN 1-55860-901-6.

[50] Using Data Mining Techniques for Fraud Detection, Solving Business Problems Using SAS® Enterprise Miner™ Software, A SAS Institute Best Practices Paper In conjunction with Federal Data Corporation.

[51] Hand D. J., Measurement Theory and Practice: The World Through Quantification, 2004, ISBN: 978-0-470-68567-9, Wiley.

[52] Brockett, P., Derrig, R., Golden, L., Levine, A. & Alpert, M. 2002. Fraud Classification using Principal Component Analysis of RIDITs. Journal of Risk and Insurance 69(3): 341-371.

[53] Dorronsoro, J. R., Ginel, F., Sanchez, C. and Cruz, C. S. 1997 Neural fraud detection in credit card operations. IEEE Transactions on Neural Networks, 8.

[54] Han J., Kamber M., Data Mining Concepts and Techniques, Second Edition, page 452, 461, Morgan Kaufmann Publishers.

[55] Tan P. N., Steinbach M., Kumar V., Introduction to Data Mining, page 506, ©2006 | Cloth | ISBN-13: 9780321321367.

[56] K. Tsiptsis and A. Chorianopoulos, Data Mining Techniques in CRM, Inside Customer Segmentation, 2009 John Wiley & Sons, Ltd., page 46.

[57] Hair, Black, Bobin, Anderson, Tatham, Multivariate Data Analysis, Sixth Edition, page 557, Pearson; 6 edition, November 7, 2005.

[58] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ACM Comput. Surv., 41(3):15:1–15:58, July 2009.

[59] M. Gupta, Jing Gao, C.C. Aggarwal, and Jiawei Han. Outlier detection for temporal data: A survey. Knowledge and Data Engineering, IEEE Transactions on, 26(9):2250–2267, Sept 2014.

[60] Maik Anderka, Timo Klerx, Steffen Priesterjahn, and Hans Kleine Bu¨ning. Automatic atm fraud detection as a sequence-based anomaly detection problem. In Proceedings of the 3rd International Conference on Pattern Recognition Applications and Methods (ICPRAM 2014). SciTePress, 2014.

[61] George Grekousis and YorgosN. Fotis. A fuzzy index for detecting spatiotemporal outliers. GeoInformatica, 16(3):597–619, 2012.

[62] Tom Fawcett and Foster Provost. Adaptive fraud detection. Data Mining and Knowledge Discovery, 1(3):291–316, 1997.

[63] T. Klerx, M. Anderka, and H. KleineBu¨ning. On the usage of behavior models to detect atm fraud. In Proceedings of the 21st European Conference on Artificial Intelligence (ECAI 2014), Prague, Czech Republic, 2014.

[64] FICO, http://www.fico.com/, Erişim Tarihi: 01.09.2012.

[65] Experian, http://www.experian.com/, Erişim Tarihi: 10.09.2012.

[66] SAS, http://www.sas.com/tr_tr/home.html, Erişim Tarihi: 12.09.2012.

[67] IBM, https://www.ibm.com/us-en/, Erişim Tarihi: 15.09.2012.

[68] RSA, https://www.rsa.com/en-us, Erişim Tarihi: 20.09.2012.

[69] Detica, http://www.baesystems.com/en/cybersecurity/capability/financial-crime. Erişim Tarihi: 10.10.2012.

[70] "Why IBM Operational Decision Management?A Case for Business Users of Information Technology", White Paper, June 2012, IBM, ibm.com/operational-decision-management.

[71] T. Morgan, Business rules and information system: aligning IT with business goals. Addison-Wesley, Boston, ISBN 0-201-74391-4, 2002.

[72] Ronald G. Ross, Principles of The Business Rule Approach, Business Rule Solutions, p.85-87, ISBN-13: 978-0201788938, ISBN-10: 0201788934.

[73] Charles Forgy, Rete: A Fast Algorithm for the Many Pattern/Many Object Pattern Match Problem, Artificial Intelligence, 19, pp 17–37, 1982.

[74] Edge, Michael; Sampaio, Pedro; Philpott, Oliver; Choudhary, Mohammed., A policy distribution service for proactive fraud management over financial data streams, Proceedings-2008 IEEE International Conference on Services Computing, SCC. Vol. 2 USA: IEEE Computer Society, 2008. p. 31-38.

