

T.C
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK BİLGİSAYAR ANABİLİM DALI
BİLGİ TEKNOLOJİLERİ BİLİM DALI

**TÜRKİYE GSM SEKTÖRÜNDE VERİ MADENCİLİĞİ
YÖNTEMİ İLE SAHTEKARLIK TESPİTİ VE BİR
UYGULAMA**
(YÜKSEK LİSANS TEZİ)

Tezi Hazırlayan: **Hakan Ahmet KILIÇARSLAN**

İstanbul, 2013

T.C
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK BİLGİSAYAR ANABİLİM DALI
BİLGİ TEKNOLOJİLERİ BİLİM DALI

**TÜRKİYE GSM SEKTÖRÜNDE VERİ MADENCİLİĞİ
YÖNTEMİ İLE SAHTEKARLIK TESPİTİ VE BİR
UYGULAMA**
(YÜKSEK LİSANS TEZİ)

Tezi Hazırlayan:
Hakan Ahmet KILIÇARSLAN
Öğrenci No:
100862002

Danışman:
Doç. Dr. Gökhan SİLAHTAROĞLU

İstanbul, 2013

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum “TÜRKİYE GSM SEKTÖRÜNDE VERİ MADENCİLİĞİ YÖNTEMİ İLE SAHTEKARLIK TESPİTİ VE BİR UYGULAMA ” başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiği ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım 10/07/2013

(İmza)

Aday: Hakan Ahmet KILIÇARLAN

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

**Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,**

Aşağıda tez adı belirtilen yüksek lisans öğrencisi 100862002 no'lu Hakan Ahmet KILIÇARSLAN'ın 10/07/2013 tarihinde yapılan tez savunma sınavı¹ sonucunda 55 dakika süreyle sunduğu ve savunduğu tezi hakkında² oybirliğiyle, **BASARILI** kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : Matematik Bilgisayar
Programı : Bilgi Teknolojileri
Tez Başlığı³ : Türkiye GSM Sektöründe Veri Madenciliği Yöntemi ile Sahtekarlık Tespiti ve Bir Uygulama

Tez Sınav Jürisi

Öğretim Üyesi

Danışman : Doç. Dr. Gökhan SİLAHTAROĞLU
Üye : Yrd. Doç. Dr. Ediz ŞAYKOL
Üye : Yrd. Doç. Dr. Jeta ALO

İmza



¹ Jüri üyeleri söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez savunma sınavına alır. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda jüri en geç onbeş gün içinde toplanarak adayı tez savunma sınavına alır. Tez savunma sınav süresi en az 45 dakikadır. Yüksek lisans tez savunma sınavı, tez çalışmasının sunulması ve bunu izleyen soru-yanıt bölümlerinden oluşur ve dinleyiciye açıktır. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-3)

² Tez sınavının tamamlanmasından sonra jüri, tez hakkında “kabul”, “düzeltme” veya “red” kararı verir. Jüri başkanı, jüri üyelerince imzalanmış sınav tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi başarısız bulunan öğrencinin Enstitü ile ilişkisi kesilir. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve yönetmelikte belirtilen usullere uygun olarak tezini aynı jüri önünde yeniden savunur. Bu savunma sınavında da tezi kabul edilmeyen öğrencinin enstitü ile ilişkisi kesilir. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

³ İleride doğabilecek aksaklıkların engellenmesi için tezin başlığının yazılması gerekmektedir.

TÜRKİYE GSM SEKTÖRÜNDE VERİ MADENCİLİĞİ YÖNTEMİ İLE SAHTEKARLIK TESPİTİ VE BİR UYGULAMA

Tezi Hazırlayan: Hakan Ahmet KILIÇARSLAN

Özet

Bu tez çalışmasında, öncelikle Türkiye'deki GSM sektörü genel hatlarıyla ele alınmıştır. Sektörün hacmi, yatırımlar ve istihdam, operatörler ve özellikleri açıklanmıştır. Sektörün bu yönü açıklandıktan sonra, bu sektörden yasadışı yollarla kazanç elde etmek isteyen şahısların, uyguladıkları yöntemler belirtilmiştir. Bunun yanında GSM sektörünü de dolandırıcılık konularını içine alan mevcut kanunlar, ve düzenlemeler belirtilmiştir. Operatörlerin satış kanallarından biri olan alternatif satış kanallarında meydana gelen sahtekarlık girişimlerinin nasıl engelleneceği üzerinde durulmuştur. Bununla beraber, müşteri bilgi ve belge güvenliği konularına değinilmiştir.

Anahtar Kelimeler: Telekomünikasyon, Dolandırıcılık, Operatör, Veri Madenciliği

FRAUD DETECTION AND AN APPLICATION IN TURKEY GSM SECTOR WITH DATA MINING

Presented by: Hakan Ahmet KILIÇARSLAN

Abstract

First Turkey GSM industry is outlined in this thesis work. Size of sector, investments and employment, operators and their properties are explained. After explaining this aspect of industry, we stated the methods used by individuals who wish to obtain illegal gains from this sector. As well as we explained existing laws and regulations that enclose fraud issues of GSM industry. We explained how to prevent from fraud attempts on alternative sales channel of operators.

Keywords: Telecommunication, Fraud, Operator, Data Mining

İÇİNDEKİLER

ÖZET	iii
ABSTRACT	iv
TABLolar LİSTESİ	v
ŞEKİLLER LİSTESİ	vi
KISALTMALAR	vii
1.GİRİŞ	1
2.TÜRKİYE’DE GSM SEKTÖRÜ	2
2.1. GSM Nedir?.....	2
2.2. GSM Mimarisi.....	3
2.3. Türkiye GSM Sektöründe Faaliyet Gösteren Şirketler	6
2.3.1. Operatörler	6
2.3.1.1. Turkcell	6
2.3.1.2. Vodafone	7
2.3.1.3. Avea	7
2.3.2. Operatörler Hakkında	8
2.4 Türkiye GSM Pazarına Ait Bilgiler.....	8
2.4.1. Genel Pazar Verileri	8
2.4.2. İşletmeci Yatırımları	11
2.4.3. İstihdam	12
2.5. GSM Sektöründeki Problemler ve Tanımlamalar	12
2.5.1. Faturalı Hat	13
2.5.2. Sim Kart Değişikliği	14
2.5.3. Kontratlı Cihaz Kavramı	14
2.5.4. Elektronik Mağaza Kavramı	14
2.5.5. Operatör Sistemleri	15
2.6. Türkiye’de GSM Sektörüne İlişkin Söyleşi	15

3. SEKTÖRDEKİ SAHTEKARLIK ÇEŞİTLERİ VE YÖNTEMLERİ.....	18
3.1. Kişiyi Gösterir Belge Dolandırıcılığı	18
3.2. Adres Gösterir Belge Dolandırıcılığı.....	18
3.3. Sim Kart Dolandırıcılığı	18
3.4. Operatöre Ait Bilgisayarları Ele Geçirme	19
3.4.1. Truva Atları	19
3.4.2. Şifre Kırıcılar	19
3.4.3. Tuş Kaydediciler.....	20
3.4.4. Koklayıcılar	20
3.5. Bilgi Elde Etme Girişimleri.....	21
3.6. Operatör Çalışanı İle Ortaklaşa Sahtekarlık Girişimi.....	21
3.7. Trafik Taşıma Yöntemi	21
3.8. Değerlendirme	21
4. SEKTÖRDEKİ MEVCUT KANUNLAR VE AÇIKLARI	24
4.1. Bilişim Suçları İle İlgili Düzenlemeler.....	24
4.1.1. Ceza İndirimi	25
4.1.2. Cezanın Ağırlaştırılması	25
4.1.3. Yaptırım.....	26
4.2. Belge Sahteciliği İle İlgili Düzenlemeler	26
4.2.1. Korunan Hukuki Değer.....	27
4.2.2. Suçun Unsurları	27
4.2.3. Resmi Belgeyi Sahte Olarak Düzenlemek.....	27
4.2.4. Resmi Belgenin Değiştirilmesi	27
4.2.5. Sahte Resmi Belgeyi Kullanma	28
4.2.6. Fail ve Mağdur.....	28
4.2.7. Suçun Konusu.....	28
4.2.8. Manevi Unsur	28
4.2.9. Yaptırımlar.....	28
4.2.9.1. Resmi Belgede Sahtecilik Suçu.....	28
4.2.9.2. Resmi Belgeyi Bozmak Yok Etmek veya Gizlemek	29
4.2.9.3. Resmi Belgeyi Çıkartmak Adına Yalan Beyanda Bulunmak	29
4.2.9.4. Resmi Özel Belgede Sahtecilik	29
4.2.9.5. Özel Belgeyi Bozmak Yok Etmek veya Gizlemek.....	29

4.3. Kanunların Tartışılması ve Değerlendirme	29
5. SAHTEKARLIK GİRİŞİMLERİNİN ENGELLENMESİ VE TAKİBİ	31
5.1. SISNET.....	32
5.1.1. SISNET' e Giriş.....	32
5.1.2. SISNET Üzerinden Cihaz Satışı Yapılması ve Onay Süreci.....	35
5.1.3. SISNET Üzerinden Diğer Hat ve Ürünlerin Satışı.....	40
5.1.4. SISNET Üzerinden Onaylanan İşlemlerin Kontrolü	40
5.2. SISNET' in Sağladığı Yararlar.....	41
5.3. Mağaza Kontrol Sistemi	41
5.3.1. Mağaza Kontrol Sisteminin Faydaları	42
5.3.2. Mağaza Kontrol Sistemi İle Satış Yapılması.....	42
5.3.3. Mağaza Kontrol Sisteminin Değerlendirilmesi	44
5.4. Veri Madenciliği Yöntemleri İle Sahtekarlık Analizi	44
5.4.1. Problemin Tanımı	44
5.4.2. Amaç.....	45
5.4.3. Veri Madenciliği.....	45
5.4.4. Verilerin Özellikleri.....	47
5.4.4.1. Abone Cinsiyeti.....	48
5.4.4.2. Abone Yaşı.....	48
5.4.4.3. Abone İkamet Yeri	48
5.4.4.4. Abone Kimlik İl	48
5.4.4.5. İşlem Yapılan Mağaza İli	48
5.4.4.6. İşlem Yapılan Mağaza.....	48
5.4.4.7. İşlemin Yapıldığı Gün	48
5.4.4.8. Personel Cinsiyeti.....	48
5.4.4.9. Personel Tecrübesi	48
5.4.4.10. Hattın Türü	48
5.4.4.11. Hattın Özelliği	49
5.4.4.12. Hattın Kategorisi	49
5.4.4.13. Mernis Doğrulama.....	49
5.4.4.14. Kapama Kısıtlama Durumu.....	49
5.4.4.15. Daha Önce Aldığı Cihaz Sayısı.....	49
5.4.4.16. Kampanya Giriş Durumu	49

5.4.5. Verilerin Analizi	50
5.4.6. Karar Ağacı Oluřturulması	54
5.4.7. Karar Ağacı Doğruluk Analizi.....	60
5.4.8. Karar Ağacının SISNET'e Entegre Edilmesi	62
5.4.9 Uygulamanın Geliřtirilme Çalıřmaları ve Scorer Özelliđi	63
5.4.10 Deđerlendirme	63
6. SONUÇ ve ÖNERİLER.....	65
KAYNAKLAR	66

TABOLAR LİSTESİ

	Sayfa No.
Tablo.1. Yıllara Göre Net Satış Gelirleri	9
Tablo.2. Yıllara Göre Operatörlerin Net Gelirleri.....	10
Tablo.3. Net Kar Değerleri	10
Tablo.4. Yıllara Göre Yatırım Tutarları	11
Tablo.5. Üç Aylık Yatırım Değerleri	11
Tablo.6. Sahtekarlık Girişimlerinin Tablolaştırılmış Görüntüsü.....	23

ŞEKİLLER LİSTESİ

	Sayfa No.
Şekil.1. Şebekelerin Hücresel Görünümü	3
Şekil.2. GSM Şebekesi Alansal Gösterim	5
Şekil.3. Toplam Gelirin İşletmeciler Arasındaki Dağılımı	9
Şekil.4. Toplam Gelirin İşletmeciler Arasındaki Dağılımı	12
Şekil.5. SISNET Giriş Ekranı	32
Şekil.6. SISNET Kullanıcı Tanımlama Ekranı	33
Şekil.7. SISNET Kullanıcı Ekranı	34
Şekil.8. SISNET Yönetici Ekranı	34
Şekil.9. SISNET Satış Ekranı	35
Şekil.10. SISNET Evrak Ekranı	36
Şekil.11. SISNET Cihaz Bilgi Giriş Ekranı	37
Şekil.12. SISNET Cihaz Satış Bilgilendirme Ekranı	37
Şekil.13. SISNET Cihaz Satışı Merkez Denetim Ekranı	38
Şekil.14. SISNET Cihaz Satışı Hata Ekranı	39
Şekil.15. SISNET Cihaz Satışı Hata Kullanıcı Ekranı	39
Şekil.16. SISNET Cihaz Onay Ekranı	39
Şekil.17. SISNET Cihaz Mağaza Onay Ekranı	39
Şekil.18. SISNET Cihaz Satışı Tamamlandı Ekranı	40
Şekil.19. SISNET Satış Onayları	40
Şekil.20. Satış İşleyiş Görünümü	42
Şekil.21. Mağaza Kontrol Sisteminden Ürün Seçimi	43
Şekil.22. Mağaza Kontrol Sisteminden Müşteri Bilgi Girişi	43
Şekil.23. Kullanıcı merkezli interaktif veri madenciliği döngüsü fuzzy sistemler, Bayesian ağları, genetik algoritmalar	44
Şekil.24. Cinsiyet Dağılımı	50
Şekil.25. İkamet Dağılımları	50
Şekil.26. İşlem Yapılan İl Dağılımları	51
Şekil.27. Mağaza Dağılımları	51
Şekil.28. Gün Dağılımları	51
Şekil.29. İşlem Yapan Personel Dağılımları	52
Şekil.30. Personel Tecrübe Dağılımları	52

Şekil.31. Hat ve Fiyat Dağılımları	52
Şekil.32. Mernis Doğrulama Dağılımı.....	53
Şekil.33. Kredi Kartı Kullanım Dağılımı.....	53
Şekil.34. Abone Dağılımları	53
Şekil.35. Verilerin Ön İzlemesi	54
Şekil.36. Color Manager Görünümü.....	55
Şekil.37. Color Manager Ayarları.....	55
Şekil.38. Karar Ağacı ve KNIME Analiz Görünümü.....	56
Şekil.39. Karar Ağacı Kampanya Giril Yöntemi.....	56
Şekil.40. Karar Ağacı Kapama Kısıtlama.....	57
Şekil.41. Karar Ağacı Cihaz Sayısı.....	58
Şekil.42. Karar Ağacı Kapama Kısıtlama 2.....	58
Şekil.43. Karar Ağacı İşlem Yapılma Günü	59
Şekil.44. Karar Ağacı İşlem Yapılma Günü 2	59
Şekil.45. Karar Ağacı İşlem Yapılan Mağaza	60
Şekil.46. Bayes Görünümü 1	60
Şekil.47. Bayes Görünümü 2	61
Şekil.48. Bayes Görünümü 3	61
Şekil.49. Bayes Görünümü 4	62
Şekil.50. Bayes Görünümü 5	62
Şekil.51. Scatter Plot Görünümü	63
Şekil.52. Kargo Gönderim Uyarısı	63
Şekil.53. Kargo Takip Uyarısı	64

KISALTMALAR

GSM	: Global System for Mobile Communications
BTK	: Bilgi Teknolojileri Kurumu
SIS	: Shop in Shop
BSS	: Base Station Sub-system
3G	: 3rd Generation
T.C.	: Türkiye Cumhuriyeti
T.C.K	: Türk Ceza Kanunu
IP	: İnternet Protocol Address

BİRİNCİ BÖLÜM

1.GİRİŞ

GSM sektörü, sürekli gelişen, geliştikçe büyüyen, hacmini her geçen yıla oranla arttıran ve her gün doğrudan kullandığımız bir alandır. Sektörün bu kadar büyük olması beraberinde de bir takım sorunlar getirmektedir. Bu sorunların en büyüğü ise sektörde fraud olarak nitelendirilen dolandırıcılık olaylarıdır. Dolandırıcılık olayları kimi zaman abonelik evraklarında, kimi zaman ise operatöre ait yazılımsal sistemlerde yapılmaktadır.

Dolandırıcılık yolu ile haksız kazanç elde eden şahıslar, operatörlere büyük zararlar vermektedir. Gerçek bir müşterinin evraklarının, farklı kişilerce, bu amaç için kullanıldığı durumlarda, hem yargısal süreç sonunda verilen cezalar, hem de Bilgi Teknolojileri Kurumunun yaptırımları operatörlere büyük darbe vermektedir.

Alternatif Kanal olarak adlandırılan, operatörlerin, elektronik mağazalar içerisinde faaliyet gösterdiği satış kanalları, dolandırıcılık olaylarına en açık noktaların başında gelmektedir. Bu satış noktalarında çalışanlar, kimi zaman bir, en çok ise 4 kişi ile müşterilere hizmet vermektedir. Dolandırıcılık girişimlerinin yaşanmaması veya minimum düzeye indirilmesi için bir takım çalışmalar yapılmış ve bu çalışmalar tezde detaylıca ele alınmıştır.

Tez çalışmasının ikinci bölümünde, Türkiye’ de GSM sektörünün hacmi, kapasitesi ve büyüklüğü anlatılmıştır. Üçüncü bölümle beraber asıl anlatılmak istenen konuya giriş yapılmış, dolandırıcılık yöntem ve çeşitleri belirtilmiştir. Sorunun ve bu sorunun uygulanış şekilleri anlatıldıktan sonra dördüncü bölümle beraber problemin çözümüne yönelik bilgiler anlatılmıştır. Dördüncü bölümde hukuksal yapıya ve açıklara bakılmış, dolandırıcılık yapan kişilerin hukuksal olarak nasıl caydırılacağı belirtilmiştir. Hukuksal yapıya alternatif olarak beşinci bölümde dolandırıcılık girişimlerinin engellenmesi ve bunu yapan kişilerin takip edilebilmesi yönünden sistemsal bir yapı modeli öne sürülmüştür.

İKİNCİ BÖLÜM

2.TÜRKİYE'DE GSM SEKTÖRÜ

2.1.GSM Nedir?

Global System for Mobile Communications veya bildiğimiz adıyla GSM bir cep telefonu iletişim protokolüdür. Avrupa Telekomünikasyon Standartlar Komitesi'nin alt kuruluşu olan Groupe Spéciale Mobile ismini taşıyan GSM, daha sonraları sistemin küresel bir büyüklüğe erişmesiyle yeni adıyla anılmaya başlanmıştır.

En yaygın cep telefonu standardı olan GSM, 212 ülkede milyarlarca insan tarafından kullanılmaktadır. En kullanışlı özelliklerinden birisi kullanıcıların aynı hat ile değişik ülkelerden görüşme yapabilmeleridir.

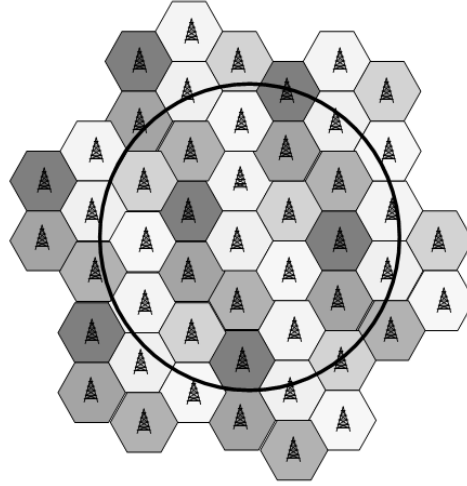
Tüm GSM standartları, hücresele ağ kullanır ve dolaşım sırasında bile hücreler arası geçiş yapma kabiliyetine sahiptir. Dolayısıyla teoride, eğer kapsama alanından çıkmazsanız, cep telefonu ile tüm dünyayı telefon konuşmasını kesmeden dolaşmak mümkündür.

GSM teknolojisi iki frekans bandıyla çalışır. Konuşmaların cep telefonları aracılığı ile baz istasyonlarına taşındığı 890-915 megahertz'lik alt band ve 935-960 megahertz'lik üst banttır.

Ayrıca bazı ağlarda Sayısal Hücresele Sistem standart da kullanılmaktadır. DCS, GSM ile aynı prensipte çalışmaktadır, ancak frekans bandı 1.8 gigahertzdır. [1]

GSM şebekesinin temelde üç bileşenden oluştuğunu söyleyebiliriz. Bunlar cihaz, baz istasyonu ve şebeke sistemidir.

Verilerin taşınabilme imkânı, özellikle iş dünyasındaki insanların ilgisini çekmektedir. [2]



Şekil.1. Şebekelerin Hücresel Görünümü

Kaynak: Yiğitbaşı, N. (2003). *Ağ Güvenliği*. (12 Kasım 2012) tarihinde http://web.itu.edu.tr/~orencik/AgGuvencigi2007Sunumlari/yigitbasi_gsm_rapor.doc alındı.

Şekil 1' e baktığımızda şebeke, hücelere bölünmüştür ve bütün hücreler altıgen şeklindedir. Hücrelerin bazıları aynı frekans bandında olduğu gibi farklı frekans bandında da olabilmektedir.

Hücrelerin altıgen olması sayesinde ise tekrar kullanılan bu frekansları kullanan kullanıcıların iletişimlerinin karışması önlenmektedir. [3]

Hücresel şebekelerde yüksek güçlü bir verici büyük bir alana hizmet verir. Düşük güçlü vericiler ise şekilde görünen hücelere hizmet vermektedir. Az önce belirtildiği gibi farklı hücrelerde aynı frekans kullanılabilir. Farklı frekansları kullanan hücreler bir “küme” oluştururlar.

