

T.C
SELÇUK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FİNANS SEKTÖRÜNDE
VERİ MADENCİLİĞİ
İLE
DOLANDIRICILIK TESPİTİ

Ercan ÖZBAY

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
Konya, 2007

Yüksek Lisans Tezi

FİNANS SEKTÖRÜNDE
VERİ MADENCİLİĞİ
İLE
DOLANDIRICILIK TESPİTİ

Ercan ÖZBAY

T.C.

Selçuk Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Bu tez 28.06.2007 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr. Ahmet ARSLAN Prof. Dr. Şirzat KAHRAMANLI Yrd. Doç. Dr. Mesut GÜNDÜZ

(Danışman)

(Üye)

(Üye)

ÖZET

Yüksek Lisans Tezi

FINANS SEKTÖRÜNDE

VERİ MADENCİLİĞİ

İLE

DOLANDIRICILIK TESPİTİ

Ercan ÖZBAY

T.C.

Selçuk Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Ahmet ARSLAN

2007, 94 Sayfa

Jüri

Prof. Dr Ahmet ARSLAN

Prof. Dr. Şirzat KAHRAMANLI

Yrd. Doç. Dr. Mesut GÜNDÜZ

Dolandırıcılık işlemleri kendisini hemen hemen her alanda göstermektedir. İnternet Bankacılığı bu saldırılara en fazla maruz kalan sektörlerin başında gelmektedir. Bu tezde internet Bankacılığında yapılan dolandırıcılık işlemlerinin, veri madenciliği teknik ve metotları kullanılarak belli ölçülerde önlenmesi sağlanmıştır. İnternet Bankacılığındaki müşteri işlemleri incelenmiştir. Müşteri grupları müşterinin yaptığı işlemlere göre belirlenerek , her bir müşteri bir müşteri grubuna atanmıştır. Veri içerisindeki müşteriler, grup olarak belirtilmiştir. Hesaplamalarda müşteri yerine müşteri grubu kullanılmıştır. Eğitim verileri belli parçalara ayrılarak sınıflandırmada veri fazlalığından kaynaklanan sorunlar en aza indirgenmiştir. Oluşturulan her bir parça için C4.5 ve Saf Bayes Sınıflandırıcı uygulanmıştır. Böylece iki adet sınıflandırıcının yetersiz olduğu noktalar azaltılmıştır. Sınıflandırıcıların sonucundan oluşan çıkış verileri üzerinde sadeleştirme işlemleri yapılarak tekrar Saf Bayes Sınıflandırıcıya sokulmuştur. Sonuçta etkili bir dolandırıcılık tespit sistemi oluşturulmuştur. 12773 adet işlem incelenmiştir. Bunun 12000 adedi yasal,773 adedi suçludur.

Anahtar Sözcükler: Saf Bayes Sınıflandırıcı, C4.5 sınıflandırıcı, Dolandırıcılık, Dolandırıcılık Tespit Sistemi, Veri Madenciliği.

ABSTRACT
Master Thesis
FRAUD DETECTION
IN
A FINANCE ASSOCIATION
BY
DATA MINING

Ercan ÖZBAY

Selçuk University
Graduate School of Natural and Applied Sciences

Department of Computer Engineering

Supervisor: Prof. Dr. Ahmet ARSLAN
2007, 94 Pages

Jury: Prof. Dr. Ahmet ARSLAN
Prof. Dr. Şirzat KAHRAMANLI
Yrd. Doç. Dr. Mesut GÜNDÜZ

Fraud processes can be seen on almost every where of the life. Internet Banking systems are primarily effected from the fraud attacks. In the thesis; the prevention mechanism of fraud processes in the Internet banking with available measurement by using data mining techniques and methods is proved. The Internet Banking customers' processes are examined. Customer groups according to customer's processes are defined and every customer is assigned to a customer group. Customer group is used instead of customer in calculations. Training data is splitted to fragments so, problems caused by large data are minimized. The C4.5 classifiers and the Naive Bayesian Classifiers are applied for every piece. By this way, disabilities of two classifiers are decreased. Outputs of the results of classifiers are simplified and then they are used as an input for Naive Bayesian Classifier. As a result effective Fraud Detection System is designed. 12773 processes is examined. 12000 processes are legal and 773 are fraud processes of these records.

Key Words: Saf Bayes Classifiers, C4.5 Classifiers, Fraud, Fraud Detection System, Data Mining.