[75] Samakovitis, G. and Kapetanakis, S. (2013), Computer-aided Financial Fraud Detection: Promise and Applicability in Monitoring Financial Transaction Fraud, Proceedings of the International Conference in Business Management and Information Systems, (ICBMIS 2013) Nov. 19-21, Dubai, United Arab Emirates.

[76] Osman Demirdogen, Sukru Yaprakli, Mustafa Kemal Yilmaz, and Jamaluddin Husain. Customer risk perceptions of internet banking a study in Turkey. Journal of Applied Business Research (JABR), 26(6), 2010.

[77] CGI Group Inc. Understanding financial consumers in the digital era, a survey and perspective on emerging financial consumer trends. Technical report, CGI Group Inc., 2014.
https://www.cgi.com/sites/default/files/pdf/br fs consumersurveyreport final july 2014.pdf.

[78] Gloria Barczak, Pam Scholder Ellen, and Bruce K. Pilling. Developing typologies of consumer motives for use of technologically based banking services. Journal of Business Research, 38(2):131 – 139, 1997.

[79] Antony Beckett, Paul Hewer, and Barry Howcroft. An exposition of consumer behaviour in the financial services industry. International Journal of Bank Marketing, 18(1):15–26, 2000.

[80] Shaoyi Liao, Yuan Pu Shao, Huaiqing Wang, and Ada Chen. The adoption of virtual banking: an empirical study. International Journal of Information Management, 19(1):63 – 74, 1999.

[81] Vincent-Wayne Mitchell. Consumer perceived risk: conceptualisations and models. European Journal of Marketing, 33(1/2):163–195, 1999.

[82] Titus Chukwuemezie Okeke. Perceived risk/security and consumer involvement with electronic payments in nigeria: A discriminant analysis. IOSR Journal of Business and Management (IOSR-JBM), 14(6):57–67, Nov.-Dec. 2013.

[83] Joaquin Aldas-Manzano, Carla Ruiz-Mafe, Silvia Sanz-Blas, and Carlos Lassala-Navarre. Internet banking loyalty: evaluating the role of trust, satisfaction, perceived risk and frequency of use. The Service Industries Journal, 31(7):1165–1190, 2011.

[84] Yi-Shun Wang, Yu-Min Wang, Hsin-Hui Lin, and Tzung-I Tang. Determinants of user acceptance of internet banking: an empirical study. International Journal of Service Industry Management, 14(5):501–519, 2003.

[85] Bruce Schneier. The psychology of security. In Serge Vaudenay, editor, Progress in Cryptology-AFRICACRYPT 2008, volume 5023 of Lecture Notes in Computer Science, pages 50–79. Springer Berlin Heidelberg, 2008.

[86] Raymond A Bauer. Consumer behavior as risk taking. In R. S. Hancock, editor, Dynamic marketing for a changing world. Chicago: American Marketing Association, 1960.

[87] Michel Laroche, Gordon H. G. McDougall, Jasmin Bergeron, and Zhiyong Yang. Exploring how intangibility affects perceived risk. Journal of Service Research, 6(4):373–389, 2004.

[88] Dale Littler and Demetris Melanthiou. Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of internet banking. Journal of Retailing and Consumer Services, 13(6):431, 443, 2006. Retail Consumer Behavior Contrasting Macro- and Micro-Perspectives on Retailing: Towards Integration.

[89] Markus Schmidt. Investigating Risk Perception: A Short Introduction in Chapter 3 of Loss of Agro-Biodiversity in Vavilov Centers, with A Specific Focus on the Risks of Genetically Modified Organisms, Ph.D. Thesis. University of Vienna.

[90] Lennart Sjberg. Factors in risk perception. Risk Analysis, 20(1):1–12, 2000.

[91] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. The psychometric study of risk perception. In VincentT. Covello, Joshua Menkes, and Jeryl Mumpower, editors, Risk Evaluation and Management, volume 1 of Contemporary Issues in Risk Analysis, pages 3–24. Springer US, 1986.

[92] Rachel Pain. Place, social relations and the fear of crime: a review. Progress in Human Geography, 24(3):365–387, 2000.

[93] Titus Chukwuemezie Okeke. Perceived risk/security and consumer involvement with electronic payments in nigeria: A discriminant analysis. IOSR Journal of Business and Management (IOSR-JBM), 14(6):57–67, Nov.-Dec. 2013.