Tüm şebeke kümelerin tekrarlanmasıdır oluşur. Yani bir şebekede pek çok küme bulunmaktadır.[4]

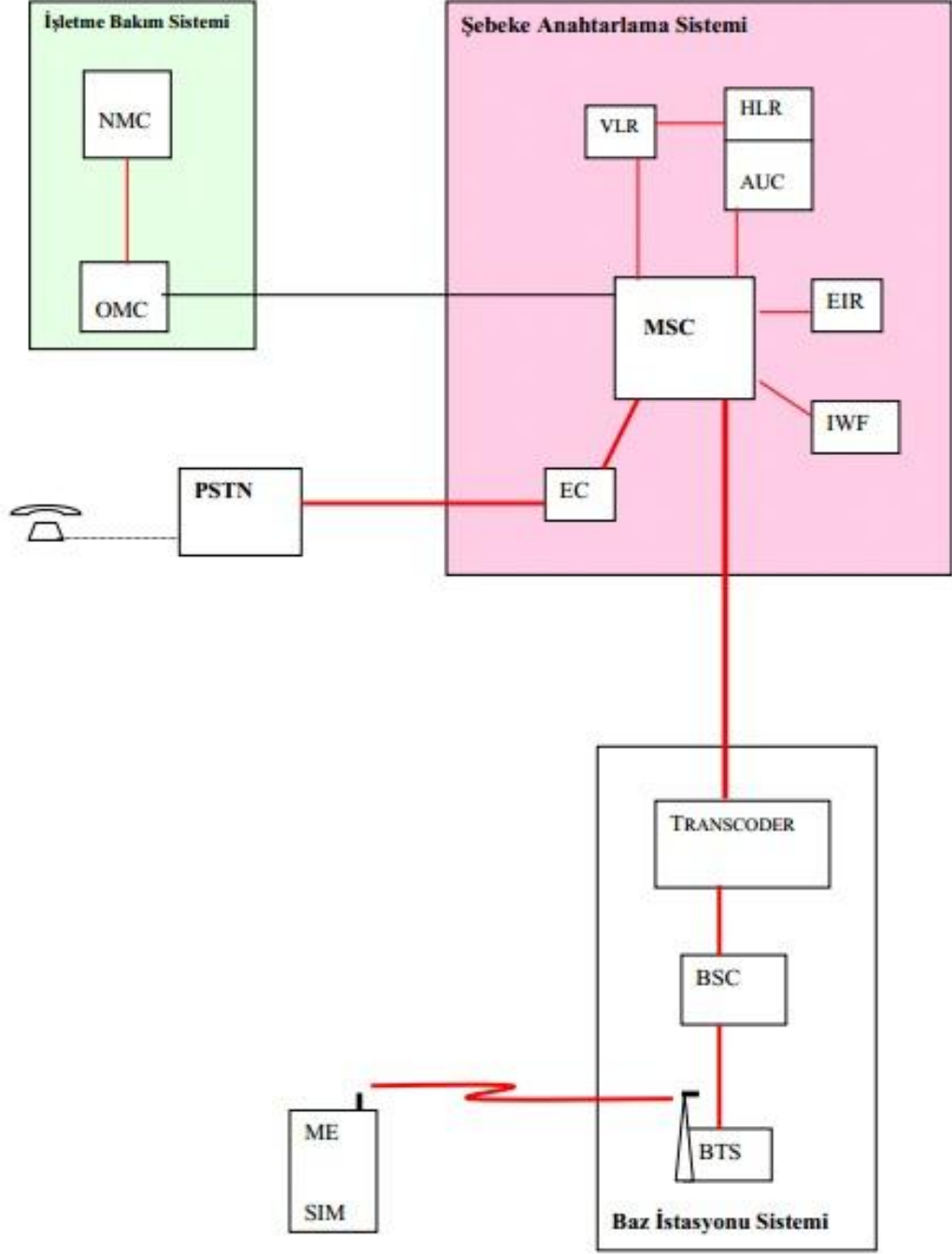
2.2.GSM Mimarisi

Bir GSM şebekesi üç bileşenden oluşmaktadır. Her bir şebeke bileşeni kendi içinde birden fazla ekipmandan oluşmaktadır. Genel olarak GSM şebeke yapısı ve elemanlar arasındaki bağlantı açık olarak ifade edilmiştir. Böylece bu standartlara göre üretilen ekipmanlar farklı üreticilerin markaları dahi olsa birbiri ile uyumlu çalışabilir. Örneğin; Motorola üretimi bir Baz istasyonu sistemi, Ericsson'a ait bir santral ile çalışabilir. Bu durum işletmeciler ve dolayısıyla aboneler için rekabet

edilebilir bir ortam saęlamakta ve esneklik her iki tarafın yararına olmaktadır. Standartlar bütün Őebeke elemanları ve yapıyı açık olarak tanımlamıŐ olmakla beraber bazı konularda teknik olarak sistem yararına olan durumlar için üreticiler esnek bırakılmıŐtır. Bu da birebir bütün elemanların deęil de ana bileŐenler bazında üreticiden baęımsız baęlantıyı mümkün kılmaktadır. Baz istasyonu, Baz istasyonu kontrol ünitesi ve Transcoder'dan oluŐan radyo sistemi (BSS: Base Station Sub-system) için bütün ekipmanlar aynı üretici grubundan olmak durumundadır.

Bazı iŐletim birimleri her ekipmanda birebir kurulmak yerine birleŐtirilerek ortak kullanılmakta ve daha verimli kılınmaktadır.[5]

GSM Őebekesi temelini oluŐturan bileŐenleri Őu Őekilde sınıflandırabiliriz, Mobile Station yani mobil istasyon denilen abonelerin görüŐme için kullanması gereken cihazlar, Base Station System denilen baz istasyonu sistemi, Network Switching System denilen santral sistemi, Operation and Maintenance System denilen iŐletme sistemi.



Şekil.2.GSM Şebekesi Alansal Gösterim

Kaynak: Can, E., *Mobil Cihazların Çalışma Sistemleri ve Çevre Üzerindeki Etkileri*, Yüksek Lisans Tezi, Gazi Üniversitesi, 2006.

2.3.Türkiye GSM Sektöründe Faaliyet Gösteren Şirketler

2.3.1. Operatörler

Türkiye GSM pazarında aktif olarak üç operatör hizmet vermektedir. Bunlar, Vodafone, Turkcell ve Avea'dır. Bu üç operatörü kısaca tanıyalım.

2.3.1.1.Turkcell

Şubat 1994'te Turkcell' in Türkiye'de hizmet vermesiyle ilk kez GSM temelli mobil iletişim başlamış oldu. Ulaştırma Bakanlığı ile 27 Nisan 1998'de imzalanan 25 yıllık GSM lisans anlaşması ile Turkcell, müşterilerine sunduğu mobil ses ve veri iletişimine dayalı hizmetlerin çeşitliliğini, kalitesini ve buna bağlı olarak müşteri sayısını da artırarak gelişimini sürdürmüştür.[6]

Turkcell üst üste dört yıl yer aldığı "INFO Tech 100" listesine 2007 yılında 83. sıradan girmiştir. Telekomünikasyon ve bilişim şirketlerinin Standard & Poor's kaynaklı finansal veriler bazında değerlendirilerek alındığı listeye, Turkcell, 20 telekomünikasyon şirketiyle birlikte, sayıları 10 bini bulan şirketlerin arasından seçilerek girmiştir.

Turkcell' in Fintur aracılığıyla sahip olduğu Azerbaycan, Kazakistan, Gürcistan ve Moldova'daki iştirakleri 31 Aralık 2007 itibarıyla 10,8 milyon aboneye, Kuzey Kıbrıs'taki iştiraki 300 bin aboneye ulaşmıştır. Turkcell' in Ukrayna'da çoğunluk hissesine sahip olduğu Astelit şirketi life, markası ile Şubat 2005'de GSM hizmetleri vermeye başlamıştır. life 31 Aralık 2007 itibarıyla 8,0 milyon aboneye sahiptir.

3G'de 110'dan fazla ülkede yaptığı anlaşmalar sonucu yurtdışı kullanımda dünyanın önde gelen operatörleri arasında yer alan Turkcell, ayrıca, GPRS dolaşımında 165'ten fazla ülkede yaptığı anlaşmalarla bu alanda dünyanın sayılı operatörlerden biridir.

2.3.1.2.Vodafone

Vodafone, İngiltere' de kurulan ilk GSM operatörü olarak 1 Ocak 1985 tarihinde İngiltere'nin ilk mobil görüşmesini yapmıştır. Şebekenin adı, cep telefonları üzerinden ses ve veri servislerinin sunulmasını simgelemek amacıyla Vodafone olarak seçilmiştir. İştirakleri, ortakları ve yatırımlarıyla Avrupa Kıtası'nda, Amerika Birleşik Devletleri'nde ve Uzak Doğu'da önemli bir konuma sahip olan Vodafone Grup, dünyanın en büyük mobil iletişim şirketidir. Vodafone, sahip olduğu küresel tecrübelerini kullanarak mobil iletişim dünyasındaki en yeni hizmet ve teknolojileri Türkiye'deki abonelerinin hizmetine sunmaktadır.[7]

Telecom adıyla telekomünikasyon sektörüne girmiştir. Kısa zamanda büyüyerek 1991 yılında bağımsız bir şirkete dönüşen ve Vodafone Group Plc adını alan şirket, 1999 yılında AirTouch Communications firmasıyla birleştikten sonra sektörde hızla büyümeye başlamıştır. Bir dizi birleşme ve satın almayla telekomünikasyon alanında dünya birinciliğine ulaşan Vodafone, şu anda birçok alt şirket ve iştirakiyle başta Avrupa, Kuzey Amerika ve Uzakdoğu olmak üzere tüm dünyada faaliyet gösteren dünyanın en büyük şirketlerinden biri haline gelmiş bulunmaktadır. Müşteri sayısı 2005 Eylül ayı itibariyle 171 milyon kişiye ulaşan Vodafone'un piyasa değeri de Kasım ayı itibariyle yaklaşık 80 milyar avro olarak hesaplanmaktadır.

2.3.1.3. Avea

Türkiye'nin ilk ve tek GSM 1800 operatörü olan Avea, 2004 yılında kurulmuştur. 2012 üçüncü çeyrek itibarıyla 13,2 milyon aboneye sahip olan Avea, Türkiye'nin en genç ve yenilikçi mobil iletişim operatörüdür. Yeni nesil şebekesi ile Türkiye nüfusunun %98'ine ulaşan şirket, "Avea" markası ile gerek kurumsal gerekse bireysel hizmetleriyle hızla büyümekte, gerek teknoloji ve altyapıya, gerekse yönetim ve 3000'e yakın çalışanına sürekli olarak yatırım yapmaktadır. [8]

2.3.2. Operatörler Hakkında

Türkiye pazarında faaliyet gösteren operatörlere ve geçmişlerine dair bilgilerine baktığımızda, sürekli gelişen, geliştikçe büyüyen ve kendini sürekli yenileyen şirketler olduğunu görmekteyiz. Operatörlerin bu kıyasıya rekabetinin tüketiciye faydasının olduğu aşikârdır.

Sürekli gelişen, geliştikçe büyüyen GSM sektöründen bir şekilde pay almak isteyen ve bunu kanun dışı yollarla yapacak olan şahıslar, sektörün içinde var olan açıkları keşfedecek, bu alanlardan içeri dalmak isteyecek ve bunu bir nebze olsa başaracaklardır. Operatörlerin görevi ise bu alanların önünü tıkamak ve gerçek müşterileri mağdur etmemektir.

İleri ki bölümlerde ayrıntılı şekilde işlenecek olan dolandırıcılık yöntem ve çeşitleri ve bunların engellenmesine yönelik çalışmalar yapılacaktır.

2.4. Türkiye GSM Pazarına Ait Bilgiler

2.4.1.Genel Pazar Verileri

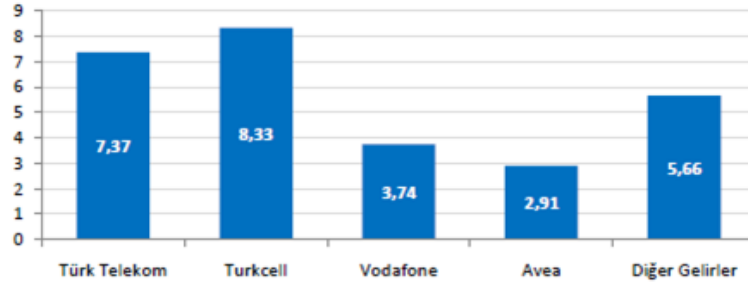
Telekomünikasyon sektöründe toplam gelirlerin yıllar itibariyle gelişimine bakıldığında özellikle mobil telekomünikasyon hizmetlerinden elde edilen gelirler başta olmak üzere artış yaşandığı görülmektedir. Tablo 1’de Türk Telekom ve mobil işletmecilerin 2008 yılından itibaren yıllık net satış gelir bilgilerine yer verilmektedir. 2010 yılında 21,2 milyar TL’ye yaklaşan toplam net satış gelirleri 2009 yılına göre %2,23 oranında artmıştır. 2011 yılında ise net satış gelirleri 21,7 milyar TL’ye yükselmiştir.[9]

Net Satış* (TL)	2008	2009	2010	2011
Türk Telekom	7.734.891.747	7.700.260.858	7.340.362.030	7.374.599.666
Turkcell	7.875.874.606	8.025.025.237	7.991.150.227	8.332.040.983
Vodafone	2.778.218.000	2.584.989.000	3.349.822.000	3.741.607.933
Avea	1.973.025.289	2.406.805.292	2.497.421.759	2.906.743.653
TOPLAM	20.362.009.642	20.717.080.387	21.178.756.016	22.354.992.235

Tablo.1. Yıllara Göre Net Satış Gelirleri

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

Şekil.3.'de 2011 yılı sonu itibariyle toplam telekomünikasyon hizmet gelirlerinin dağılımı gösterilmektedir. Pazarda Türk Telekom ve mobil işletmeciler haricindeki işletmecilerin net satış gelirleri toplamı 5,66 milyar TL olarak gerçekleşmiştir.[10]



Şekil.3. Toplam Gelirin İşletmeciler Arasındaki Dağılımı

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

Tablo.2.'de Türk Telekom ve mobil işletmecilerin üç aylık net satış gelirlerine yer verilmekte olup, söz konusu gelir bilgileri işletmecilerin BTK' ya bildirdiği kesinleşmemiş gelir bilgilerini içermektedir. 2012 yılı ikinci üç aylık

dönemde Türk Telekom ve mobil işletmecilerinin net satış gelirleri yaklaşık 6 milyar TL olarak gerçekleşmiştir.[11]

Net Satış (TL)	2012-1	2012-2
Türk Telekom	1.801.121.668	1.820.043.711
Turkcell	1.984.227.414	2.149.093.949
Vodafone	1.103.364.990	1.199.722.784
Avea	787.017.463	856.321.702
TOPLAM	5.675.731.536	6.025.182.146

Tablo.2. Yıllara Göre Operatörlerin Net Gelirleri

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

Tablo.3.'de ise Türk Telekom ve mobil işletmecilerin 2008-2011 yılları arasında elde ettikleri net kar rakamlarına yer verilmektedir.[12]

Net Kâr* (TL)	2008	2009	2010	2011
Türk Telekom	2.610.791.956	2.746.613.306	2.956.000.797	2.468.971.871
Turkcell	2.777.908.000	2.237.697.000	2.154.605.000	2.262.195.067
Vodafone	-582.206.309	-1.397.657.291	-239.277.770	-696.907.047
Avea	-514.343.382	-1.240.086.183	-962.938.607	-1.054.556.808

Tablo.3. Net Kar Değerleri

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

2.4.2. İşletmeci Yatırımları

Tablo.4.'de ve Tablo.5.'de sırasıyla Türk Telekom ve mobil işletmecilerin 2008-2011 yılları arasındaki toplam yıllık yatırım miktarlarına ve 2012 yılı üç aylık yatırım bilgilerine yer verilmektedir. Toplam yıllık yatırım bilgilerine bakıldığında 2011 yılı sonunda bir önceki yıla kıyasla Türk Telekom'un yatırımında %24,77 oranında bir artış görülmektedir. Aynı dönemler için Turkcell'in yatırımları %14,75 oranında artarken, Vodafone yatırımları %23,34, Avea yatırımları ise %4,64 oranında azalmıştır.[13]

Yatırım (TL)	2008	2009	2010	2011
T.Telekom	1.375.310.179	1.214.950.018	1.099.376.770	1.371.661.333
Turkcell	587.380.000	1.823.087.000	779.323.342	894.292.038
Vodafone	446.725.928	1.556.997.971	1.043.320.000	799.790.152
Avea	958.236.891	1.208.795.929	838.780.574	799.871.483
TOPLAM	3.367.652.998	5.803.830.918	3.760.800.686	3.865.615.006

Tablo.4. Yıllara Göre Yatırım Tutarları

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

Tablo.5.'de yer alan üç aylık yatırım bilgilerine bakıldığında; 2012 yılı ikinci çeyrekte Türk Telekom ve mobil işletmecilerin toplam yatırım miktarının yaklaşık 818,6 milyon TL olarak gerçekleştiği ve bir önceki çeyreğe göre toplam yatırım miktarında %7,71 oranında artış yaşandığı görülmektedir.[14]

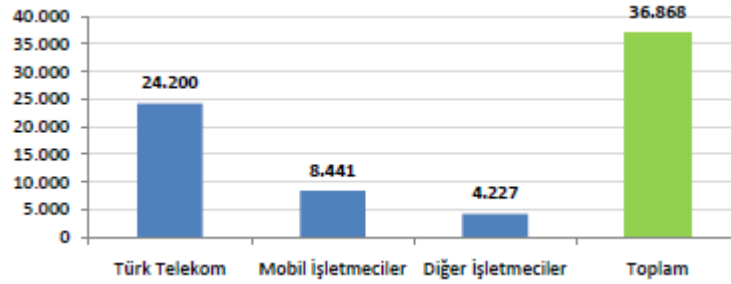
Yatırım (TL)	2012-1	2012-2
T.Telekom	232.399.025	445.353.927
Turkcell	160.000.762	166.538.135
Vodafone	232.241.513	72.443.449
Avea	135.360.448	134.255.772
TOPLAM	760.001.748	818.591.283

Tablo.5. Üç Aylık Yatırım Değerleri

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

2.4.3 İstihdam

Şekil.3.'de 2012 ikinci çeyrek dönemi itibariyle Türk Telekom, mobil işletmeciler ve sektördeki diğer işletmecilerin istihdam ettiği çalışan sayılarına yer verilmektedir. Türk Telekom'un çalışan sayısı 24.200, mobil işletmecilerin toplam çalışan sayısı 8.441 ve diğer işletmecilerin çalışan sayısı 4.227 olarak gerçekleşmiştir. 2012 ikinci çeyrekte sektörde toplam çalışan sayısı 36.868'dir.[15]



Şekil.4. Toplam Gelirin İşletmeciler Arasındaki Dağılımı, 2011, Milyar TL

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Üç Aylık Pazar Verileri Raporu*. (12 Kasım 2012) tarihinde http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, alındı.

2.5. GSM Sektöründeki Problemler ve Tanımlamalar

Daha önceki bölümlerden de anlaşıldığı üzere GSM sektörü sürekli büyümektedir. Ancak bu büyümeye paralel olarak güvenlik tedbirlerinin de geliştiği konusu muammadır. Bu tez çalışmasında, sektörün bu kolu mercek altına alınmıştır.

Sektör içerisindeki en büyük problemlerin başında dolandırıcılık olarak tabir edilen dolandırıcılık olayları gelmektedir. Bu tip işlemler neticesinde aboneler madur olmakta, operatörler ise büyük cezalar almaktadır.

Ancak öncelikle bazı terimlerin açıklanmasında fayda olacaktır. Bu tez çalışmasında Alternatif Kanal olarak belirtilen, operatörlerin elektronik mağazalar içerisindeki satış kanalları incelenmektedir.

Bu satış kanalında, operatörler, herhangi bir elektronik mağaza içerisinde müşterilere hizmet vermektedir. Bu hizmetlerin başlıcaları, faturalı ve faturasız hatlar, sim kart değişiklikleri ve kontratlı cihazlardır.

Dolandırıcılık girişiminde bulunan kişilerin öncelikli hedefi kontratlı cihazlardır. Bunun nedeni ise, müşterilerin işlemlerinin tamamlanmasının ardından, elektronik mağazadan çıkmadan önce, mağaza içerisindeki kasiyere fatura kestirmeleri ve bu fatura kestirme sırasında, cihaz kontratlı alındığı için hiçbir ücret vermeyecek olmalarıdır.

Kontratlı cihaz kavramı, herhangi bir abonenin, sözleşme imzalayarak cihaz bedelinin faturasına gelmesi olayıdır.

Dolandırıcılık teriminin, sektör içerisindeki anlamı, gerçek müşteri evrakları ya da belgeleri ile bu bilgileri ele geçiren şahısların gerçek abone yerine işlem yaptırmasıdır. Bunun yanında operatör çalışanı ile ortaklaşa yapılan dolandırıcılık girişimleri de bulunmaktadır. Operatör çalışanı, operatör sistemlerine abone bilgilerini girmeden, şahısa sözleşme imzalatır ve mağaza kasiyerine hiçbir bedel ödetmeksizin cihazı mağazadan çıkarır.

Tez içerisinde, dolandırıcılık girişiminde bulunan şahısların yöntemleri açıklanmış, hukuksal altyapıya bakılmış, yukarıda bahsi geçen iki dolandırıcılık çeşidinin önüne nasıl geçileceği belirtilmiş ve dolandırıcı kişilerin analizi yapılmıştır. Bununla beraber abonelerin bilgi ve belgelerinin nasıl korunacağına yönelik çözümler açıklanmıştır.

Yukarıdaki bilgilerin daha iyi anlaşılabilmesi adına tezde konu olan bazı kavramların detaylıca açıklanması önem arz etmektedir.