ÖNSÖZ

İnternet günümüzde olmazsa olmaz gerçekler arasına girmiştir. Bu gerçeği kendi yapısına entegre etmemiş kurumlar yok olmaya mahkumdur. İnternet teknolojisinden tüm şirketler, devlet kurumları mümkün olduğunca faydalanmaktadır. En büyük kullanım oranı ise bankacılık sektöründe kendini göstermektedir. Banka şubeleri internete taşınmıştır. Böylece müşteriler için daha az bekleme, daha çok iş ortaya çıkmakta, banka için ise daha az personel ,ihtiyacı ve daha çok müşteri memnuniyeti oluşmaktadır. Bu tezde müşterilerin İnternet Bankacılığından en iyi şekilde yararlanırken , oluşabilecek maddi manevi zararı önlemeye veya azaltmaya çalışılmıştır.

Bu tez çalışmasında bana büyük desteği ve katkısı olan danışmanım Prof. Dr. Ahmet ARSLAN' a , Şeker Bilişim Şube Müdürü Volkan IRAVUL'a ve manevi desteğini hiçbir zaman esirgemeyen eşim Hülya ÖZBAY'a çok teşekkür ederim.

İÇİNDEKİLER

1	GİRİŞ	1
1.1	Problemin Tanımı	1
1.2	Amaç	2
2	LİTERATÜR ARAŞTIRMASI	3
3	İNTERNET BANKACILIĞI	5
3.1	İnternet Bankacılığında Yapılabilecek İşlemler	6
3.1.1	Hesaplar	6
3.1.1.1	Varlıklar	6
3.1.1.2	Hesap Hareketleri	6
3.1.1.3	Yatırım Hesapları	6
3.1.1.4	Kredi Hesapları	6
3.1.1.5	İnternet İşlemleri	7
3.1.1.6	Özel Hesap İşlemleri	7
3.1.1.6.1	Özel Hesap Tanımlama	7
3.1.1.6.2	Günlük Ödeme Bilgileriniz	7
3.1.1.6.3	Özel Hesap Görüntüleme/Güncelleme	8
3.1.1.6.4	Özel Hesap Günlük İşlem Bilgileriniz	8
3.1.1.7	Karta Hesap Bağlama	8
3.1.1.8	Hesap Açılışı	8
3.1.1.9	Portföy	8
3.1.2	Çek ve Senet İzleme	9
3.1.2.1	Tahsil Teminat Çekleri	9
3.1.2.2	Senetler	9
3.1.2.3	Çek Karnesi	9
3.1.3	Döviz İşlemleri	9
3.1.3.1	Döviz Alış	9
3.1.3.2	Döviz Satış	10
3.1.4	Kredi Kartları	10
3.1.4.1	İzleme	10
3.1.4.2	Borç Ödeme	10
3.1.4.3	Kart No ile Borç Ödeme	10
3.1.4.4	Nakit Avans	10
3.1.4.5	Ekstre Talimatı	10
3.1.4.6	Otomatik Ödeme Talimatı	10
3.1.4.7	Şifre Alma / Değişirme	11
3.1.4.8	Telefonla Uyarı	11
3.1.4.9	Kart Başvurusu	11
3.1.4.10	Görüntüleme/Güncelleme	11
3.1.4.11	İşlem ve Saat Limitleri	11
3.1.5	Tanımlamalar	12
3.1.5.1	Parola Değişirme	12
3.1.5.2	Şifre Değişirme	12
3.1.5.3	Güvenlik Ayarları	12
3.1.5.3.1	Zaman Ayarları	12
3.1.5.3.2	IP Aralık Belirleme	12
3.1.5.3.3	Tatil Tanımlama	12
3.1.5.3.4	Para Transferini Kapama/Kısıtlama	12