[94] Clausius, R.; Hirst, T. The Mechanical Theory of Heat: With its applications to the steam-engineand to the physical properties of bodies; J. van Voorst: London, UK, 1867.

[95] Shannon, C. A Mathematical Theory of Communication. Bell Syst. Tech. J. 1948, 27, 379–423.

[96] Altan Mesut, Veri Sıkıştırmada Yeni Yöntemler, Doktora Tezi, 2006, Edirne.

[97] Kullback, S. Information Theory and Statistics; Wiley: New York, NY, USA, 1959.

[98] Cover, T.; Thomas, J. Elements of Information Theory; Wiley: Hoboken, NJ, USA, 2006.

[99] Wenke Lee, Dong Xiang, Information-Theoretic Measures for Anomaly Detection, 1081-601 1/01 $10.00 0 2001 IEEE.

[100] Przemysław Berezinski, Bartosz Jasiul, Marcin Szpyrka, An Entropy-Based Network Anomaly Detection Method, Entropy 2015, 17, 2367-2408; doi:10.3390/e17042367.

[101] Rongxi Zhou, Ru Cai and Guanqun Tong, Applications of Entropy in Finance: A Review, Entropy 2013, 15, 4909-4931; doi:10.3390/e15114909.

[102] http://www.mdpi.com/journal/entropy. Erişim Tarihi: 01.06.2015.

[103] Takeshi Kurashima, Tomoharu Iwata, Go Irie, and Ko Fujimura. Travel route recommendation using geotags in photo sharing sites. In Proceedings of the 19th ACM International Conference on Information and Knowledge Management, CIKM '10, pages 579–588, New York, NY, USA, 2010. ACM.

[104] Yan-Tao Zheng, Zheng-Jun Zha, and Tat-Seng Chua. Mining travel patterns from geotagged photos. ACM Trans. Intell. Syst. Technol., 3(3):56:1–56:18, May 2012.

[105] D.J. Gagne, A McGovern, J. Brotzge, and Ming Xue. Severe hail prediction within a spatiotemporal relational data mining framework. In Data Mining Workshops (ICDMW), 2013 IEEE 13th International Conference on, pages 994–1001, Dec 2013.

[106] Sarah Hosein, Raid Al-Tahir, and Bheshem Ramlal. Spatiotemporal analysis of dengue hemorrhagic fever and dengue shock syndrome incidence within trinidad, west indies. In Proceedings of the Second ACM SIGSPATIAL International Workshop on the Use of GIS in Public Health, HealthGIS '13, pages 8–17, New York, NY, USA, 2013. ACM.

[107] Ickjai Lee, Guochen Cai, and Kyungmi Lee. Exploration of geo-tagged photos through data mining approaches. Expert Systems with Applications, 41(2):397 – 405, 2014.

[108] Sarvar Patel, Location, Identity and Wireless Fraud Detection, 0-7803-4298-4/97/$10.ooO 1997 IEEE.

[109] Sigi Goode and David Lacey. Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. Decision Support Systems, 50(4):702 – 714, 2011. Enterprise Risk and Security Management: Data, Text and Web Mining.

[110] http://egefuzzylogic.weebly.com/uploads/4/9/1/9/49194479/fuzzy_matlab_uygulamalari.pdf.

[111] Ross T. J., Fuzzy Logic with Engineering Applications, Second edition, Wiley.

[112] http://bm.bilecik.edu.tr/Dosya/Arsiv/odevnot/bulanik_mantik.pdf. Erişim Tarihi: 03.08.2016.

[113] www.yarbis1.yildiz.edu.tr/web/userCourseMaterials/eakdogan_36828f938370f2b8f904bf105c4370f3.pdf. Erişim Tarihi: 03.08.2016.

[114] web.itu.edu.tr/~ozgerme/Sunumlar/Fuzzy_09_12_10.pptx. Erişim Tarihi: 04.08.2016.

[115] M. Aburrous, M.A. Hossain, K. Dahal and F. Thabtah, Intelligent phishing detection system for e-banking using fuzzy data mining, Expert Systems with Applications 37(12) (2010), 7913 –7921.

[116] P.J. Bentley, J. Kim, G. Jung and J. Choi, Fuzzy darwinian detection of credit card fraud, In Proc of 14th Annual Fall Symposium of the Korean Information Processing Society, 2000.