2.5.1. Faturalı Hat

Müşterilerin, BTK tarafından kabul edilen, kimlik bilgilerini gösteren bir belge ile adreslerini gösteren ikinci bir belge ile operatöre başvurması ve operatör tarafında da, abonelik sözleşmesi denilen bir başka belgeyi imzalayarak başvurdukları hat türüdür. Bu hat türünde, vergiler ve seçilen tarife ücreti, abonenin belirlediği bir tarihte aboneye gönderilmektedir.

Birçok operatör kampanyasının faturalı hat temeline oturması ve abonenin görüşme ücretinin daha sonradan aboneye gönderilmesi, alınan belgelerin doğru olmasının önemini arttırmaktadır.

2.5.2.Sim Kart Değişikliği

Hattı çeşitli nedenler ile kaybolan veya bozulan müşterilerin, operatörlerden, GSM numarası aynı kalmak koşulu ile başvurdukları işlemdir. Bu işlem türünde aboneden aynı şekilde, kimlik bilgilerini gösteren bir belge alınmakta ve sim kartı değiştirdiğine dair bir belge imzalatılmaktadır.

Bankacılık işlemlerinin telefonlara gelen onay mailinin ardından yapıldığı günümüzde, sim kart değişiklikleri yapılırken dikkatli olunması gerekmektedir. Zira dolandırıcılık girişiminde bulunan şahıslar bu alanı çok defa kullanmaktadır.

2.5.3. Kontrathlı Cihaz Kavramı

Faturalı hat sahibi müşterilerin, BTK tarafından da denetlenen ve düzenlenen bir sözleşmeyi imzalayarak, cihaz ücretinin faturasına, belirli aylara bölünerek gelmesi kurgusudur.

Operatörlerin belli şartlarını sağlayan abonelerin, cihaz bedeli direk faturalarına gelmekte, sağlamayan müşteriler ise belli bir ücreti kredi kartlarından çekmektedir. Dolandırıcılık girişiminde bulunacak şahıslar genellikle, tüm şartları sağlayan aboneler üzerinden işlemlerini yaptırmak istemektedirler.

Günümüzde akıllı cihaz olarak tabir edilen, i-Phone'lar, BlackBerry'ler ve bu tip pahalı cihazlar, dolandırıcı kişilerin en öncelikli hedeflerinin başında yer almaktadır.

2.5.4. Elektronik Mağaza Kavramı

Operatörlerin ürün ve hizmetlerini sunduğu birçok satış kanalı bulunmaktadır. Kurumsal satış kanalları, franchising diye tabir edilen bayi kanalları, alt bayi kanalları bunlardan bir kaçıdır. Bunlarla beraber Türkiye'de hizmet vermekte olan elektronik mağazalar içerisindeki operatöre ait noktalarda yapılan satışlar bulunmaktadır. Bu satış türü, alternatif satış kanalı olarak isimlendirilmektedir. Bu

noktalarda yapılan satışlar, öncelikle operatöre ait sistemlere girilir ve elektronik mağazaya ait kasalardan ürünün çıkışı ve faturalandırması sağlanır.

2.5.5. Operatör Sistemleri

Müşterilere verilen faturalı, faturasız hatların, kontratlı cihazların veya bunlar gidi diğer ürün ve hizmetlerin girişinin yapıldığı yazılım programlarıdır. Operatör çalışanı yaptığı işlemi öncelikli olarak bu sistemlere girmektedir. Bu sistemlere girilen çoğu işlem için, işlemi yaptıran müşteriden bir takım belgeleri almak, operatör çalışanın görevidir.

Operatör çalışanı aldığı bu belgeleri, operatöre ait sistemlere girişini yapar ve müşterilerin talepleri doğrultusunda işlemlerini gerçekleştirir. Bu işlemler, VPN denilen güvenli sanal özel ağ üzerinden operatöre ait sunuculara ulaşır ve kayıt altına alınır.

2.6. Türkiye’de GSM Sektörünün Yorumlanması

İlk çıktığı günlerde GSM, sadece cebinde parası olanın ya da işi dolayısıyla ona muhtaç olanın kullandığı bir gereçti. Günümüzde ise 7’ den 70’ e tüm insanların kullandığı bir elektronik ürün haline gelmiştir. Bunun başlıca 2 nedeninin olduğunu söyleyebiliriz. Bunlardan ilki, insanların tüm işlemlerini tek bir cihaz ve internet ile gerçekleştirebilmeleridir. Diğer bir nedeni ise, bu kadar işlemin gerçekleştirildiği bir cihazın boyutlarının oldukça küçük olmasıdır. İnsanlar her gittiği yere bu cihazı götürebilmektedir. İnsanlar bu küçük alet ile her türlü işlemini bir bilgisayara ihtiyaç duymadan yapabilmektedir.

Bu endüstrinin oyuncularını olan operatörler ve cihaz üreticileri aynı zamanda global oyunculardır. 70 milyonluk bir nüfusu ve hatırı sayılır bir gelir düzeyini baz aldığımızda, GSM teknolojilerinde dünyaya paralel gittiğimizi söyleyebilmekteyiz.

Mesleđi sektör dıřında olan insanlar bile, en az sektördeki insanlar kadar bilgi sahibi. Bunun nedeni reklamların haricinde, sürekli arařtıran, bilinçli tüketicide yatmaktadır. Tüketici aradığı bilgiye, günümüz şartları ile anında ulaşabilmekte ve kolaylıkla kıyaslama yapabilmektedir.

Sektör sürekli geliřmekte ve teknolojiler ile büyümektedir. Bu teknolojiye ve deđişimlere ayak uyduramayan, günü takip edemeyen ve çağın gerisinde olan firmalar yok olmaktadır.

Daha öncede belirtildiđi üzere kıyasıya bir rekabetin yaşandıđı bu sektörde, bazı kuralları belirlemek ve bu kurallar ekseninde herkese eşit mesafede olmak önemlidir. Bu günümüze kadar başarabilen, Bilgi Teknolojileri Kurumunun görev ve sorumlulukları önem arz etmekte ver her geçen gün katlanarak büyümektedir.

Data akışının artmasının başlıca nedenlerinden biri olarak 3G teknolojisinin hizmete girmiş olması ve Türk insanının sosyal alanlara olan eğilimi su götürmez bir gerçektir. Özellikle internet üzerinden video ve ses trafiđi data kaleminin büyük bir bölümünü oluşturmaktadır.

İnsanların istedikleri bilgiye mobil olarak ulaşabilmeleri ve tüm işlemlerini bir cihaz üzerinden yapabilmeleri kişilere büyük fayda sağlamaktadır. Bu bakımdan, GSM sektörünün, beklide bitmek tükenmek bilmeyen bir endüstri olduđu gerçektir ve sürekli büyüyecektir.

Bunun yanı sıra gelecekte şimdiki bildiđimiz anlamda GSM operatörlerinin işlevinin azalacağı da kimi çevrelerce öngörülmektedir. Akıllı telefonların artışıyla birlikte internet üzerinden ücretsiz görüşme imkanının olması ve bu kanalın geliřmesi ile operatörlerin bu işlevinin azalacağı tahmin edilmektedir. Bu açıdan bakıldığında ise sektörün ilerleyen zamanlarda büyük bir rekabete girmesi ve kurumların farklı inovatif çözümlerle müşterilerine farklılık yaratarak onları elinde tutması önem arz etmektedir.

Telekomünikasyon sektöründe bir kurumun, müşteriye kendinde tutması için harçayacağı zaman ve para, müşteriye kaybettikten sonra geri kazanabilmesi için harçayacağı zaman ve paradan çok daha azdır. Bu açıdan bakıldığında, kurumların farklılık yaratmak için zaman kaybetmemesi ve anında uygulamaya sokması son derece önemlidir.

ÜÇÜNCÜ BÖLÜM

3. SEKTÖRDEKİ SAHTEKARLIK ÇEŞİTLERİ VE YÖNTEMLERİ

GSM sektörü, bir önceki bölümde anlatıldığı üzere sürekli büyüyen, gelişen ve kendisine doğrudan ya da dolaylı olarak bağlı birçok ekosisteme kazanç sağlayan bir alandır. Ancak bu kazançtan yasa dışı yollarla kar elde etmek isteyen gruplarda yok değildir.

Bu bölümde, sektör içerisindeki dolandırıcılık çeşitleri ve yöntemleri ele alınacaktır.

3.1. Kişiyi Gösterir Belge Dolandırıcılığı

Kişiyi gösterir belgeler, BTK tarafından belirtilen, şahsın isim, soy isim, doğum tarihi gibi bilgileri içeren belgelerdir. Bunların bazıları, nüfus cüzdanı, kamu kurum kimliği ve ehliyettir. Bu tip resmi belgelerin birçoğunda güvenlik tedbirleri yer almaktadır.

Dolandırıcılık girişiminde bulunacak kişiler, elde ettikleri şahıs bilgileri ve belgeleri ile operatöre ait satış noktasına gelir ve işlem yaptırır.

Bu tip evraklarda dikkat edilmesi gereken bazı noktalar bulunmaktadır.

3.1.1. Kimlik Seri Numarası

Kimlik seri numarası, erkeklerde tek bayanlarda çifttir. Seri numarasının yazım karakteri özeldir.

3.1.2. Türkiye Cumhuriyeti Kimlik Numarası

Kimlik numarası 11 hanelidir ve kişiye özeldir. İşlem yaptıracak abonelerin kimlikteki T.C. kimlik numarası ve operatördeki bilgileri karşılaştırılmalıdır.

3.1.3. Soğuk Mühür

Kimlik, ehliyet gibi özel belgelerde soğuk mühür bulunmaktadır. Soğuk mühür bulunmayan kimlikler sahtedir.

3.1.4. Diğer Dikkat Edilmesi Gereken Noktalar

Kimliklerde yer alan doğum tarihi ile kimlik veriliş tarihi arasındaki fark alınarak, fotoğrafa bakılır. Şahısların, kimlik yaşları ile fotoğrafları uyumlu olmalıdır

Kimlik seri numarasında, mor ışık altında matlaşma görülmektedir.

Ocak 2001 tarihi sonrasında nüfus müdürlüklerine gönderilen genelgede, kimliklerde ortalama yazım getirilmiştir. Bu tarihten sonra verilmiş bir kimlikte, sola veya sağa dayalı yazım karakteri olan kimlikler sahtedir.

3.2. Adres Gösterir Belge Dolandırıcılığı

Adres gösterir belge, BTK tarafından belirtilen, elektrik, su ve doğalgaz faturaları ile ikametgâh gibi şahsın adresini belirten belgelerdir.

Müşteriler faturalı hat almak istediklerinde mutlaka suretle bu belgeyi vermek zorundadırlar.

Bir satış noktasına giden ve dolandırıcılık girişiminde bulunacak kişiler, sahte adres gösterir belgeleri verebilmektedirler. Bu açıdan bu belgelerinde iyi incelenmesi gerekmektedir.

3.3. Sim Kart Dolandırıcılığı

Günümüzde birçok bankacılık işlemi, cep telefonlarına gönderilen onay SMS ile yapılmaktadır. Dolandırıcılık yapacak şahıslar, elde ettikleri müşteri bilgileri ile bu işlemi gerçekleştirememektedirler. Bunun için, sahte olarak düzenledikleri, kişi gösterir belge ile operatöre başvururlar. Şahıslar, elde etmek istedikleri GSM numarasına ait sim kart için yedek sim kart başvurusunda bulunur ve kartı alırlar. Sim kartı elde eden şahıslar, onay SMS' inin akabinde müşteriye ait bankadan işlemi yaptırırlar.

3.4. Operatöre Ait Bilgisayarları Ele Geçirme

Operatör sistemlerinin ele geçirilmesi amacıyla girişimde bulunan şahıslar, belge dolandırıcılığına nazaran çok daha büyük tehlike arz etmektedirler. Birçok müşteriye ait bilgi ve dokümanın bulunduğu bu bilgisayarlar, bu şahıslar için vazgeçilmez bir nimet olmaktadır. Bu yöntemlerden en önemlilerini açıklayalım.

3.4.1. Truva Atları

Truva atı efsanesi hemen her kesim tarafından bilinmektedir. Truva şehri, hiçbir şekilde savaşılarak fethedilemez, bunun üzerine sanki bir hediyeymiş gibi şehre bir at gönderilir ve bu atın içerisine saklanmış olan askerler tarafından şehir fethedilir.

Truva atları aynı mantık ile çalışmaktadır. Normalde faydalıymiş gibi gözükken bir programın içerisine yerleştirilmiş olan bu zararlı programcıklar, arka planda bir çok bilgiyi göndericisine iletmektedir. Bilgilerin iletilmesinin haricinde, göndericisine bilgisayar kontrolü de sağlayarak işlem yapabilmesini gerçekleştirir.

Truva atları ile operatöre ait programların giriş şifreleri ele geçirilebilmekte, müşteri evrak ve dokümanları alınmakta, operatöre ait bir bilgisayardan diğer başka bilgisayarlara erişim sağlanabilmektedir.

3.4.2. Şifre Kırıcılar

Password creaker denilen bu yöntemde amaç kaynak bilgisayarın yani operatöre ait bilgisayarların kullanıcı adlarını ve şifrelerini ele geçirmektir. Tahmin etme, sözlük saldırısı ve kaba kuvvet olarak üç yöntemi bulunmaktadır. Diğer yöntemlere oranla başarı oranı düşüktür. Bunun nedeni ise, operatör sistemlerinin belli bir hatalı şifre giriş izni vermesidir. Daha sonra, şifreler bloke edilmektedir.

3.4.3. Tuş Kaydediciler

Mail, sahte web sitesi gibi çeşitli yollarla bilgisayarlara gönderilen ve keylogger olarak nitelendirilen bu yöntemde, operatörlere ait bilgisayarlarda, girilen tuşlar, internet siteleri, belirli aralıklarla ekran görüntüsü alıcısına gönderilmektedir.

3.4.4. Koklayıcılar

Sniffer olarak nitelendirilen bu yöntemde, ağ üzerinde akan bilgiler takip edilmektedir. Koklayıcılar bir program veya donanım olabilmektedirler. Bu programlar ağ trafiği üzerinde herhangi bir değişiklik yapmaz ya da müdahale etmezler, bu nedenle tespit edilebilmeleri oldukça güçtür.

3.5. Bilgi Elde Etme Girişimleri

Kimyada, yapı olarak birbirinden farklı iki madde zararsız olarak görülebilir. Ancak bu maddeler bir araya getirildiğinde güçlü bombalar yapılabilmektedir. Bu yöntemde aslında bunlardan birisidir. Bir müşteriye ait bilgileri ele geçirme çabasında olan şahıslar, operatöre ait bir satış noktasına giderek hatlarla ya da müşteri ile ilgili ufak zararsız olarak nitelendirilebilecek bilgiler elde edebilirler. Aynı kişiler başka bir noktaya daha giderek başka bilgiler elde ederler. Bu bilgiler daha sonradan birleştirildiğinde, o müşteriye ait aslında tüm bilgiler elde edilmiş olunur.

3.6. Operatör Çalışanı İle Ortaklaşa Dolandırıcılık Girişimi

Bu yöntemde, operatör çalışanı, dolandırıcılık yapacak olan diğer şahıslar ile ortaklaşa hareket etmektedir. Ancak en büyük sorun, alınan cihazın faturalandırması esnasında istenen sözleşmedir. Şahıslar bunu bildikleri için bir takım yöntemler ile bunu aşarlar. Operatör çalışanı, şahısların kimliklerini alır ve sözleşme imzalatırlar. Ancak operatör sistemlerine girişi yapılması zorunlu olan kontratlı cihaz girişini bilerek yapmazlar. Sözleşme, kimlik ve alınmak istenen cihaz veya cihazlarla faturanın kesileceği alana giderler ve faturayı kestirirler. Daha sonradan operatör sistemleri incelendiğinde böyle bir girişin olmadığı fark edilir. Cihaz yada cihazlar mağazadan çıkmış olur, operatör çalışanı ise kayıplardadır. Bu yönetime bakacak olursak şahıslar, çoğu zaman kendi adamlarını, operatörlere sokmaktadır.

3.7. Trafik Taşıma Yöntemi

Bu yöntemde, yurtdışı kaynaklı bir telefon numarası aranmaktadır. Aranılan numara, Türkiye'deki 900'lü hatlar ile benzer özelliktedir. Şahıs, o numarayı aradıkça, aranılan numara sürekli trafik almakta, bunun karşılığında ise ücret talep etmektedir. Türkiye'de alınan hat ise sahte belgelerle alınmıştır.

3.8. Değerlendirme

Tezin bu aşamasında, konuyu daha iyi kavrayabilmek amacı ile sektörün bu alanı ile ilgili operatörlerin önde gelen isimleri ile tanışma ve tartışma fırsatım olmuştur. Hızlı gelişen GSM sektörü kadar, hızlı gelişen dolandırıcılık çeşitleri olduğunu öğrendik. Özellikle dolandırıcılık girişiminde bulunacak şahısların her

zaman bir adım önde olduğu, operatörlerin ise bu açıkları anında öğrenip kapatmak olduğu kanısına vardık. Ancak bu süreç zarfında hiçbir şeyden haberi olmayan müşterilerin mağdur olacağı gerçeğini de göz ardı etmememiz gerekmektedir.

Şahısların özellikle GSM sektörünü hedef almalarının asıl nedeni ise hepimizin bildiği yükte hafif, pahada ağır olgusu içerisinde olan yüksek değerli cihazlar. Bu türden cihazların, piyasa içerisinde anında alıcı bulması ve talebin fazla olması, herkes gibi dolandırıcı kişilerinde bu alana yönelmesinde önemli bir etken olmuştur.

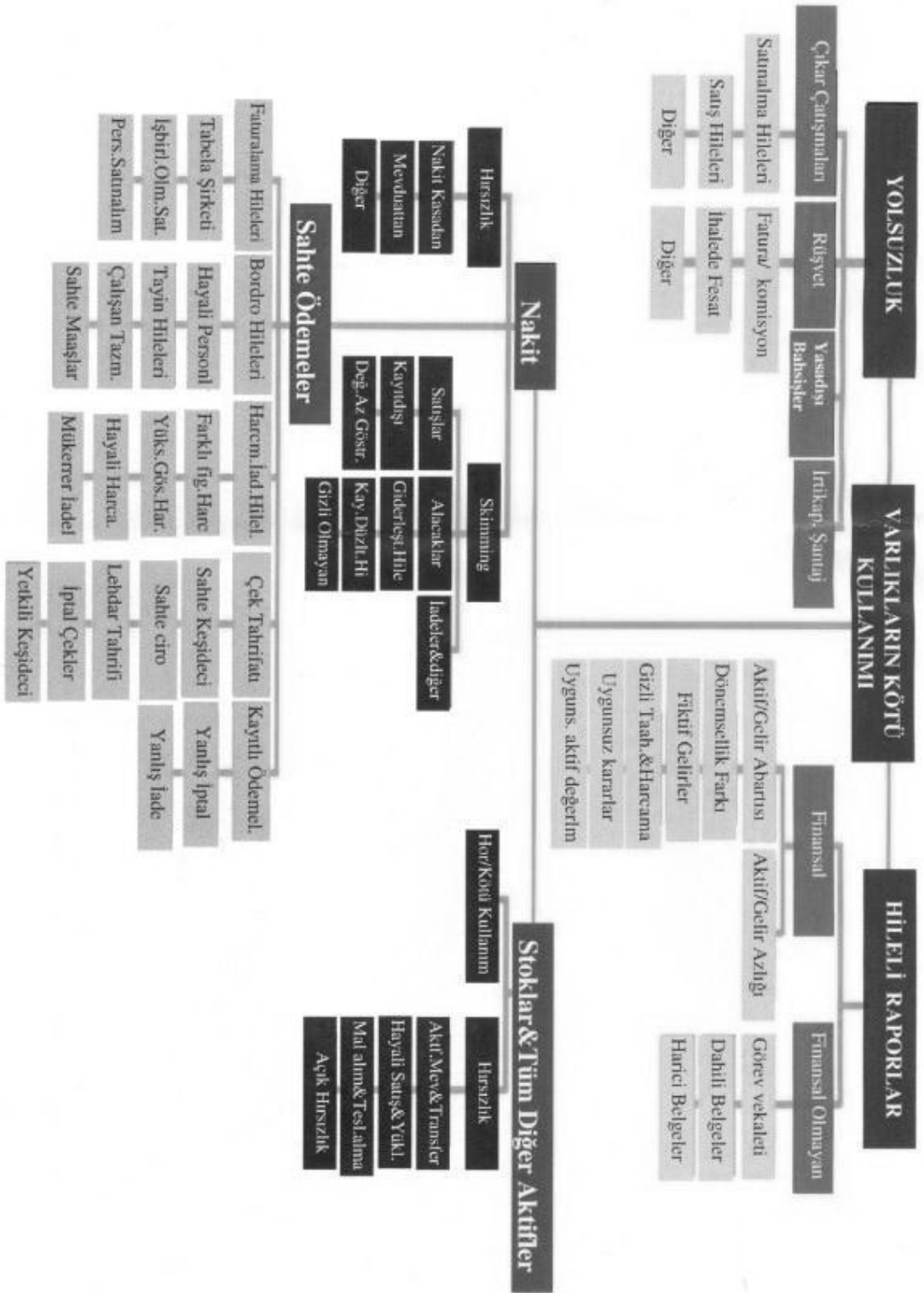
Bankacılık işlemleri konusunda, özellikle Vodafone' un, BTK' ya ve bankalara göndermiş olduğu bir çözüm önerisi dikkatimi çekmiştir. Buna göre, eğer herhangi bir sim karta son 6-12 saat içerisinde yedek sim kart çıkartılmış ise, bu değişiklik Vodafone tarafından bankaya bildirilmekte ve şifrenin gönderilmesi engellenmektedir. Böylelikle, önemli ölçüde büyük bir dolandırıcılığın önüne geçilebilmektedir.

Bunun yanında operatörler, kendi kara listelerini ve müşteri profillerini oluşturmaktadır. Buna göre riskli müşteri analizi yapılmakta ve takibi sağlanmaktadır.

Görüşmelerimiz sırasında gazetelere de haber olmuş çok ilginç bir olay ile tanıştık. Şanlıurfa' da 70 köyde toplam 3500 kişinin kontör dolandırıcılığı yaptığı ve jandarmanın yapmış olduğu baskın sırasında yaşları 14 ile 17 arasında değişen gençlerin bulunduğu ve bu gençlerinde yapılan araştırma neticesinde ikna kabiliyetlerinin yüksek olduğu görülmüştür. [38]

Türkiye'de hizmete sokulmaya çalışılan çipli kimlik kartları ise, belirtilen tarih geçmesine rağmen güvenlik sebepleri nedeni ile henüz yürürlüğe girmemiştir. Çipli kimlik kartlarının güvenlik seviyelerinin yüksek olması gerekmektedir. Aksi takdirde, mevcut durumdan çok daha kolay bir şekilde ve zahmetsiz müşteri bilgileri değiştirilebilecektir.

Sektör yöneticilerinden aldığımız ve ACFE, tarafından gönderilen görüntüde ise, sadece GSM değil, tüm sektörlerdeki dolandırıcılık olayları gruplandırılmıştır.



Tablo.6. Dolandırıcılık Olaylarının Tablolaştırılmış Görüntüsü

DÖRDÜNCÜ BÖLÜM

4. SEKTÖRDEKİ MEVCUT KANUNLAR VE AÇIKLAR

Üçüncü bölümde anlatılan, Sahtekârlık Yöntem ve Çeşitleri başlığı ile ilgili hukuksal düzenlemeler bu bölümde incelenecektir. Sahtekârlık girişimlerinin engellenmesine ve önüne geçilmesine yönelik adımlardan birisi olan yasal düzenlemeler ile ilgili çalışmalar incelenecektir. Bu bölümdeki yasal düzenlemeler iki kısma ayrılacaktır. Operatör sistemlerinin, yani operatörlere ait bilgisayarların ele geçirilmesine yönelik bilişim suçları, bir diğeri ise evrakta sahtecilik suçlarıdır.

4.1. Bilişim Suçları ile İlgili Düzenlemeler

80’li yıllarla beraber kişisel bilgisayarların kullanımının Dünya’da hızlı bir şekilde artmaya başlaması, bununla beraber 90’lı yıllarda da bilgisayarların birbirlerine bağlanarak kendi aralarında veri transferini gerçekleştirebilecekleri teknolojilerin gelişmesiyle birlikte, ülkemizde de bilgisayarın kullanılması yaygınlaşmaya başlamıştır.

Türk hukukunda siber suçlarla ilişkin ilk düzenleme, 6.6.1991 tarih ve 3756 sayılı Kanunun 20’nci maddesi ile 756 sayılı TCK’nın ikinci kitabına ‘‘Bilişim Alanında Suçlar’’ adıyla 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir bab ilave edilmesidir. [16]

1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Kanununda (TYCK) siber suçlar, ‘‘ Bilişim Alanında Suçlar’’ adıyla ikinci kitabın Toplum Karşı Suçlar başlıklı Üçüncü Kısımının 10’uncu Bölümünde 4 madde (m.242-244-245-246) halinde düzenlenmiştir.

Bunlar, ‘‘haberleşmenin gizliliğini ihlal suçu’’(m.132), ‘‘haberleşmenin engellenmesi suçu’’ (m.124), ‘‘hakaret suçu’’(m.125), ‘‘bilişim sistemlerinin kullanılması yoluyla işlenen hırsızlık suçu’’(m.142 fkr.2 b. ‘‘e’’), ‘‘bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu’’(m.158 fkr.1 b. ‘‘f’’) ve ‘‘müstehcenlik suçu’’ dur (m.226).[17]

Suçun oluşması için gerekli şartlar hukuka aykırı olarak bilişim sisteminin bir kısmına veya tamamına girilmiş olması yeterli kabul edilmemekte, aynı zamanda giriş yapılmasının akabinde de belirli bir süre devam etmesi yani suçlunun bir süre bilişim sisteminde kalması gerekmektedir.

243'üncü maddede "orada kalmaya devam etme" eylemi suçun bir unsuru olarak düzenlenmiş olmasına rağmen, kalmaya devam etme eyleminin süresinin ne kadar olacağı konusunda madde metninde ve gerekçesinde açıklık yoktur. Yalnız, "orada kalmaya devam eden" ifadesi, "kalan" sözcüğüne nazaran zihinde daha geniş bir anlam oluşturmaktadır. [18]

Operatör sistemlerine illegal yollarla giriş yapmış şahısların, istedikleri bilgileri elde edip, sistemlerden çıkışının akabinde, yukarıda bahsi geçen, "orada kalmaya devam etme" hükmünü yerine getirmemiş olacaklardır. Buna istinaden, sadece sistemlere izinsiz girişten yargılanmaları, kanunda belirtilen nitelikler sağlanmadığı için kimi durumda güç olmaktadır.

4.1.1. Ceza İndirimi

243'üncü maddenin ikinci fıkrasında yasadışı bilişim sistemine girme ve orada kalma suçu, bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi hali, daha az ceza verilmesini gerektiren bir durum olarak düzenlenmiştir. Madde metninden ve gerekçesinden bedeli karşılığı yararlanma kavramıyla tam olarak neyin kastedildiği anlaşılmamaktadır.

İnternet üzerinden ücret karşılığı hizmet veren internet siteleri, internet kafe gibi yerlerde olduğu üzere belli bir bedel karşılığı bilişim sistemlerinin kiralanması, bir kuruluş tarafından belli bir sistemin bedel karşılığı sunulması ve belli bir süre internet servisinin sağlanması olarak ifade edilmiştir.[19]

4.1.2. Cezanın Ağırlaştırılması

Hukuka aykırı bir bilişim sistemine girme ve orada kalma fiili nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi durumunda, kanun koyucu bu durumu anılan suç bakımından cezanın ağırlaştırılmasını gerektiren bir sebep olarak düzenlemiştir.

Eğer failin, verileri yok etmek veya değiştirmek kastıyla hareket etmişse bu maddeden değil, YTCK m.244’de düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan dolayı cezalandırılması gerekecektir.[20]

4.1.3. Yaptırım

Suçun basit şekli için öngörülen yaptırım, bir yıla kadar hapis ya da para cezasıdır. Burada hâkim ulaştığı sonuca göre faile ya hapis ya da para cezası verecektir. Kanunun açık hükmü uyarınca hapis ve para cezası bir arada verilemeyecektir. Bu düzenleme ile hâkime takdir yetkisi tanınmıştır. Ayrıca YTCK’nın 49’uncu maddesinin 1’nci fıkrasına göre, sürekli hapis cezası kanunda aksi belirtilmeyen durumlarda bir aydan az yirmi yıldan fazla olamaz. Bu sebeple, 243’üncü maddenin 1’nci fıkrasındaki hapis cezanın alt sınırı bir aydan başlamaktadır.

Suçun, bedeli karşılığında yararlanabilen sistemler hakkında işlenmesi halinde ise yaptırım yarı oranda indirilecektir. Yasadışı erişim nedeniyle sistemin içerdiği veriler yok olur veya değişirse yaptırım, altı aydan iki yıla kadar hapis cezasıdır.[21]

4.2. Belge Sahteciliği İle İlgili Düzenlemeler

Resmi belgelerde yapılan sahtecilik, operatörlere ait satış kanallarında sıkça rastlanan bir durumdur. Şahıslar kimi zaman elde ettikleri bilgiler ile belge oluşturmakta, kimi zaman ise, resmi belgeler üzerinde oynama yaparak, operatörlere ait satış noktalarından yüksek değerli cihazlar almak istemektedirler.

Sahtecilik suçları 5237 sayılı TCK’nin “Topluma Karşı Suçlar ”başlıklı üçüncü kısmının “Kamu Güvenine Karşı Suçlar” isimli 4. Bölümde, 204-212’nci maddeler arasında düzenlenmiştir. Resmi Belgede Sahtecilik Suçu TCK’nin 204’ncü maddesinde düzenlenmektedir. TCK’nin 210’ncü maddesinde ise resmi belge hükmünde olan özel belgeler düzenlenmektedir.[22]

4.2.1. Korunan Hukuki Deęer

Bu suçta korunan hukuki deęerin “Kamu Güveni” olduęu genel kabuldür, ancak bu suçla korunan hukuki deęerin “Özel Mülkiyetin, Devlet İdaresinin” olduęu da kabul edilmektedir. Sonuç olarak diyebiliriz ki bu suç ile korunan iki ayrı hukuki yarar var.[23]

4.2.2. Suçun Unsurları

Bir şahsa evrak sahtecilięi suçundan, işlem yapılabilmesi için öncelikle suçun oluşturan unsurların gerçekleşmesi gerekmektedir. Bunlar, resmi belgeyi sahte olarak düzenlemek, resmi belgeyi başkalarını aldatacak şekilde deęiştirmek, aldatma kabiliyeti ve sahte resmi belgeyi kullanmaktır.

Bu seçimlik hareketler yukarıda sayıldıęı gibi resmi belgeyi sahte olarak düzenlemek, gerçek bir resmi belgeyi başkalarını aldatacak şekilde deęiştirmek veya sahte resmi belgeyi kullanmaktır. Bu üç seçimlik hareketten herhangi birisinin icra edilmesi ile fiil tamamlanmaktadır.[24]

4.2.3. Resmi Belgeyi Sahte Olarak Düzenlemek

Bu fiil gerçekte var olmayan resmi bir belgeyi sahte olarak düzenlemek şeklinde ortaya çıkar. Burada yapılan bir taklittir ve resmi belgeden farksız, aldatıcı özellięi olan bir taklittir, sıradan bir taklit deęildir. Buradaki aldatıcılık özellięi suçun unsurudur. Bu belgenin özel bir işlem haricinde veya uzman olmayan kişiler dışında anlaşılır olmaması gerekir. [25]

4.2.4. Resmi Belgenin Deęiştirilmesi

Mevcut bir resmi belgeyi üzerinde deęişiklikler yapmak suretiyle başkalarını aldatıcı hale getirmek fiilidir. Buna verilecek örnek mevcut bir kimlik belgesinde deęişiklik yaparak başka bir isme düzenlemektir.[26]

4.2.5. Sahte Resmi Belgeyi Kullanma

Burada kiři sahte bir resmi belgeyi kullanırsa; örneđin sahte bir çeki piyasaya ciro ederse sahte resmi belgeyi kullanma suçunu işlemiř olur. Ancak sahte resmi belgenin bilerek kullanılması gerekir, örneđin sahte bir çeki ciro yoluyla edinen, aldatıcı özelliđinden ötürü çekin sahte olduđunu bilmeyen ve bu çeki ciro yoluyla dolařıma koyan kiři suçun manevi unsuru oluřmadıđı için sahte resmi belgeyi kullanma suçunu işlemiř olmaz.[26]

4.2.6.Fail ve Mađdur

Resmi Belgede Sahtecilik suçunun faili herkes olabilir. Suçun bir kamu görevlisi tarafından işlenmesi hali ađırlařtırıcı nedendir.[27]

4.2.7. Suçun Konusu

Suçun konusunu Resmi Belge veya TCK 210 uncu madde ile “resmi belge hükmünde sayılan belgeler” oluřturur.[28]

4.2.8. Manevi Unsur

Failin suçu, suçun unsurlarını bilmesi ve sonucu istemesi gerekmektedir. Sanık işlediđi suçun farkında deđilse, sonucu istememiřse suç oluřmaz. Resmi evrakta sahtecilik suçlarında kiřinin zarar verme bilincinin bulunması ve bunun ispat olunması gerekir.[29]

4.2.9. Yaptırım

Resmi belgede sahtecilik yapan kiřiler ve suça ortak olanlar, ilgili kanun hükmü ile cezalandırılırlar.

4.2.9.1. Resmi Belgede Sahtecilik Suçu

MADDE 204. - Bir resmî belgeyi sahte olarak düzenleyen, gerçek bir resmî belgeyi başkalarını aldatacak şekilde deđiřtiren veya sahte resmî belgeyi kullanan kiři, iki yıldan beř yıla kadar hapis cezası ile cezalandırılır.[30]

Görevi geređi düzenlemeye yetkili olduđu resmî bir belgeyi sahte olarak düzenleyen, gerçek bir belgeyi başkalarını aldatacak şekilde deđiřtiren, gerçeđe

aykırı olarak belge düzenleyen veya sahte resmî belgeyi kullanan kamu görevlisi üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.[31]

Resmî belgenin, kanun hükmü gereği sahteliği sabit oluncaya kadar geçerli olan belge niteliğinde olması hâlinde, verilecek ceza yarısı oranında artırılır.[32]

4.2.9.2. Resmi Belgeyi Bozmak Yok Etmek veya Gizlemek

MADDE 205 Gerçek bir resmî belgeyi bozan, yok eden veya gizleyen kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Suçun kamu görevlisi tarafından işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.[33]

4.2.9.3. Resmi Belgeyi Çıkartmak Adına Yalan Beyanda Bulunmak

MADDE 206 Bir resmî belgeyi düzenlemek yetkisine sahip olan kamu görevlisine yalan beyanda bulunan kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.[34]

4.2.9.4. Resmi Özel Belgede Sahtecilik

MADDE 207. Bir özel belgeyi sahte olarak düzenleyen veya gerçek bir özel belgeyi başkalarını aldatacak şekilde değiştiren ve kullanan kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.[35]

Bir sahte özel belgeyi bu özelliğini bilerek kullanan kişi de yukarıdaki fıkra hükmüne göre cezalandırılır.[36]

4.2.9.5. Özel Belgeyi Bozmak Yok Etmek veya Gizlemek

MADDE 208. Gerçek bir özel belgeyi bozan, yok eden veya gizleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.[37]

4.3. Kanunların Tartışılması ve Değerlendirme

İnternet yolu ile operatör sistemlerine illegal giriş yapılması, Bilişim Suçlarını kapsamaktadır. Kanunda belirtilen, “ orada kalmaya devam etme” niteliği tanım olarak yorumlara açıktır. Kanunun bu bölümünün net olarak belirtilmesi önem arz etmektedir. Operatör sistemlerinde, birçok müşterinin bilgileri saklıdır. Dolayısıyla, “orada kalmaya devam etme” niteliği haricinde, sistemlere girişin yani yeltenmenin

suç olarak kabul edilmesi, açık ve caydırıcı bir kanun hükmüne bağlanması gerekmektedir.

Resmi belgelerde yapılan sahtecilik unsuru ile ilgili en dikkat edilmesi gereken noktalardan bir tanesi ise aldatıcılık özelliğidir. ‘‘Bir belgenin özel bir işlem haricinde veya uzman olmayan kişiler dışında anlaşılır olmaması gerekir’’ ifadesi, suçun oluşması için gerekli şart olarak anılmaktadır. Bu hükme istinaden, Sahtekârlık girişiminde bulunacak şahıs ya da şahıslar, ceza almamak veya suç unsuruna göre indirimden yararlanabilmek adına, belgelerde gözle görülür kusurlar bırakmaktadır. Bu hükmün müşteriler, ya da mağdur olan/olabilecek kişiler lehinde genişletilmesi ve düzenlenmesi gerekmektedir. Zira operatörün satış noktasına gelen şahısların niyeti, şirketi dolandırmaktır.

Kişi gösterir belgelerden olan, nüfus cüzdanı, ehliyet gibi resmi belgelerini kaybeden şahıslar, dilekçe ile emniyet ve nüfus müdürlüğüne başvurmaktadır. Bu sırada, kimliğini kaybeden şahsın mağdur olmaması adına, kimliğinin kaybedildiğini bildiren veriler, vergi dairesi veri tabanına işlenmektedir. Aynı şekilde, bu müşteriler adına işlem yapılmaması için, bir yasal düzenleme ile BTK aracılığıyla operatörlere de bilgi verilmeli ve operatörler de kendi sistemlerine işlemeleridir.

BEŞİNCİ BÖLÜM

5. SAHTEKARLIK GİRİŞİMLERİNİN ENGELLENMESİ VE TAKİBİ

Alternatif satış kanallarında, yükselen sahtekarlık olayları akabinde, bu girişimlerin engellenmesine yönelik bir takım çalışmalar yapılmıştır. Daha önceki bölümde anlatılan, ‘‘Sahtekarlık Yöntem ve Çeşitleri’’ dikkate alınarak, sistem kurgulanmış ve satış kanallarında hizmete sokulmuştur.

Bunlardan ilki, satış kanallarında operatörün kendini güvenceye aldığı sistem olan SISNET projesidir. SISNET kelimesi, İngilizcede Shop in Shop .NET baş harflerinden gelmektedir. Bu sistem, NICEYE yazılım şirketi desteği ile, BRIGHTSTAR proje geliştirme müdürümüz, Sn. Cenk Çolpan önderliğinde, çalışma arkadaşım, merkez denetim birimi uzmanı Ersel Tosun ile birlikte hayata geçirdiğimiz bir projedir.

Bu sistem ile, kontrolsüz olan hat ve cihaz satışları belli bir düzene oturtulmuş ve denetim mekanizması kazandırılmıştır. Bu sistem, alternatif satış kanallarında, ilk defa uygulamaya sokulmuş ve büyük bir başarı elde edilmiştir.

Bunun yanında, elektronik mağazalarında kendi denetim ve kontrol mekanizmasını geliştirmiştir. Böylelikle, her iki sistem birbirine entegre hale getirilmiş, sahtekarlık girişimlerinin önüne geçilmeye çalışılmıştır.

Bu bölümde, bu iki sistemin çalışma prensip ve kurguları görsellerle beraber anlatılacaktır.

Bunun yanında, sahtekarlık girişiminde bulunan ve bulunmayan yani gerçek müşterilerin verileri ortak bir veri ambarında toplanacak ve suçluluk profilleri analiz edilerek açıklanacaktır.

Hangi müşteri gruplarının suça yatkın olduğu ya da, hangi durumlarda sahtekarlık girişimlerinin başarıya ulaştığı, analiz edilerek bulunacak, bunların engellenmesine yönelik, sistemsal yenilikler açıklanacaktır.

5.1. SISNET

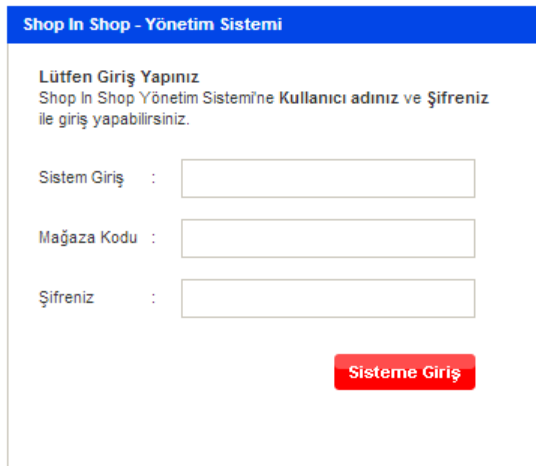
SISNET adını, İngilizcede Shop in Shop terimlerinden almaktadır. Artan sahtekarlık olayları sonrasında SISNET projesi hayata geçirilmiş ve başarı ile uygulamaya koyulmuştur.

Bu sistem temel olarak iki ana aşamadan oluşmaktadır. Bunlar, ürün ve hizmet verilen müşterilerin evraklarının taratılarak SISNET'e yüklenmesi, SISNET'e yüklenen müşteri evraklarının kontrol edilerek onaylanması aşamalarıdır. Kısaca bu sistemde, tüm işlemleri kontrol eden ve onaylayan bir merkez denetim birimi bulunmaktadır.

SISNET, evrak kontrolü için aracı site olmanın yanında, çalışanların satışlarının görüldüğü ve raporlandığı, güncel bilgilerin paylaşıldığı bir oryantasyon sitesidir. Ancak bu tez çalışmasında sahtekarlık girişimlerinin SISNET üzerinden nasıl engellendiği gösterilecektir.

5.1.1. SISNET'e Giriş

SISNET'e, <http://sis.brightstar.com.tr/> sitesi üzerinden girilmektedir. Giriş sırasında, kullanıcı adı, mağaza kodu ve kullanıcı şifresi istemektedir. Kullanıcı adları ve mağaza kodları sabit, kullanıcı şifreleri ise belli periyotlarla değiştirilmektedir.



Shop In Shop - Yönetim Sistemi

Lütfen Giriş Yapınız
Shop In Shop Yönetim Sistemi'ne Kullanıcı adınız ve Şifreniz ile giriş yapabilirsiniz.

Sistem Giriş :

Mağaza Kodu :


Şifreniz :

Sisteme Giriş

Şekil.5. SISNET Giriş Ekranı

Statik IP altyapısının oluşturulması ile beraber, sisteme giriş yapabilecek olan kullanıcılar eşleştirilecek, IP'leri eşleşmeyenlerin sisteme girişleri bloke edilecektir.

Yeni Kullanıcı Ekle

 **UYARI:** Sistem Giriş Kodu kullanıcıların sisteme giriş yapabilmeleri için gereklidir. Bu yüzden bu kodun oluşturulan kullanıcıya verilmesi gerekmektedir.