[117] P.A. Estevez, C.M. Held and C.A. Perez, Subscription fraud prevention in telecommunications using fuzzy rules and neural networks, Expert Systems with Applications 31 (2) (2006), 337–344.

[118] F.S. Nezhad and H.R. Shahriari, Fuzzy logic and takagisugeno neural-fuzzy to deutsche bank fraud transactions. In e-Commerce in Developing Countries: With Focus on e-Security (ECDC), 2013 7th Intenational Conference on, 2013, pp. 1–15.

[119] M.J. Lenard and P. Alam, Encyclopedia of Information Science and Technology, Second Edition, chapter Application of Fuzzy Logic to Fraud Detection, IGI Global, 2009, pp. 177–181.

[120] Viaene, S., Derrig, R. & Dedene, G. (2004). A Case Study of Applying Boosting Naive Bayes to Claim Fraud Diagnosis. IEEE Transactions on Knowledge and Data Engineering 16(5): 612-620.

[121] Brockett, P., Derrig, R., Golden, L., Levine, A. & Alpert, M. (2002). Fraud Classification using Principal Component Analysis of RIDITs. Journal of Risk and Insurance 69(3): 341-371.

[122] Belhadji, E., Dionne, G. & Tarkhani, F. (2000). A Model for the Detection of Insurance Fraud. The Geneva Papers on Risk and Insurance 25(4): 517-538.

[123] He, H., Graco, W. & Yao, X. (1999). Application of Genetic Algorithms and k-Nearest Neighbour Method in Medical Fraud Detection. Proc. of SEAL1998, 74-81.

[124] Phua, C., Alahakoon, D. & Lee, V. (2004). Minority Report in Fraud Detection: Classification of Skewed Data, SIGKDD Explorations 6(1): 50-59.

[125] Wheeler, R. & Aitken, S. (2000). Multiple Algorithms for Fraud Detection. Knowledge-Based Systems 13(3): 93-99.

[126] Chen, R., Chiu, M., Huang, Y. & Chen, L. (2004). Detecting Credit Card Fraud by Using Questionaire-Responded Transaction Model Based on Support Vector Machines. Proc. of IDEAL2004, 800-806.

[127] Kim, M. & Kim, T. (2002). A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection. Proc. of IDEAL2002, 378-383.

[128] Maes, S., Tuyls, K., Vanschoenwinkel, B. & Manderick, B. (2002). Credit Card Fraud Detection using Bayesian and Neural Networks. Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.

[129] Aleskerov, E., Freisleben, B. & Rao, B. (1997). CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection. Proc. of the IEEE/IAFE on Computational Intelligence for Financial Engineering, 220-226.

[130] Moreau, Y. & Vandewalle, J. (1997). Detection of Mobile Phone Fraud Using Supervised Neural Networks: A First Prototype. Proc. of 1997 International Conference on Artificial Neural Networks, 1065-1070.

[131] Rosset, S., Murad, U., Neumann, E., Idan, Y. & Pinkas, G. 1999. Discovery of Fraud Rules for Telecommunications - Challenges and Solutions. Proc. of SIGKDD99, 409-413.

[132] Moreau, Y., Lerouge, E., Verrelst, H., Vandewalle, J., Stormann, C. & Burge, P. (1999). BRUTUS: A Hybrid System for Fraud Detection in Mobile Communications. Proc. of European Symposium on Artificial Neural Networks, 447-454.

[133] A. Srivastava, A. Kundu, S. Sural, A.K. Majumdar, Credit card fraud detection using hidden Markov model, IEEE Transactions on Dependable and Secure Computing 5 (1) 2008 37–48.

[134] J.T.S. Quah, M. Sriganesh, Real-time credit card fraud detection using computational intelligence, Expert Systems with Applications 35 (4) 2008 1721–1732.

[135] V. Zaslavsky, A. Strizhak, Credit card fraud detection using self-organizing maps, Information & Security 18, 2006, 48–63.

[136] Yamanishi, K., Takeuchi, J., Williams, G. & Milne, P. 2004. On-Line Unsupervised Outlier Detection Using Finite Mixtures with Discounting Learning Algorithms. Data Mining and Knowledge Discovery 8: 275-300.

[137] Kim, J., Ong, A. & Overill, R. 2003. Design of an Artificial Immune System as a Novel Anomaly Detector for Combating Financial Fraud in Retail Sector. Congress on Evolutionary Computation.