Sistem Giriş Kodu:

Mağaza:

İsim - Soyisim:

TC Kimlik Numarası:

Şifre:

Şifre (Tekrar):

Email:

Yetki Tipi:

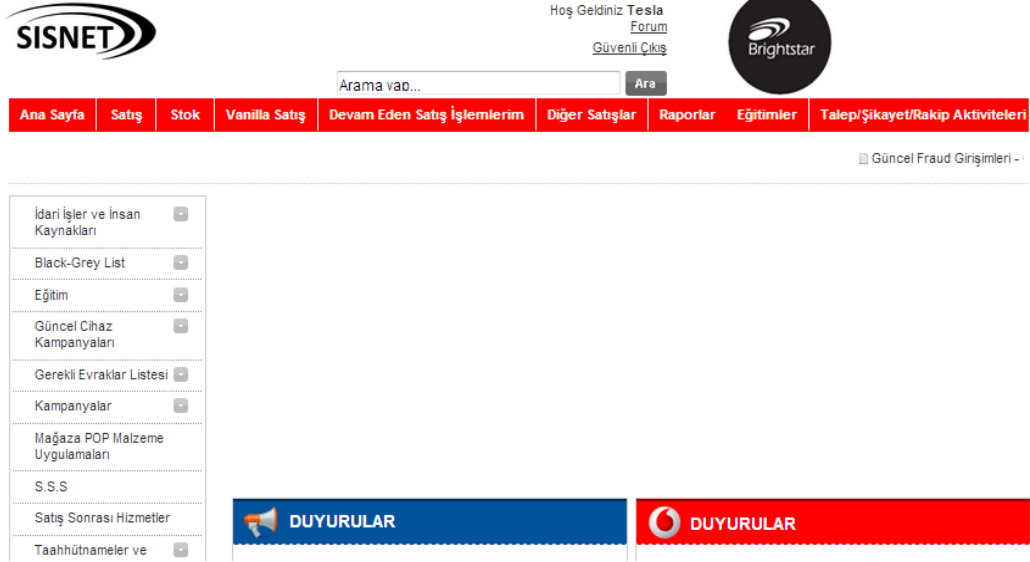
Kullanıcı Tipi:

Hesap Son Geçerlilik tarihi

Şekil.6. SISNET Kullanıcı Tanımlama Ekranı

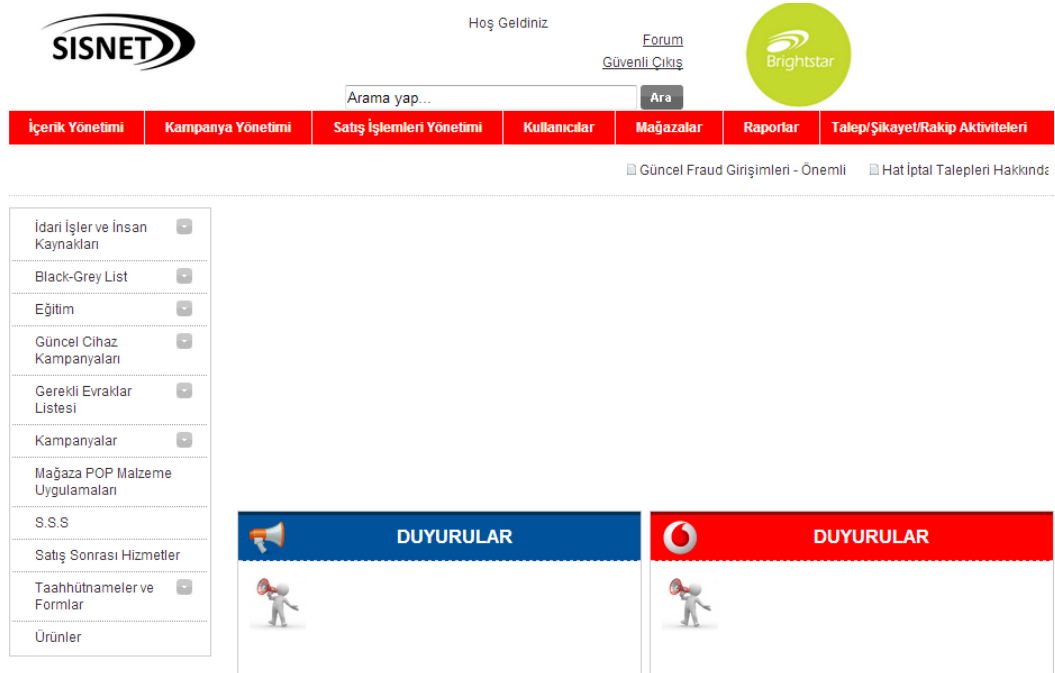
Şekil.5. 'da görüldüğü üzere sisteme giriş yapabilecek olan kullanıcılar ve yetkileri tanımlanmaktadır. Kullanıcıların yetki düzeylerine göre erişim alanları oluşturulmuştur. Hesap geçerlilik tarihi kısa tutularak, şifreler sürekli yenilenmektedir.

Şifre giriř ekranını başarılı bir şekilde geen kullanıcılar ařağıdaki ekran ile karřılařmaktadır.



řekil.7. SISNET Kullanıcı Ekranı

Kullanıcıların yanında, SISNET giriř ekranını başarılı bir şekilde geen sistem yöneticileri için ařağıdaki ekran açılmaktadır.



řekil.8. SISNET Yönetici Ekranı

5.1.2. SISNET Üzerinden Cihaz Satış Yapılması ve Onay Süreci

Kullanıcılar satış girecekleri zaman öncelikle Ürün Satışı alanına tıklayarak ilgili alana giriş gerçekleştirirler. Bu ekran üzerinde müşteriye ait bilgiler sorulmaktadır. Bu bilgilere göre, müşteriye imzalatılacak olan operatör sözleşmesi basılı olarak gelecektir. Operatör çalışanları, ekstradan sözleşme doldurmak için zaman kaybetmeyeceklerdir.

Ürün Satışı

Lütfen satmak üzere olduğunuz cihaza ait dökümanları yükleyiniz.

1. Müşteri Bilgileri

Ad:	<input type="text" value="DENEME"/>	İl	<input type="text" value="Adana"/>
Soyad:	<input type="text" value="DENEME"/>	İlçe	<input type="text" value="Seyhan"/>
TC Kimlik No:	<input type="text" value="22133242423"/>	Semt	<input type="text" value="Hükümet"/>
Kimlik Tipi:	<input type="text" value="Nüfus Cüzdanı"/>	Mahalle - Köy	<input type="text" value="Karacaoğlan Mah."/>
Kimlik Seri No:	<input type="text" value="D11 11111"/>	Cadde / Sokak	<input type="text" value="DENEME"/>
Kimlik Verilme Tarihi:	<input type="text" value="01.01.2013"/>	Bina Adı / Bina No / Daire No	<input type="text" value="DENEME"/>
Cinsiyet:	<input checked="" type="radio"/> Erkek <input type="radio"/> Kadın		
Anne Kızlık Soyadı:	<input type="text" value="DENEME"/>		
İrtibat Numarası:	<input type="text" value="(111) 111 11 11"/>		
Doğum Tarihi:	<input type="text" value="05.05.1966"/>		
Doğum Yeri:	<input type="text" value="DENEME"/>		
Baba Adı:	<input type="text" value="DENEME"/>		
Anne Adı:	<input type="text" value="DENEME"/>		

2. GSM No

GSM:	<input type="text" value="(111) 111-1111"/>
Tekrar Giriniz:	<input type="text" value="(111) 111-1111"/>

3. Abonelik Türü

<input type="text" value="Lütfen seçiniz..."/>
--

Şekil.9. SISNET Satış Ekranı

Müşteri bilgileri girildikten sonra abonelik türü seçilmektedir. Seçilen abonelik türüne göre işleyiş değişmektedir. Bu bölümde cihaz satış süreci işleneceği için bu alanda, temlik seçilerek devam edilmektedir.

İlgili alanlar doldurulduktan sonra ekran aşağıdaki gibi değişmektedir. Bu alanda işlem türüne göre operatör çalışanından müşteriye ait belgeler istenmektedir. Operatör çalışanı müşteriden aldığı ve tarattırdığı belgeleri ilgili alanlara yükler ve satışı kaydet butonuna basar.

3. Abonelik Türü

Yeni Hat / Temlik ▼

4. Faturalı / Faturasız

Faturalı ▼

5. Lütfen dosyaları yükleyiniz.

Abonelik Sözleşmesi

Dosya Seç Dosya seçilmedi



Adres Gösterir Belge

Dosya Seç Dosya seçilmedi

Kimlik Fotokopisi

Dosya Seç Dosya seçilmedi

Temlik Sözleşmesi - Ürün seçimi ekranında yüklenecek

Dosya Seç Dosya seçilmedi

Kredi Kartı Slip

Dosya Seç Dosya seçilmedi

Sair İşlem Evrakları

Dosya Seç Dosya seçilmedi

Yükle ve Satışı Kaydet

Şekil.10. SISNET Evrak Ekranı

Satış kaydedildikten sonra ilgili ekran aşağıdaki gibi otomatik değişmektedir. Bu ekranda operatör çalışanı, müşteriye vereceği cihaz ile ilgili bilgileri girer. Satılan cihaz, ilgili ürün modelleri içerisinde bulunur, cihazın IMEI bilgisi girilir ve en son aşamada müşteriye imzalatacağı taahhünameyi seçer. Taahhüname içerisindeki müşteri adı, tarih ve adres bilgisini sistem, ilk aşamada girilen müşteri bilgilerinden seçer ve otomatik olarak yazdırır. Böylelikle tekrardan taahhüname doldurulması ile geçecek olan zaman kaybı kapatılır. Operatör çalışanı sözleşmenin çıktısını alarak

müşteriye imzalatır. Müşteriye imzalatılan sözleşme ve alınan evraklardan sonra, cihaz kampanyası girişi, operatör sistemlerine girilir ve imzalanmış taahhütname ilgili ekran üzerinden SISNET' e yüklenilir. Operatör sistemleri ile SISNET' in farklı ekranlar olduğu unutulmamalıdır.

Ürün Satışı

DENEME DENEME - (111) 111-1112

Lütfen satışını gerçekleştirmek istediğiniz ürünü seçiniz.

Ürün Modelleri:	HTC Explorer
<input type="text"/>	İsim: : HTC Explorer
HTC Desire X (White)	Kod: : 99HNZ090-00
HTC Desire Z	Marka: : HTC
HTC Endeavor One X (White)	Model: : Explorer
HTC Evo 3D	IMEI: : 1111111111111111
HTC Explorer	Kampanya: : Kampanyasız Satış
HTC Flyer 3G+WIFI (32G)	Temlik Sözleşmesi
HTC Golf Desire C (Black)	Seçiniz...
HTC Golf Desire C (Red)	<input type="button" value="Satış İşlemini Tamamla"/>

Şekil.11. SISNET Cihaz Bilgi Giriş Ekranı

Satış İşlemini Tamamla butonuna basıldıktan sonra ilgili satış, merkez denetim birimi ekranına düşer ve bilgilendirme ekranı kullanıcının karşısına gelir. Müşterinin ismi, işlemin hangi mağazadan yapıldığı, cihaz bilgisi ve işlem tarihi bunlardandır. Bunların yanında, kullanıcıya işlemin Brs Onayında olduğu bilgiside verilmektedir. Brs Onayında ifadesi, işlemin kaydedildiği ve merkez denetim birimin ekranlarına düştüğü ve kontrol edildiği anlamına gelmektedir.

Tüm Satış İşlemleri	Tüm Satışlar
Bu kategorideki 30 satış işlemi listelenmektedir.	Tarih: <input type="text"/>
DENEME DENEME	MAGAZA2 / NICEYE
(111) 111-1112	Yeni Hat /
IMEI:	Temlik » Faturalı
22222222344444	15 Ocak 2013
	10:32
	Brs Onayında

Şekil.12. SISNET Cihaz Satışı Bilgilendirme Ekranı

Merkez denetim birimine düşen satış aşağıdaki gibi gözükmektedir. Bu aşama, satışın en önemli bölümüdür. Merkez denetim birimi çalışanı SISNET' e yüklenen belge ve bilgiler için sahtekarlık kontrolü yapar. Bununla beraber, kampanya girişinin operatör sistemlerine girilip girilmediğini kontrol eder.

DENEME DENEME MAGAZA2 / NICEYE (111) 111-1112 Yeni Hat / 15 Ocak 2013 Brs Onayında
IMEI: Temlik » Faturalı 10:32
22222222344444

Satış ID: #19544

Abonelik Sözleşmesi
Bu dosya 15 Ocak 2013 10:32 tarihinde yüklenmiş.

Adres Gosterir Belge
Bu dosya 15 Ocak 2013 10:32 tarihinde yüklenmiş.

Kimlik Fotokopisi
Bu dosya 15 Ocak 2013 10:32 tarihinde yüklenmiş.

Kredi Kartı Slip
Bu dosya 15 Ocak 2013 10:32 tarihinde yüklenmiş.

Sair İşlem Evrakları
Bu dosya 15 Ocak 2013 10:32 tarihinde yüklenmiş.

Temlik Sözleşmesi
Bu dosya 15 Ocak 2013 11:12 tarihinde yüklenmiş.

Bir İşlem Seçiniz:
Lütfen bir işlem seçiniz...
Lütfen bir işlem seçiniz...
Hatalı Evrak
Reddet
Onayla
Hatalı İşlem Turu

Şekil.13. SISNET Cihaz Satışı Merkez Denetim Ekranı

Herhangi bir problem olduğunda kullanıcıya aşağıdaki gibi geri dönüş yapılır.

Bir İşlem Seçiniz:
Hatalı Evrak

Kredi Kartı Slip
Tutarı Hatalıdır.
Lütfen Düzeltiniz.

Kaydet

Satışı Sil

Şekil.14. SISNET Cihaz Satışı Hata Ekranı

Kullanıcıya yapılan bu geri dönüş, kullanıcı ekranında aşağıdaki gibi görülmektedir.

The screenshot shows the 'Devam Eden Satış İşlemlerim' (My Ongoing Sales Transactions) page. The page title is 'Devam Eden Satış İşlemlerim' and it indicates that 30 sales transactions are displayed in this category. The table below shows the details of a sales transaction:

Müşteri	GSM	Satış Tipi	Tarih	Durum
DENEME DENEME	(111) 111-1112	Yeni Hat / Temlik » Faturalı	15 Ocak 2013 10:32	Hatalı Evrak

Satış ID: #19544

Yüklemiş olduğunuz dosyalarda hatalı evrak bulunmaktadır. Aşağıda gerekli açıklamayı bulabilirsiniz.

Kredi Kartı Slip Tutarı Hatalıdır. Lütfen Düzeltiniz.

15 Ocak 2013 11:18

Şekil.15. SISNET Cihaz Satışı Hata Kullanıcı Ekranı

Satış ile ilgili bir problem olmaması durumunda satışa onay verilir.

The screenshot shows a form titled 'Bir İşlem Seçiniz:' (Select an Operation). The form has a dropdown menu with 'Onayla' (Approve) selected. Below the dropdown are two buttons: 'Kaydet' (Save) and 'Satışı Sil' (Delete Sale).

Şekil.16. SISNET Cihaz Onay Ekranı

Satışa onay verilmesinin akabinde, kullanıcı ekranı aşağıdaki gibi görülmektedir. Brs Onayında görülen satış, onayın akabinde Mağaza Onayında statüsüne dönmüştür.

The screenshot shows the 'Devam Eden Satış İşlemlerim' (My Ongoing Sales Transactions) page. The page title is 'Devam Eden Satış İşlemlerim' and it indicates that 30 sales transactions are displayed in this category. The table below shows the details of a sales transaction:

Müşteri	GSM	Satış Tipi	Tarih	Durum
DENEME DENEME	(111) 111-1112	Mevcut Abone / Temlik » Faturalı	15 Ocak 2013 10:32	Mağaza Onayında

Satış ID: #19544

Kimlik Fotokopisi
Bu dosyayı 15 Ocak 2013 10:32 tarihinde yüklemiştir.

Kredi Kartı Slip
Bu dosyayı 15 Ocak 2013 10:32 tarihinde yüklemiştir.

Temlik Sözleşmesi
Bu dosyayı 15 Ocak 2013 11:25 tarihinde yüklemiştir.

Müşteri Onay ve Bilgi Formu
Gözet
Yükle

Cihaz Faturası
Gözet
Yükle

Şekil.17. SISNET Cihaz Mağaza Onay Ekranı

Bu aşamada, operatör çalışanı onayı almış ve cihazı müşteriye teslim etmiştir. Elektronik mağaza içerisindeki kasadan faturalandırma işlemi yapılır ve müşterinin belirtilen cihazı aldığını gösterir belge olan müşteri onay bilgi formu imzalatılır. Fatura ve müşteri onay bilgi formu da SISNET' e yüklenir ve satış tamamlanır.

Müşteri	Mağaza Adı	GSM	Satış Tipi	Tarih	Durum
DENEME DENEME	MAGAZA2 / NICEYE	(111) 111-1112 IMEI: 22222222344444	Mevcut Abone / Temlik » Faturalı	15 Ocak 2013 10:32	Tamamlandı

Şekil.18. SISNET Cihaz Satışı Tamamlandı Ekranı

5.1.3. SISNET Üzerinden Hat ve Diğer Ürünlerin Satışı

Kontratlı cihaz satışında olduğu gibi müşteri bilgileri girilerek satışı yapılacak ürün seçilir. Seçilen ürün türüne göre, operatör çalışanından gerekli evraklar istenmektedir. Operatör ekranlarına giriş yapıp evraklar SISNET' e yüklenilir ve merkez denetim biriminden onay beklenilir. BRS onayında görülen satış, merkez denetim biriminden gelen onaydan sonra tamamlandı olarak gözüktür ve fatura kesimi sağlanır.

5.1.4. SISNET Üzerinden Onaylanan İşlemlerin Kontrolü

Merkez denetim biriminin verdiği tüm onaylar kayıt altına alınmaktadır. Böylelikle hangi işleme kimin onay verdiği, işlem üzerinde ne gibi bir değişiklik yaptığı bilgisi görülmektedir.

15054	Hakan KILIÇARSLAN	Brs Onayında	Mağaza Onayında	2012-11-07 13:13:40
15591	Hakan KILIÇARSLAN	Brs Onayında	Mağaza Onayında	2012-11-07 13:13:02

Şekil.19. SISNET Satış Onayları

5.2. SISNET' in Sağladığı Yararlar

SISNET üzerinden onay alınması, tüm cihaz ve diğer ürünlerin satışı için zorunlu kılınmıştır. Bu sayede hat ve cihaz satışları belli bir kontrole girmiştir. SISNET ile personellerin özellikle kampanya girişi ve gerekli operatör sistemlerine tanımlama yapılıp yapılmadığı kontrol edilerek onay verilmektedir. Bu sayede hatalı kampanya girişleri, operatör sistemlerine tanımlama yapılmadan cihaz satılması ve sahte evraklarla işlem yaptıracak müşterilerin önemli ölçüde önüne geçilmiştir.

SISNET, önceleri oryantasyon sitesi olarak tasarlanmıştır. Operatörden gelen son dakika duyuruları, güncel kampanyalar veya değişiklikler bunun yanında farklı türden raporlar barındırmaktaydı.

Gelişen ve çeşitlenen sahtekarlık olaylarından sonra böyle bir değişime gidilmiş, SISNET üzerinden onay alınma süreci zorunlu kılınmıştır. Ancak operatöre ait çalışanlarında sahtekarlık yapma riskinin olması ve elektronik mağazalarında kendilerini güvenceye almak istemesi neticesinde, mağaza kontrol sistemi oluşturulmuştur. Böylelikle, satışın iki kolu olan, operatör tarafı ve mağaza tarafı kendi güvenliklerini sağlamanın yanında, ortaklaşa bir güvenlik sistemi kurmaktadır.

5.3. Mağaza Kontrol Sistemi

Mağaza kontrol sistemi temel olarak, bir ucu SISNET' e , diğer ucu mağaza faturalandırma sistemine bağlı programdır. Bir cihaz ya da herhangi bir satışın, SISNET' e yüklenmeden ve onay verilmeden satılmasının önüne geçmektedir. Böylelikle hem elektronik mağaza, hemde operatör satılan cihazın güvenliğini eşzamanlı sağlamaktadır.

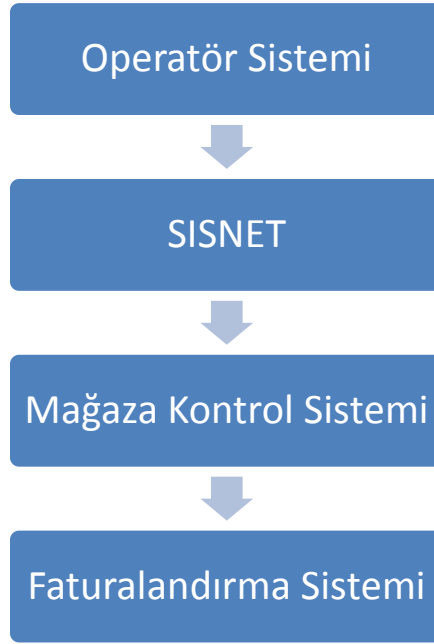
Mağaza kontrol sistemi birkaç adımdan oluşmaktadır. Öncelikle satılmak istenen cihaz ve müşteri bilgileri mağaza kontrol sisteminden giriş yapılır. Girişi yapılan bilgiler SISNET' e düşer, operatör çalışanı, cihaz bilgilerini operatör sistemine girer ve evraklarını tarayarak SISNET' e yükler. Merkez denetim birimi satışı kontrol eder. Onay verilmesinin ardından, hem SISNET üzerinden hem de mağaza kontrol sistemi üzerinden satışın onaylandığı görülür. Mağaza kontrol sistemine onaylanan satış olarak düşen işlem, mağaza faturalandırma sistemine aktarılır ve faturası kesilir. Böylelikle hiçbir şekilde SISNET' e yüklenmeden cihaz satışı yapılmamakta ve kontrolü anlık olarak sağlanmaktadır.

5.3.1. Mağaza Kontrol Sisteminin Faydaları

Operatörlerin, elektronik mağazalara gönderdikleri kontratlı ve kontratsız cihazların ayrıştırılması ve kayıt altına alınmasında yardımcı olmaktadır. Müşteriler, elektronik mağaza içerisinde, sistemin ara yüzü ve bir bilgisayar ile kontrat-fiyatlandırma bilgisine ulaşabilmektedir. Bunun yanında operatörler ile mutabık kalınması yönünden son derece önemlidir.