[138] W. Yang, S. Hwang, A process-mining framework for the detection of healthcare fraud and abuse, Expert Systems with Applications 31 (1), 2006, 56–68.

[139] Bolton, R. & Hand, D., 2001, Unsupervised Profiling Methods for Fraud Detection. Credit Scoring and Credit Control VII.

[140] Kokkinaki, A., 1997, On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling. Proc. of IEEE Knowledge and Data Engineering Exchange Workshop, 107-113.

[141] Cortes, C. & Pregibon, D. 2001. Signature-Based Methods for Data Streams. Data Mining and Knowledge Discovery 5: 167-182.

[142] Burge, P. & Shawe-Taylor, J., 2001, An Unsupervised Neural Network Approach to Profiling the Behaviour of Mobile Phone Users for Use in Fraud Detection. Journal of Parallel and Distributed Computing 61: 915-925.

[143] Murad, U. & Pinkas, G., 1999, Unsupervised Profiling for Identifying Superimposed Fraud. Proc. of PKDD99.

[144] Bentley, P., 2000, Evolutionary, my dear Watson: Investigating Committee-based Evolution of Fuzzy Rules for the Detection of Suspicious Insurance Claims. Proc. of GECCO2000.

[145] Von Altrock, C., 1997, Fuzzy Logic and Neurofuzzy Applications in Business and Finance. 286-294. Prentice Hall.

[146] Stefano, B. & Gisella, F., 2001. Insurance Fraud Evaluation: A Fuzzy Expert System. Proc. of IEEE International Fuzzy Systems Conference, 1491-1494.

[147] Cox, E., 1995, A Fuzzy System for Detecting Anomalous Behaviors in Healthcare Provider Claims. In Goonatilake, S. & Treleaven, P. (eds.) Intelligent Systems for Finance and Business, 111-134. John Wiley and Sons Ltd.

[148] Bentley, P., Kim, J., Jung., G. & Choi, J., 2000, Fuzzy Darwinian Detection of Credit Card Fraud. Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.

[149] Edge E. M., Sampaio P., A survey of signature based methods for financial fraud detection. Computers & Security, Volume 28, Issue 6, September 2009, Pages 381–394.

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

EKLER

EK A: Sahtekârlık işlemlerinin tespitinde kullanılan veri madenciliği teknikleri

Sahtekârlık işlemlerinin tespitinde kullanılan veri madenciliği teknikleri

Sahtekârlık Alanı	**Sigortacılık**	**Kredi/Kredi kartı**	**Telekom**	**Derleme Makaleleri**
Veri Madenciliği Yöntemi				
Sınıflandırma ve Regresyon	[120], [121], [122], [123], [124],	[125], [126], [127], [128], [129]	[130], [131], [132]	
Kümeleme		[133], [134], [135]		
Anomali Tespiti	[136]		[137]	
Birliktelik Kuralları ve Dizi Analizleri	[138]			
Müşteri Profilleme ve İmza Tabanlı Analizler		[139], [140]	[14], [13], [141], [142], [143]	
Bulanık Mantık	[144], [145], [146], [147]	[148]		
Derleme Makaleleri				[9], [149], [150], [16]

ÖZGEÇMİŞ

Betül Ekizoğlu, 05.09.1984'de Kayseri'de doğdu. 2002 yılında Uşak Şehit Abdulkadir Kılavuz Anadolu Öğretmen Lisesi'nden mezun oldu. Aynı yıl başladığı Erciyes Üniversitesi Endüstri Mühendisliği Bölümü'nü 2006 yılında ikincilik derecesi ile bitirdi. 2006 yılında İstanbul Teknik Üniversitesi Endüstri Mühendisliği'nde yüksek lisans eğitimine başladı. Yüksek lisans eğitimi devam ederken bir katılım bankasının bilgi teknolojileri departmanında sistem analisti olarak çalışmaya başladı. 2009 yılında Sakarya Üniversitesi Endüstri Mühendisliği'nde doktora eğitimine başladıktan sonra, finans sektöründeki bilgi teknolojileri çalışmalarına da sistem analisti ve proje yöneticisi olarak devam etti. Halen bilgi teknolojileri ve proje yönetimi çalışmalarını bireysel olarak sürdürmektedir.