5.3.2. Mağaza Kontrol Sistemi İle Satış Yapılması

Mağaza kontrol sistemi, aşağıdaki şekilde de görüldüğü üzere SISNET ile bağlantılıdır. Operatör sistemlerine girişi yapılan ve müşteri evrakları SISNET' e yüklenen satış, onay verilmesinin akabinde, mağaza kontrol sistemine düşmekte ve faturalandırılması için işlem yapılabilmektedir.



Şekil.20. Satış İşleyiş Görünümü

Elektronik mağazaya gelen kişiler öncelikle bu sistemde tanımlı cihaz kampanyalarından birini seçer ve kimlik bilgilerini girerler.



Şekil.21. Mağaza Kontrol Sisteminden Ürün Seçimi

Müşteri cihazı seçtikten sonra bilgilerini girer.

İSİM	<input type="text"/>
SOYİSİM	<input type="text"/>
TELEFON NO	<input type="text"/>
ADRES	<input type="text"/>
İL	<input type="text"/>
İLÇE	<input type="text"/>
ÜLKE	<input type="text"/>
CİHAZ İMEİ	<input type="text"/>

Şekil.22. Mağaza Kontrol Sisteminden Müşteri Bilgi Girişi

Seçilen cihaz ve girilen müşteri bilgileri onaylandıktan sonra satış, tüm verilerle beraber, SISNET' e aktarılır. Bu aşamada, operatör çalışanı müşterinin belirttiği cihaz kampanyasını operatör sistemine tanımlar ve onay almak üzere, müşterinin

belgelerini taratarak, merkez denetim birimine gönderir. Merkez denetim birimi satışı onaylar ve satış, hem SISNET üzerinden hem de mağaza kontrol sistemi üzerinden onaylandı olarak gözükür. Bu aşamada mağaza kontrol sistemi, fatura kesilmesi için gereken izni verir ve satışın faturası kesilir. Merkez denetim biriminin geri bildirimine göre, satış düzeltilebilir veya iptal edilebilir. Tüm bu geri dönüşler mağaza kontrol sisteminde görülmekte ve işlemin faturalaştırılması için onaylandı statüsüne ihtiyaç duyulmaktadır.



5.3.3 Mağaza Kontrol Sisteminin Değerlendirilmesi

Mağaza kontrol sistemi ile, elektronik perakende firmaları, rahatlıkla operatöre ait ürün ve hizmetleri güvenli olarak satabilmektedir. SISNET onaysız hiçbir satışın yapılmaması ve SISNET' in merkez denetim birimi tarafından kontrol ediliyor olması, cihaz ve diğer ürün mutabakatlarında kolaylık getirmiştir.

Bunun yanında operatörlere ait ürünlerin bu sisteme kaydedilmesi ve ayrıştırılması, ürün sayımlarında ve kontrollerinde de büyük kolaylık sağlamaktadır.

5.4. Veri Madenciliği Yöntemleri İle Sahtekârlık Analizi

Bu bölümde veri madenciliği yöntemleri ile dolandırıcılık analizi yapılacaktır.

5.4.1. Veri Madenciliği

Veri madenciliği, bilinmeyen, saklı, anlamlı ve yararlı bilgilerin veri ambarlarından otomatik ve sistematik bir biçimde elde edilmesini sağlayan veri tabanlarındaki keşif ve analiz sürecidir.

Veri madenciliği günümüzde birçok alanda kullanılmaktadır. Bunlar, pazarlama, bankacılık, finans, biyoloji, kimya, tıp, meteoroloji ve atmosfer bilimleri, sosyal bilimlerdir.

Veri madenciliğinin kökeni ENIAC (Electrical Numerical Integrator And Calculator)'a kadar dayanmaktadır. 1946 yılında geliştirilen ve bugün kullandığımız kişisel bilgisayarların atası olan ENIAC, ABD'li bilimadamları John Mauchly ve J. Presper Eckert tarafından, II. Dünya Savaşı sırasında ABD ordusu için geliştirilmiştir. [39]

30 tonluk ağırlığıyla 170 m²lik bir alanı kaplayan bu “ilk” bilgisayarın 60 sene içerisinde geçirmiş olduğu evrimin nihai boyutlarını şu anda masa üstünüzdeki bilgisayara bakarak anlamanız mümkündür. [40]

Donanım merkezli hazırlanan eski bilgisayarların, yazılım ile bütünleştiği günümüzde, bilgisayarların nasıl bir evrim sürecinden geçtiği, günümüz bilgisayarlarına bakıldığında rahatlıkla anlaşılmaktadır.

Zaman içerisinde verilerin kaydedilmek istenmesiyle depolama birimleri, oluşma ve gelişme evresine girmiştir. Veri ambarı kavramının ortaya çıkışı bu dönemlere rastlamaktadır.

Kaybedilmek istemeyen veriler, bir ambar misali fiziksel sürücülerde tekrar kullanılmak üzere saklanmaktaydı. Gittikçe büyüyen veri tabanlarının organizasyonu, düzenlenmesi ve yönetimi de buna paralel olarak güç bir hal almaya başladı. Bu safhada veri modelleme kavramı ortaya çıktı.

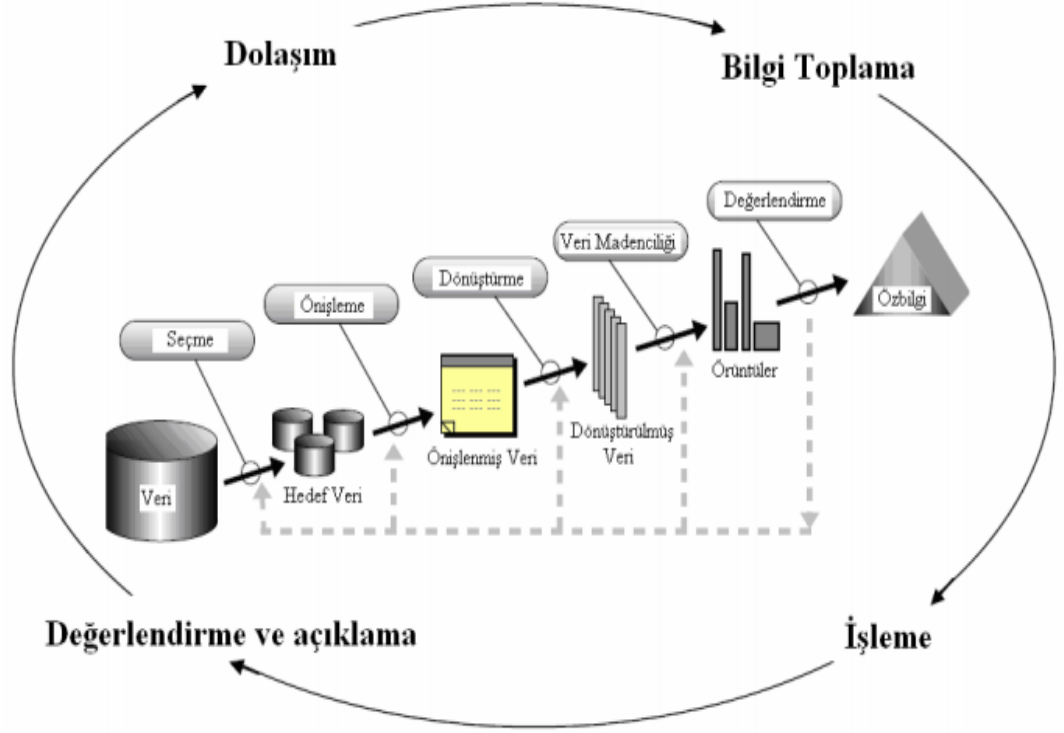
İlk olarak basit veri modelleri olan Hiyerarşik ve Şebeke veri modelleri geliştirildi. Hiyerarşik veri modelleri, ağaç yapısına sahip, temelinde bir kök olan ve bu kök vasıtasıyla üstünde her daim bir, altında ise n sayıda düğüm bulunan veri modelleriydi.

Şebeke veri modelleri ise kayıt tipi ve bağlantıların olduğu, kayıt tiplerinin varlık, bağlantılarınsa ilişki tiplerini belirlediği bir veri modeliydi. Şebeke veri modelinde herhangi bir eleman bir diğeri ile ilişki içerisine girebiliyordu.

Veri madenciliği kullanılarak bir sistem oluşturulmak isteniyorsa, bu sistemin taşınması gereken bir takım özellikler bulunmaktadır. Tasarlanan sistem kararlı ve standartlara uygun, gerçek dünya ile paralellik gösterebilen, kullanıcı dostu, kullanıcının işlemlerini rahatla yapabildiği, istediği an işlemleri geri alabildiği özellikleri taşımalıdır.

Bu özelliklerin yanı sıra, tasarlanan sistem kullanıcının hafıza yükünü minimize edebilmeli, hata önleme mekanizmasına sahip olmalı, hata mesajları anlaşılır olmalı ve kullanıcıya çözüm yolu sunabilmelidir. Ayrıca kullanıcı, tasarlanan sistemin yardım ve dokümantasyon özelliğine olabildiğince az ihtiyaç duymalıdır.

Veri tabanlarında öz bilgi keşfine ihtiyaç duyan kullanıcılar, geliştirilen veri madenciliği sistemlerinin dört tür etkileşim özelliğine sahip olmasını istemektedir. Bunlar dolaşım, bilgi toplama, işleme, değerlendirme ve açıklamadır. Veri tabanlarında öz bilgi keşif sürecine bu dört etkileşim özelliğinin adapte edilmesi ile kullanıcı merkezli interaktif veri madenciliği döngüsü elde edilmektedir. Şekil 1'de bu döngü yer almaktadır.



Şekil.23. Kullanıcı merkezli interaktif veri madenciliği döngüsü fuzzy sistemler, Bayesian ağları, genetik algoritmalar.

Kaynak: Karacan, H. Yeşilbudak, M., *Kullanıcı Merkezli İnteraktif Veri Madenciliği: Bir Literatür Taraması*, Bilişim Teknolojileri Dergisi, 2010.

5.4.2. Problemin Tanımı

Dünyada özellikle ülkemizde, GSM suçları gün geçtikçe artmaktadır. Özellikle kontratlı cihaz alan müşterilerin aslında belirttikleri müşteri olmadıkları, bilgilerinin çalındıkları veya belirtilen kişi olmasına rağmen hiçbir endişe duymadan onlarca kişiyi dolandırdıkları tespit edilmiştir.

Her yıl bu sebepten ötürü, binlerce dava açılmakta birçok müşteri mağdur olmaktadır. Bunun yanında, operatörlere verilen dolandırıcılık cezaları ve yargılama sonrasındaki yaptırımlar operatörlerin haksız yere cezalar almasına ve sektörün gerilemesine yol açmaktadır.

5.4.3. Amaç

Bu tez çalışmasında elektronik mağazalarda işlem yapmış müşteriler analiz edilerek dolandırıcılıkları tespit edebilecek bir sistem geliştirilmiştir.

Bu bağlamda, daha önce operatörlere ait elektronik mağazalardaki noktalarda yaptıkları işlemler bilinen ve bu işlemler neticesinde dolandırıcı olup olmadıkları anlaşılan müşteriler arasındaki bağlantılar incelenmiştir. Dolandırıcı müşterilerin hangi özelliklerinin gerçek müşterilerden ayırdıklarına bakılmıştır. Bu bağlamda veri madenciliği yöntemleri kullanılmıştır.

5.4.4. Verilerin Özellikleri

Tez kapsamında, bir operatörden alınan veriler analiz edilmeye ve dolandırıcılık analizi yapılmaya çalışılacaktır.Öncelikle elde edilen veriler ve özellikleri bu bölümde açıklanacaktır.

5.4.4.1. Abone Cinsiyeti

Abonelerin cinsiyeti ‘‘Erkek’’ ve ‘‘Kadın’’ olarak belirtilmiştir.

5.4.4.2. Abone Yaşı

Satış noktalarında işlem yaptırabilen 18 yaş üzeri abonelerin kaydı alınmıştır.

5.4.4.3. Abone İkamet Yeri

Abonelerin mevcut ikamet ettikleri lokasyonlar baz alınmıştır

5.4.4.4. Abone Kimlik İl

Abonelerin nüfusa kayıtlı oldukları iller dikkate alınmıştır

5.4.4.5. İşlem Yapılan Mağaza İli

Abonelerin kontratlı cihaz aldıkları mağazaların buldukları illerdir.

5.4.4.6. İşlem Yapılan Mağaza

Abonelerin işlem yaptırdıkları mağazalardır. Bu mağazalar harfler ile gösterilecektir.

5.4.4.7. İşlemin Yapıldığı Gün

Abonelerin işlem yaptırdıkları günler dikkate alınmıştır.

5.4.4.8. Personel Cinsiyeti

Noktalarda çalışan, operatöre ait çalışanın cinsiyetini ifade etmektedir.

5.4.4.9. Personel Tecrübesi

Operatöre ait noktalarda çalışan personellerin sektör tecrübeleri baz alınmıştır.

5.4.4.10. Hattın Türü

Abonelerin kullanmış oldukları mevcuttaki hatları veya satış noktalarında cihazla beraber aldıkları faturalı hatlar, ‘‘ Yeni Hat Faturalı’’ olarak, başka bir operatörden gelmiş ise, ‘‘Numara Taşıma’’ olarak belirtilmiştir

5.4.4.11. Hattın Özeliği

Ses yani konuşma hattı ile, veri yani data hattı olarak belirtilmiştir.

5.4.4.12. Hattın Kategorisi

Hattın kategorisi ‘‘Düşük’’, ‘‘Orta’’ ve ‘‘Yüksek’’ olarak belirtilmiştir. Buradaki kategoriler fiyatlandırma açısından 3’ e ayrılmıştır.

5.4.4.13. Mernis Doğrulama

Abonelerin kimliklerinde yer alan bilgiler ile, mernis kimlik doğrulama sisteminden çekilen bilgilerin örtüşüp örtüşmediğini belirtmektedir. Bilindiği gibi operatörlerin nüfus kayıt sistemine erişim yetkileri bulunmaktadır. Buradaki veriler ‘‘Var’’ veya ‘‘ Yok’’ olarak belirtilmiştir.

5.4.4.14. Kapama-Kısıtlama Durumu

Abonelerin borçlarını zamanında ödemedikleri durumda hatlarının kısıtlamaya, ileriki aşamalarda da kapamaya girdikleri durumdur. Buradaki verilerde ‘‘ Evet’’ ve ‘‘ Hayır’’ olarak belirtilmektedir.

5.4.4.15. Daha Önce Aldığı Cihaz Sayısı

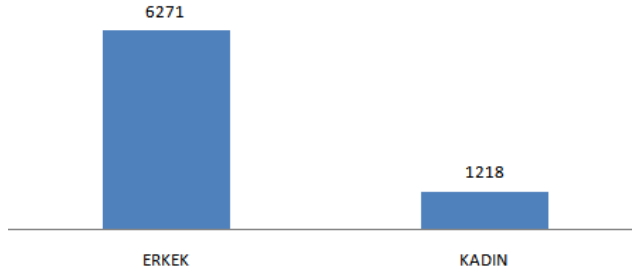
Abonelerin, cihaz almak istedikleri hatlarının haricinde daha önceden kontratlı olarak aldıkları hatların sayısını belirtmektedir.

5.4.4.16. Kampanya Giriş Durumu

Abonelerin cihaz kampanyalarından ‘‘Kredi Kartlı’’ yada ‘‘Kredi Kartsız’’ yararlanacağını gösteren alandır.

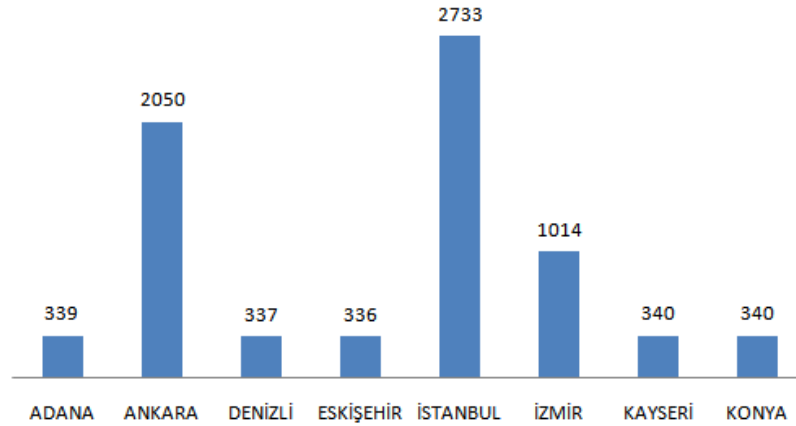
5.4.5. Verilerin Analizi

Kullanılan verilerde 6271 adet erkek, 1218 tane kadın müşteri bulunmaktadır.



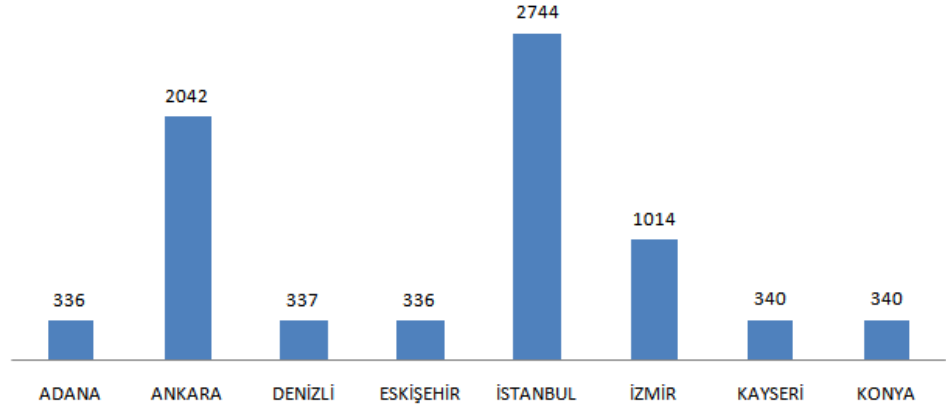
Şekil.24. Cinsiyet Dağılımları

Kişilerin ikamet ettikleri yerler ve adetleri aşağıdaki gibidir.



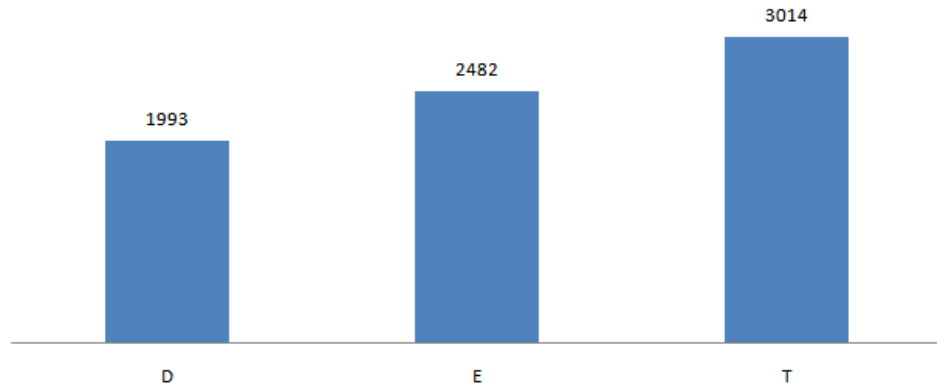
Şekil.25. İkamet Dağılımları

Kişilerin işlem yaptırdıkları iller aşağıdaki gibidir.



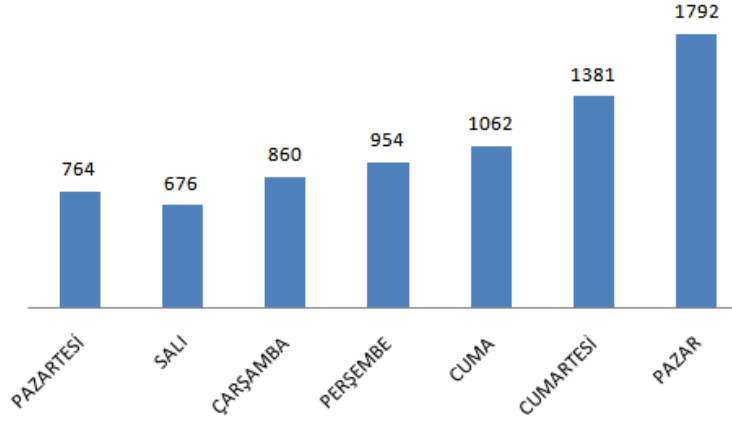
Şekil.26. İşlem yapılan İl Dağılımları

Kişilerin işlem yaptırdıkları mağazalar aşağıdaki gibidir.



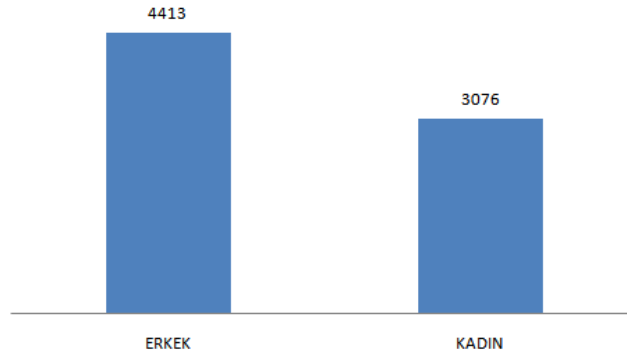
Şekil.27. Mağaza Dağılımları

Abonelerin işlem yaptıkları günler aşağıdaki gibidir.



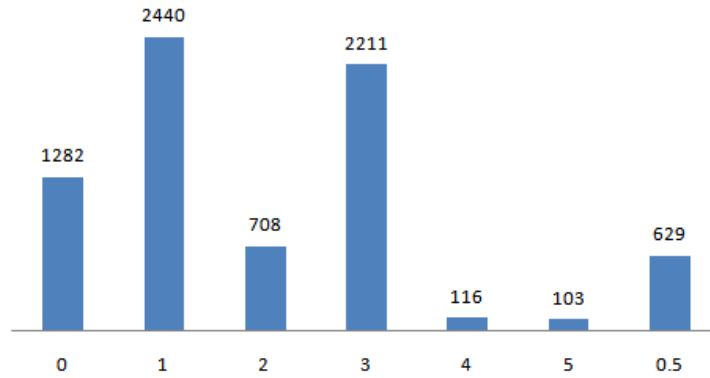
Şekil.28. Gün Dağılımları

İşlemleri alan personellerin cinsiyetleri aşağıdaki gibidir.



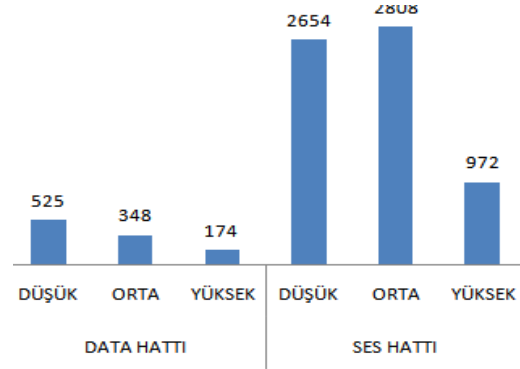
Şekil.29. Personel Cinsiyet Dağılımları

İşlemleri alan personellerin iş tecrübeleri aşağıdaki gibidir.



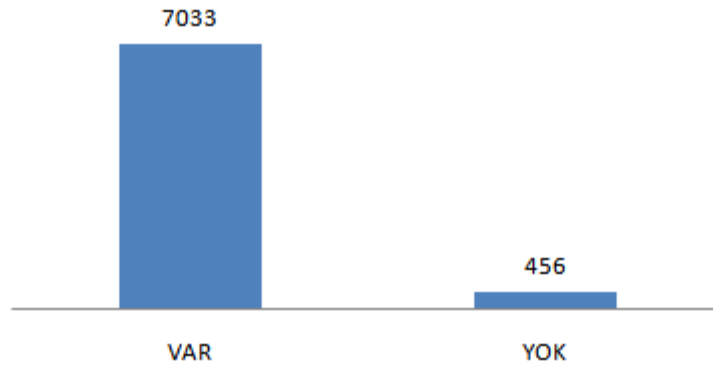
Şekil.30. Personel Tecrübe Dağılımları

İşlem yapılan hatların ve hatların fiyatlarına göre dağılımları aşağıdadır.



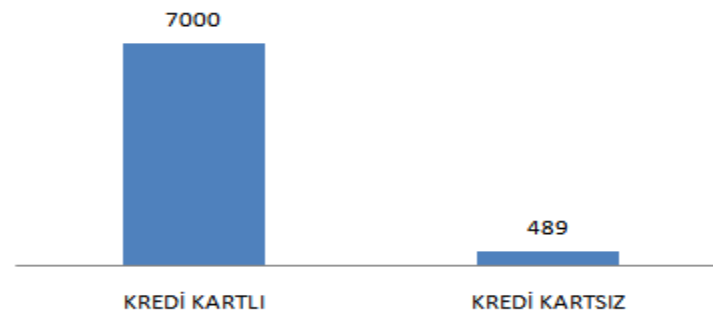
Şekil.31. Hat ve Fiyat Dağılımları

Mernis yani kimlik doğrulama yapılan veya yapılmayan abonelerin sayıları aşağıdaki gibidir.



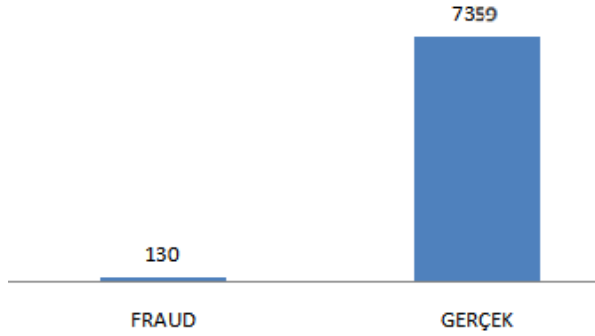
Şekil.32. Mernis Doğrulama Dağılımı

Kredi kartlı ve kredi kartsız olarak cihaz kampanyasından yararlanan abone sayıları aşağıdaki gibidir.



Şekil.33. Kredi Kartı Kullanım Dağılımı

Son olarak gerçek ve dolandırıcı abone sayıları aşağıdaki gibidir.



Şekil.34. Dolandırıcı/Gerçek Abone Dağılımı

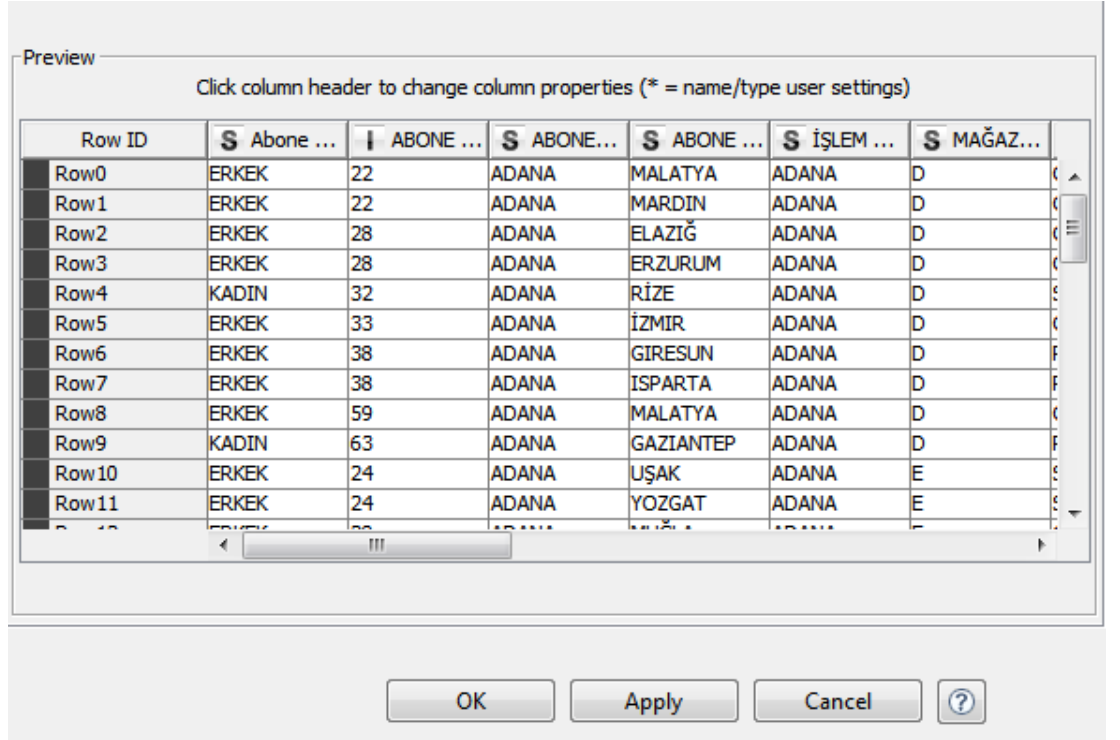
5.4.6. Karar Ağacı Oluşturulması

Karar ağaçları sınıflandırma problemlerinde en çok kullanılan algoritmalarından biridir. Diğer yöntemlerle kıyaslandığında karar ağaçlarının yapılandırılması ve anlaşılması kolaydır denilebilir. Bu teknikte sınıflandırma için bir ağaç oluşturulur.; daha sonra, veritabanındaki her bir kayıt bu ağaca uygulanır ve çıkan sonuca göre bu kayıt sınıflandırılır. Temel olarak iki adımdan oluştuğu söylenebilir; Birincisi ağacın kurulması, ikincisi de verilerin teker teker ağaca uygulanarak sınıflandırmanın gerçekleşmesi şeklindedir. [40]

Tez çalışmasında KNIME programından yararlanılmıştır.

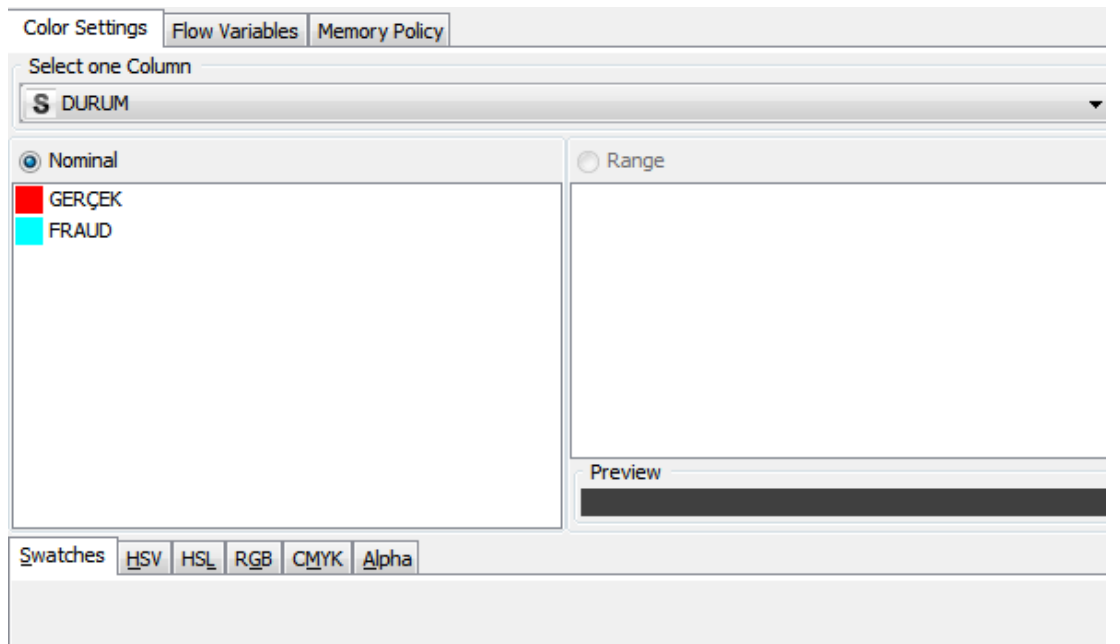
Öncelikle Excel türündeki veriler, CVS (Virgülle Ayrılmış) olarak değiştirilmiştir. Bu veriler KNIME üzerinde yer alan, IO, Read, File Reader ile açılmıştır.

Veriler sunucudan çekildiği sırada yaklaşık 10-15 hücre kayıptı. Veri kaybına yol açan bu alanlar, kendisine en yakın özellikteki satırlar baz alınarak, bir üstteki ve bir alta ki alanların ortalaması alınarak giderilmiştir.



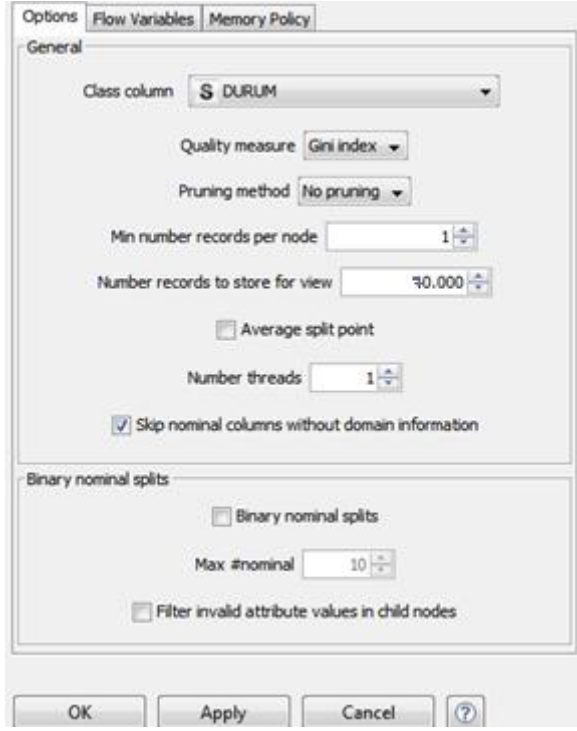
Şekil.35. Verilerin Ön İzlemesi

Verilerin okutulmasının ardından, verilerin düzenlenmesi ve ayrıştırılması aşamalarına geçilmiştir. Data Views, Property, Color Manager sekmesi açılarak amacımızın sahte ve gerçek müşterilerin ayrıştırılması olduğu ve bunun için hangi kolonu baz alacağı belirtilmiştir.



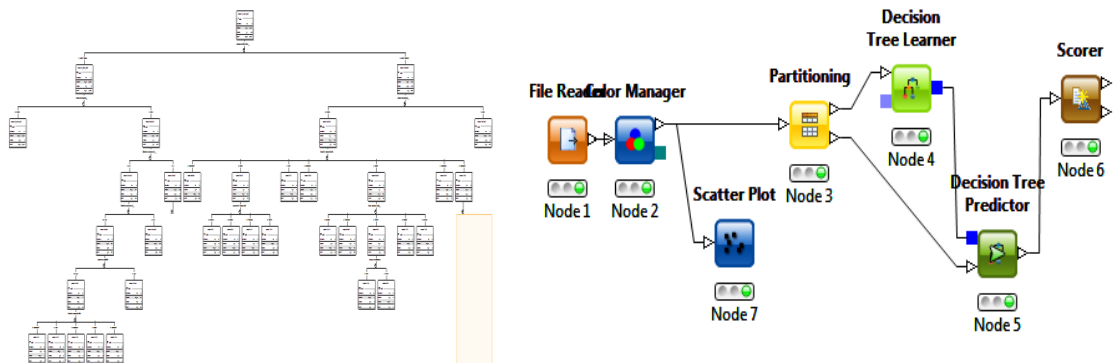
Şekil.36. Color Manager Görünümü

Veriler düzenlendikten sonra Mining, Decision Tree, Decision Tree Learner seçeneğine girilmiştir. Analizdeki amacımız, sahte ve gerçek müşteri ayırımı olduğu için Class column olarak ‘Durum’ seçilmiştir. Min number records per node olarak 1, for view için analizde kullanacağımız durum kadar sayı seçilmiştir. Analiz sırasında 10.000’ e yakın veri kullanılmıştır.



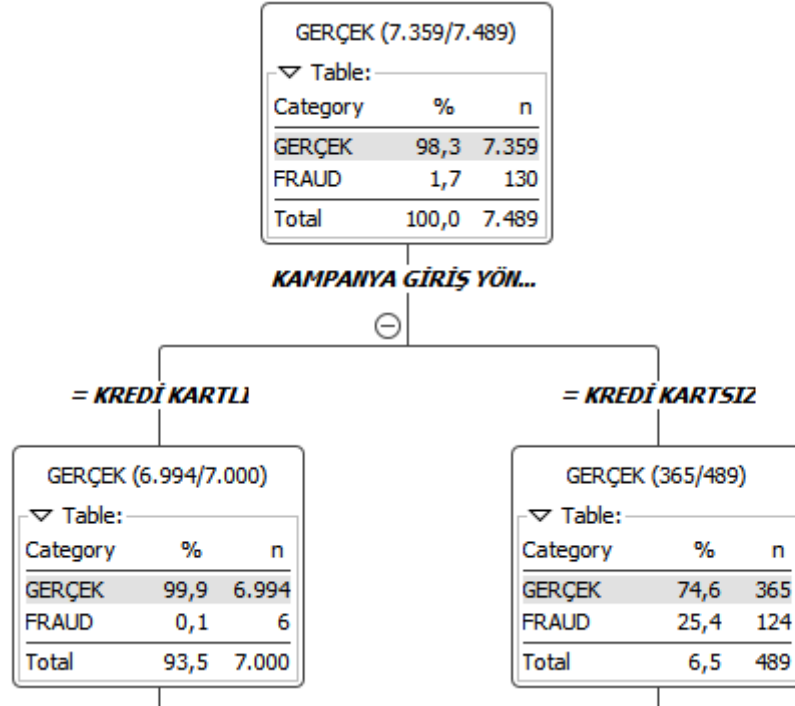
Şekil.37. Color Manager Görünümü

Ayarların yapılmasının akabinde karar ağacı oluşturulmuştur. Oluşturulan karar ağacının ve kullanılan araçların ekran görüntüleri aşağıdaki gibidir.



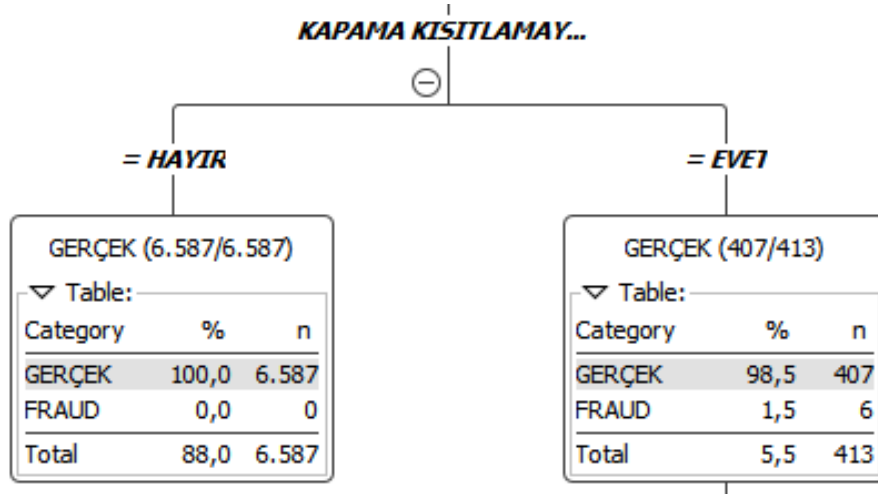
Şekil.38. Karar Ağacı ve KNIME Analiz Görünümü

Uygulamada kullandığımız tüm verilerde dolandırıcılık oranı %1.7'dir. Dolandırıcılık tahmininde en önemli parametrenin ise kredi kartı kullanılıp kullanılmaması olduğu görülmektedir. Şekilde görüldüğü gibi normalde %1.7 olan dolandırıcılık oranı kredi kartı olmadan yapılan işlemlerde %25.4'e çıkmaktadır



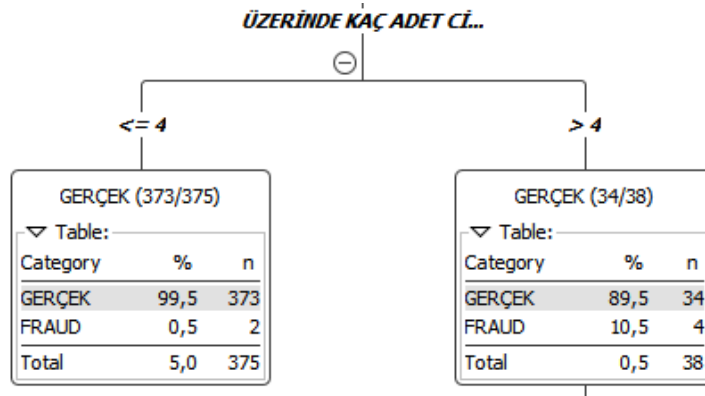
Şekil.39. Karar Ağacı Kampanya Giriş yöntemi

Kredi kartı alanındaki düğümünden ağaç açılmaya devam edilmiştir. Bir sonraki düğüm noktası abonenin kapama kısıtlamaya girip girmediğidir. Hem kredi kartı ile yararlanıp hem de kapama kısıtlamaya girmeyen abonelerden 6587 tanesi gerçek abonedir. Bunun nedeni, kredi kartlı yararlanacağını bilmesine rağmen hiçbir borcunu ve faturasını geç ödemiş ve kapama kısıtlama görmemiştir. Kredi kartlı yararlanabilmesi sadece fatura toplamının istediği cihaz için gerekli minimum tutarı sağlamıyor oluşudur. Ancak kredi kartlı yararlanan ve kapama kısıtlama görmüş aboneler içerisinde 6 adet sahte müşteri bulunmaktadır. Çünkü bu şahıslar, kredi kartlı yararlanacağını bildikleri için, borçlarını da ödemiş ve kısıtlama görmüşlerdir.



Şekil.40. Karar Ağacı Kapama Kısıtlama Görünümü

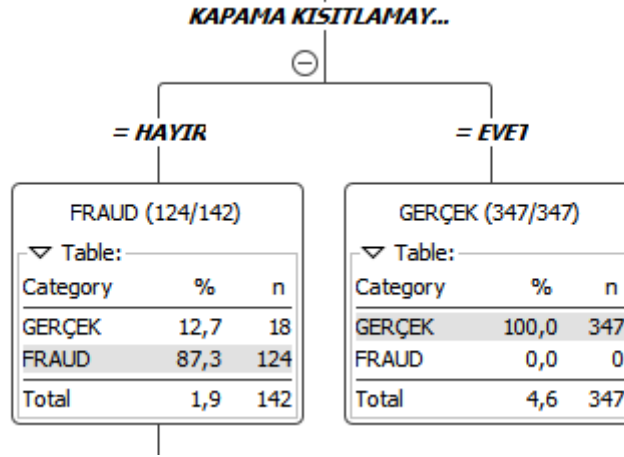
Kapama kısıtlaması evet olan düğüm açılmaya devam edilmiştir. Bir sonraki düğüm şahısın üzerinde kaç adet cihazın olduğu ile ilgilidir. Dört ve dörtten az cihazı olan 375 müşterinin 373 ü gerçek iken 2 tanesi dolandırıcıdır. Diğer taraftan dörtten fazla cihazı olan 38 müşterinin dördü sahte müşteridir. 6 adet dolandırıcı müşterinin böylelikle hangi özelliklerinin olduğunu ve hangi alanda kendilerine yer edindiğini gördük.



Şekil.41. Karar Ağacı Cihaz Sayısı Görünümü

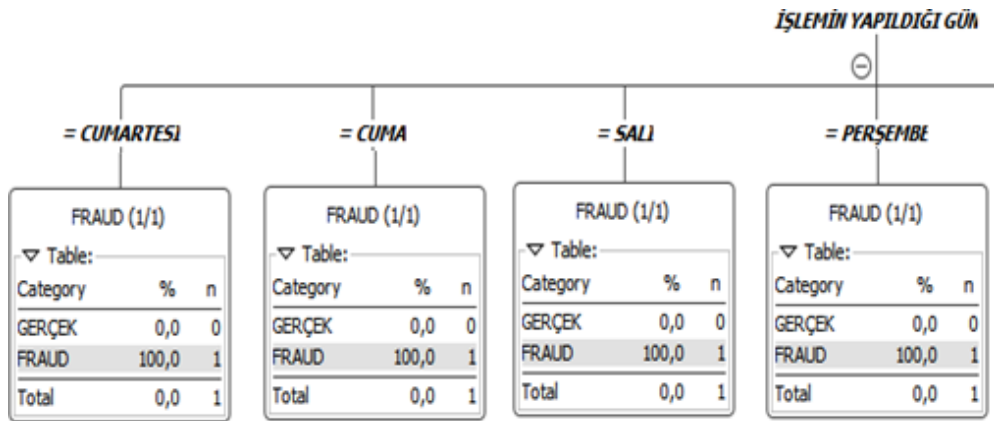
Dolandırıcı müşterilerin en fazla başvurdukları kredi kartsız cihaz kampanyalarından yararlanma alanı için, karar ağacımızın kredi kartsız düğümü açılmıştır. Bir sonraki düğüm kapama kısıtlama görüp görmediği ile ilgilidir. Bu düğümde dikkat edilmesi gereken bir nokta bulunmaktadır. 347 müşteri kredi kartsız cihaz kampanyasından yararlanırken neden kapama kısıtlama görmüştür. Diğer

tarafından kapama kısıtlama görmüş 347 müşteri neden kredi kartsız cihaz kampanyasından yararlanmaktadır. Yapılan çalışmalarda 347 müşterinin simkartlarını kaybettiği kendilerinin bilgisi dahilinde hatlarını operatör yardımı ile kısıtlıya aldıkları görülmüştür. Herhangi bir geç ödeme yada borç ile bu müşteriler kısıtlama ve kapama görmedikleri için cihaz kampanyasına giriş izni kredi kartsız olarak verilmektedir.



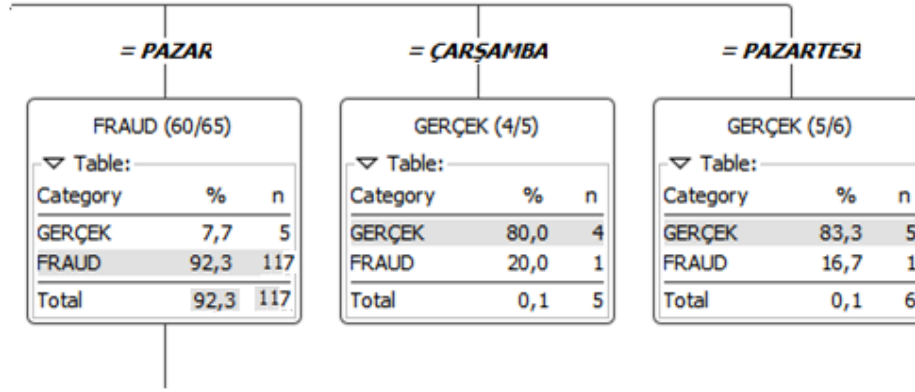
Şekil.42. Karar Ağacı Kapama Kısıtlama Durumu

Kapama kısıtlaması hayır olan düğüm açılmaya devam edilmiştir. Bir sonraki düğüm işlemin yapıldığı gündür. Pazar günleri yani müşteri yoğunluğunun en fazla olduğu günlerde dolandırıcılık girişimleri en fazla adeti aldığı görülmüştür.



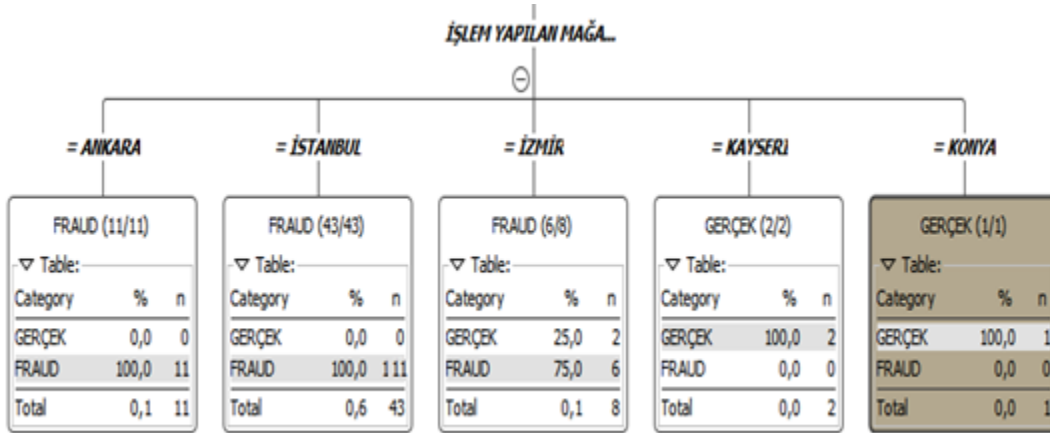
Şekil.43. Karar Ağacı İşlem Yapılma Günü

Pazar günü 124 sahte işlemin 117 sinin yapıldığı gündür.



Şekil.44. Karar Ağacı İşlem Yapılma Günü

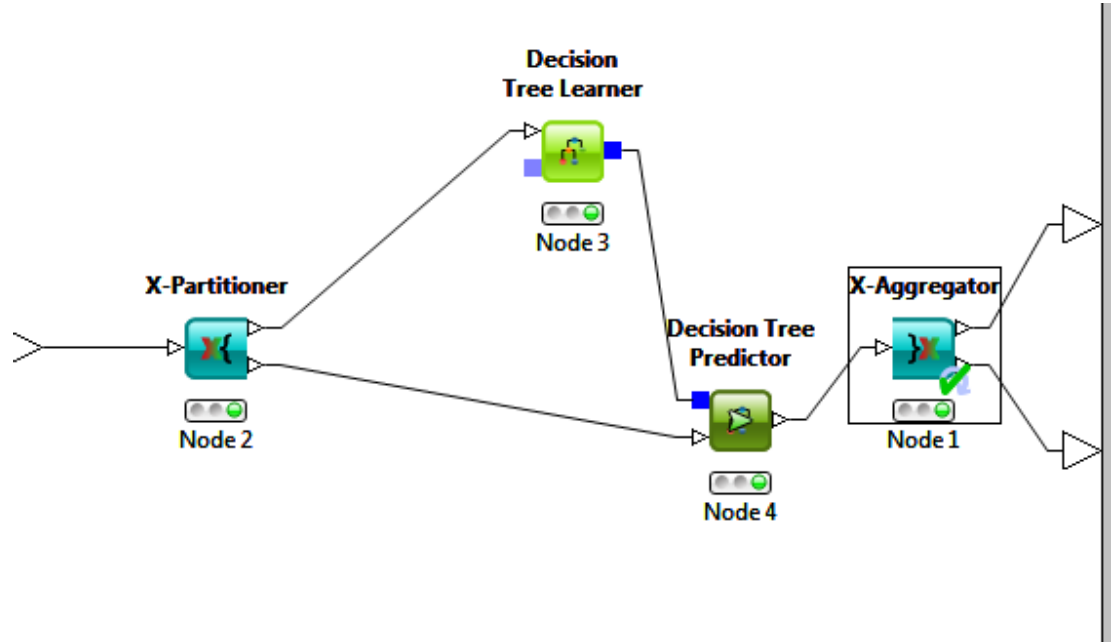
Karar ağacı açılmaya devam edilmiştir. Bir sonraki düğüm işlemin yapıldığı mağazaların bulunduğu illerdir. En fazla dolandırıcılık girişiminin olduğu mağazalar İstanbul da görülmektedir. İstanbul da yer alan mağazalar incelemeye alınmıştır. Bu mağazaların büyük bir çoğunluğunun polis noktasına olan uzaklıklarının diğer illerdeki mağazalara oranla yüksek olduğu görülmüştür.



Şekil.45. Karar Ağacı İşlem Yapılan Mağaza

5.4.7. Karar Ağacı Doğruluk Analizi

Karar ağacı ile yapılan analizin doğru olup olmadığını KNIME içerisindeki ‘Validation’ özelliği ile test ettik. Veriler ilk X-Partitioner ile ayrıştırıldı, ve veriler doğrulandı. Karar ağacına uygulanan yöntem aşağıdaki şekilde görüldüğü gibidir.



Şekil.46. Karar Ağacı Doğruluk Analizi

5.4.8. Karar Ağacının SISNET' e Entegre Edilmesi

Karar ağacından 3 en önemli sonuç çıkmıştır. Bunlar müşterinin kapama kısıtlama durumu, müşterinin hatlarındaki cihaz sayısı, işlem yapılan gün ve işlem yapılan mağazadır. Bunlara göre SISNET üzerinde entegre aşamasında olan yeni bir sistem daha geliştirilmiştir. Müşterinin bilgileri girildikten sonra sağ tarafta, ekstradan operatör sistemine bakılıp yazılabilecek alanlar eklenmiştir. Kapama kısıtlama durumu ve abonenin üzerindeki hat sayısı operatör sistemine bakılıp yazılacaktır. Diğer iki alan ise doldurulduktan sonra devam tuşu tıklanacak ve müşterinin hangi statüde olduğu görülecektir.

1. Müşteri Bilgileri

Ad:	<input type="text"/>	KAPAMA KISITLAMA DURUMU	<input type="text"/>
Soyad:	<input type="text"/>	MÜŞTERİNİN HATLARINDAKİ CİHAZ SAYISI	<input type="text"/>
TC Kimlik No:	<input type="text"/>	İŞLEM YAPILAN GÜN	<input type="text"/>
Kimlik Tipi:	<input type="text" value="Nüfus Cüzdanı"/>	İŞLEM YAPILAN MAĞAZA	<input type="text"/>
Kimlik Seri No:	<input type="text"/>		
Kimlik Verilme Tarihi:	<input type="text"/>		
Cinsiyet:	<input checked="" type="radio"/> Erkek <input type="radio"/> Kadın		
Anne Kızlık Soyadı:	<input type="text"/>		
İrtibat Numarası:	<input type="text"/>		
Doğum Tarihi:	<input type="text"/>		
Doğum Yeri:	<input type="text"/>		
Baba Adı:	<input type="text"/>		
Anne Adı:	<input type="text"/>		

Şekil.46. SISNET Dolandırıcı Müşteri Tespiti

DOLANDIRICILIK ANALİZ EKRANI

KAPAMA KISITLAMA DURUMU : HAYIR
MÜŞTERİNİN HATLARINDAKİ CİHAZ SAYISI : 8
İŞLEM YAPILAN GÜN : PAZAR
İŞLEM YAPILAN MAĞAZA : KONYA E. MAĞAZASI

SONUÇ : MÜŞTERİ YÜZDE 76.5 DOLANDIRICI OLABİLİR. İŞLEM YAPMADAN ÖNCE MERKEZ İLE İLETİŞİME GEÇİNİZ.

Şekil.47. SISNET Dolandırıcı Müşteri Uyarı Ekranı

Hangi yüzdelerde işleme izin verileceği hangi yüzdelerde uyarı çıkarılıp işlemin engelleneceği operatöre bağlıdır.

5.4.9. Uygulamanın Geliştirilme Çalışmaları ve Scorer Özelliği

SISNET'e entegre edilen mevcut uygulama, statik veriler içermektedir. Yani belli bir dönem arasında dolandırıcılık girişimi yapan şahısları kapsamaktadır. Geliştirilecek uygulama ile verilerin dinamik yani sürekli kendini yenileyen halde olması sağlanacaktır. Böylelikle belli bir noktada artan dolandırıcılık analizi sisteme işlenecek ve o noktaya özel önlem alınmaya çalışılacaktır.

Bunun yanında SISNET'e entegre edilecek olan KNIME SCORER özelliği ile istatistiki veriler çekilerek bir ön izleme oluşturulacaktır. Bu özellik ile dolandırıcılık girişimlerinin birbirleri ile ilişkisi, hangi noktalarda ve abone profillerinde bağlılık gösterdiği, kullanıcıya veya denetleyiciye bir ön bilgi vermek amacıyla eklenecektir.

5.4.10. Değerlendirme

Dolandırıcılık tespiti literatürde fark sapmaları adıyla da anılmaktadır. Dolandırıcılık tespiti aslında bir örüntü tanıma problemidir. Bilgisayar alışveriş yapan hesapları sürekli takip ederek daha önce dolandırıcılık yaptığı belirlenen hesaplardaki alışveriş örüntüsüyle izlenmekte olan hesabın alışveriş örüntüsünü karşılaştırarak bu hesaplar arasında benzerlik arar. Daha önce dolandırıcılık yaptığı belirlenen hesaplar ile izlenen hesaplar arasında benzerlik aramaktadır.[41]

Operatörlerin kendilerine ait bir veri bankası bulunmaktadır. Ancak bu veri bankaları genel olarak müşterilerin konuşma zamanlarını, attıkları sms leri ya da, geç ödedikleri faturalarına göre müşterileri kategorize etmektedir. Kısaca operatörler kampanya yapabilecek müşteri aramakta ve daha fazla gelir elde etme çabasındadırlar. Unutulmamalıdır ki gelir elde etmenin yanında, elde edilen geliri korumak ve suçsuz müşterileri korumakta operatörlerin görevidir. Bu bağlamda düşünüldüğünde, yaptığımız karar ağacına benzer bir yöntemi operatörler kendi sistemlerine entegre etmelidirler.

Veriler içerisinde 130/7359 dolandırıcı oranı bulunmaktadır. Asıl amaç bu oranın aşağıya çekilmesidir. Karar ağacı incelenip, dolandırıcılığa asıl etkenin nelerin olduğuna bakıldığında ve bu etkenler, SISNET üzerine bir uygulama olarak eklendiğinde dolandırıcı kişilerin kaçış yolu olmayacaktır.

SISNET bir evrak kontrol alanıdır. Personellerin hata yapabileceği ve evraklarda var olan dolandırıcılık olaylarını göremeyecekleri için geliştirilmiştir. Keza mağaza kontrol birimi de, SISNET e yüklenmeden herhangi bir işlemin yapılmasının önüne geçilmesi amacıyla mağazaların kendilerinin oluşturdukları bir alandır. Ancak her iki alanı geçebilecek dolandırıcı kişilerin önüne veri madenciliği gelmelidir. Veri madenciliği ile dolandırıcılık tespiti aslında geçmişten ders alma ve bunu anlaşılır olarak görebilmektir.

SONUÇ ve ÖNERİLER

Sahtekarlık girişiminde bulunacak şahıslar her zaman yükte hafif pahada ağır ürünler tercih ederler. GSM sektöründe de durum aynıdır. Yüksek değerlikte ve piyasada anında paraya dönüştürülebilecek cihazlar sahtekar kişilerin en önemli hedefleridir.

Sektördeki sahtekarlık çeşitleri gün geçtikçe çeşitlenmekte ve artmaktadır. Buna istinaden operatörler her zaman bir adım geriden takip etmekte ve bu açığı bulup kapatma gayretindedirler. Bu bağlamda çeşitli öneriler tezde belirtilmiştir.

SISNET yani online evrak kontrolü sahtekar kişilerin önüne büyük ölçüde geçecektir. Verdikleri evrakların bir çok kişi tarafından kontrol edileceğini bilen şahıslar bu sistemin kurulu olduğu mağazalara gelirken bir kere daha düşüneceklerdir.

Mağaza kontrol birimi sisteminin kurulması ve uygulanması ilede, operatör çalışanı ile ortaklaşa yapılabilecek sahtekarlık girişiminin önüne geçilecek, hiçbir işlem SISNET onaysız mağazadan dışarı çıkamayacaktır.

Diğer taraftan tüm bu birimlerin bir şekilde geçildiği çaresiz kaldırı durumlarda devreye veri madenciliği gelecektir. Veri madenciliği ile sahtekarlık tespiti bir koşullu öğrenmedir. Yani sahtekarlık girişiminde bulunan şahıslar ile gerçek müşterilerin bilgileri veri ambarında depolanacak, yeni gelen müşteriler için uygulanacaktır. Yeni gelen müşterilerin özelliklerinin hangi kategoriye girdiği daha önce elde edilen veri ambarından veri madenciliği ile çıkarılacak ve müşteriye uygulanacaktır. Bu sistemlerin kurulması ve entegre edilmesi ile sahtekarlık girişimleri önemli derecede düşecek şahıslara hiçbir açık kapı bırakılmayacaktır.

KAYNAKLAR

- [1] Özgün, A., *Cep Telefonuna Yönelik Suçlar*, s. 15, Adalet Yayınevi, Ankara, 2009
- [2] Özgün, A., *Cep Telefonuna Yönelik Suçlar*, s. 15, Adalet Yayınevi, Ankara, 2009
- [3] Yiğitbaşı, N., *Ağ Güvenliği*,
http://web.itu.edu.tr/~orencik/AgGuvenligi2007Sunumlari/yigitbasi_gsm_rapor.doc, 2012.
- [4] Yiğitbaşı, N., *Ağ Güvenliği*,
http://web.itu.edu.tr/~orencik/AgGuvenligi2007Sunumlari/yigitbasi_gsm_rapor.doc, 2012.
- [5] Can, E., *Mobil Cihazların Çalışma Sistemleri ve Çevre Üzerindeki Etkileri*, Yüksek Lisans Tezi, Gazi Üniversitesi, 2006.
- [6] Turkcell, *Genel Bakış*,
<http://www.turkcell.com.tr/site/tr/turkcellhakkinda/Sayfalar/genel-bakis/genel.aspx>, 2012.
- [7] Vodafone, *Tarihçe*,
http://www.vodafone.com.tr/VodafoneHakkinda/tarihce_home.php?default_id=hakkimizda-tarihce, 2012
- [8] Avea, *Avea Hakkında*,
http://www.avea.com.tr/web/Hakkimizda/SirketHakkinda/AveaHakkinda?sc_device=default&persistent=true, 2012
- [9] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [10] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [11] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [12] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012

- [13] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [14] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [15] Bilgi Teknolojileri ve İletişim Kurumu, *Üç Aylık Pazar Verileri Raporu*.
http://tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php, 2012
- [16] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [17] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [18] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [19] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [20] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [21] Turhan, O., *Bilgisayar Ağları İle İlgili Suçlar*, Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.
- [22] Ofluoğlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [23] Ofluoğlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [24] Ofluoğlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.

- [25] Ofluođlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [26] Ofluođlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [27] Ofluođlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [28] Ofluođlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [29] Ofluođlu, R., *Resmi Belgede Sahtecilik*, <http://rahmiofluoglu.wordpress.com/vekalet-bilgileri/dernek-uye-formu/iletisim/adaleti-adaletten-talep-edelim/haciz/nitelikli-dolandiricilik/resmi-belgede-sahtecilik-suclari>, 2012.
- [30] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [31] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [32] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [33] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [34] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [35] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [36] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [37] Türk Ceza Kanunu, <http://www.tbmm.gov.tr/kanunlar/k5237.html>, 2012
- [38] Haber Türk, <http://www.haberturk.com/gundem/haber/750780-bu-haber-aslinda-neyi-anlatiyor-biliyor-musunuz>, 2012
- [39] Karacan, H. Yeşilbudak, M., *Kullanıcı Merkezli İnteraktif Veri Madenciliđi: Bir Literatür Taraması*, Bilişim Teknolojileri Dergisi, 2010.

- [40] Karacan, H. Yeşilbudak, M., *Kullanıcı Merkezli İnteraktif Veri Madenciliği: Bir Literatür Taraması*, Bilişim Teknolojileri Dergisi, 2010.
- [41] Silahtarođlu, G., *Kavram ve Algoritmalarıyla Temel Veri Madenciliđi*, s. 46, Papatya Yayıncılık, İstanbul, 2008
- [42] Silahtarođlu, G., *Kavram ve Algoritmalarıyla Temel Veri Madenciliđi*, s. 38, Papatya Yayıncılık, İstanbul, 2008

ÖZGEÇMİŞ

23 Ocak 1989 İstanbul doğumluyum. İstanbul Tayfur Sökmen İlköğretim Okulu ve Kumsal Ortaokulunu bitirdikten sonra Kadriye Morođlu Lisesinde, öğrenimime devam ettim. Kırıkkale Üniversitesi Fen Fakültesi Kimya Bölümünü bitirdikten Beykent Üniversitesi Bilgi Teknolojileri Bölümünde yüksek lisansa başladım. Öğrenim hayatıma devam ederken, Türkiye'nin önde gelen GSM ve distribütör firmalarında çalışma şerefine eriştim. Bekarım ve İngilizce bilmekteyim.

Hakan Ahmet KILIÇARSLAN

TEŐEKKÜR

Öncelikle her türlü destek ve emeğini esirgemeyen ablam Meral KILIÇARSLAN ve annem Meryem GÜNEY'e, tezin hazırlanmasında ve her türlü aşamalarda destek veren Doç. Dr. Gökhan SİLAHTAROĞLU hocama, SISNET projesinin hayata geçirilmesinde öncü olan ve bizlere yol gösteren proje müdürüm Sn. Cenk ÇOLPAN' a, söyleşimi kabul eden ve cevaplarıyla 1. Bölüm'de yer alan Türkiye'de GSM Sektörünün Yorumlanması alanına destek veren genel müdürüm Sn. Koray ÖZCAN' a, ve değerli çalışma arkadaşım Ersel TOSUN' a en derin saygı ve şükranlarımı sunarım.