3.1.5.3.5	Para Transferi Uyansız Tanımlama	12
3.1.5.3.6	Hesap ayarları	13
3.1.5.3.7	Güvenlik Sorusu	13
3.1.5.3.8	Güvenlik Sorusu Değişirme	13
3.1.5.3.9	Durum İzleme	13
3.1.5.4	Telefon Bankacılığı Şifre Değişirme	13
3.1.5.5	Hesap Rumuzu Tanımlama	13
3.1.5.6	Renk Seçimi	13
3.1.5.7	Şifre Üretici İşlemleri	13
3.1.5.7.1	Şifre Üreticisini Kullanma Açma	13
3.1.5.7.2	Şifre Üreticisini Kullanarak İnternet Bankacılığına Giriş	14
3.1.5.7.3	Şifre Üreticinin Ürettiği Şifrenin Yanlış Girilmesi	14
3.1.5.7.4	Şifre Üreticinin Kaybolması veya Çalınması	14
3.1.5.7.5	Şifre Üreticini Kullanma Kapatma	14
3.1.6	Kur ve Oranlar	15
3.1.6.1	Döviz Kurları	15
3.1.6.2	Repo Faiz Oranları	15
3.1.6.3	Vadeli Mevduat Faiz Oranları	15
3.1.6.4	Bireysel Krediler Faiz Oranları	15
3.1.6.5	Kıymet Fiyatları	15
3.1.7	Ödemeler	16
3.1.7.1	Fatura Ödeme	16
3.1.7.2	Fatura Ödeme Talimatı	16
3.1.8	Para Transferleri	16
3.1.8.1	Havale ve EFT	16
3.1.8.2	Hesaplarınız Arasında Transfer	17
3.1.8.3	Başka Banka KK Ödeme	17
3.1.8.4	Toplu Para Transferi	17
3.1.8.5	Düzenli Ödeme	17
3.1.8.6	Talimat İzleme	17
3.1.8.7	Çok Kullandıklarım	18
3.1.8.8	Döviz Transferi(SWIFT)	18
3.1.8.8.1	Giriş	18
3.1.8.8.2	İptal	19
3.1.8.8.3	İşlem Ücret ve Limiti	19
3.1.8.8.4	Önemli Noktalar	19
3.1.8.9	Hızlı Gönder	20
3.1.9	Yatırım İşlemleri	20
3.1.9.1	Repo	20
3.1.9.2	Repo İzleme	20
3.1.9.3	Vadeli Hesap İşlemleri	20
3.1.9.4	Fon İşlemleri	21
3.1.9.5	Fon Alım/Satımı	21
3.1.9.6	Fon Fiyatları	21
3.1.9.7	Fon Portföy	21
3.1.9.8	Fon Hareketleri	21
3.1.9.9	Fon Emir Listesi	21

	3.1.9.10	Hazine Bonosu/Devlet Tahvili/Eurobond	22
	3.1.9.11	Hisse Senedi İşlemleri	23
	3.2	Sonuç	23
4		İNTERNET BANKACILIĞINDA GÜVENLİK	24
	4.1	İnternet Bankacılığında Güvenlik Unsurları	24
	4.1.1	SSL 128 Bit Şifreleme	24
	4.1.2	Şifre Alma Aşamasında Bankamatik Kart Şifresinin Sorulması	24
	4.1.3	Banka Telefon Yetkilisi Tarafından Sorulan Güvenlik Soruları	24
	4.1.4	Doğum tarihi ve TC. Kimlik No Kontrolü	24
	4.1.5	Sanal Klavye Kullanımı	24
	4.1.6	Şifre Üreteci	25
	4.1.7	Hatalı Parola ve Şifre Girişinin Gösterilmesi	25
	4.1.8	Otomatik Oturum Kapatma	25
	4.1.9	Güvenlik Sorusu	25
	4.1.10	Zaman ve Tatil Ayarları	25
	4.1.11	IP Aralık Belirleme	25
	4.1.12	Para Transferini Kapatma ve Kısıtlama	26
	4.1.13	Para Transferi Uyarısı Tanımlama	26
	4.1.14	Hesap Ayarları	26
	4.2	İnternet Bankacılığında Saldırıları	26
	4.2.1	Keylogger Saldırıları	27
	4.2.2	Keylogger Saldırılarından Korunma	27
	4.2.3	Olta(Phishing) Saldırıları	28
	4.2.4	Olta(Phising) Saldırılarından Korunmak İçin	29
	4.2.5	Casus Yazılımlar ve Diğer Saldırıları	30
	4.2.6	Alınması Gereken Önlemler	31
	4.2.7	İnternet Explorer ve Güvenlik	32
	4.3	Sonuç	33
5		DOLANDIRICILIK	34
	5.1	Bilişim Dolandırıcılığı	34
	5.1.1	Bilişim Suçlarının Kapsamı, Tanımlamaları ve Sınıflandırılması	34
	5.1.2	Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme	35
	5.1.3	Bilgisayar Sabotajı	35
	5.1.4	Bilgisayar Yoluyla Dolandırıcılık	36
	5.1.5	Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı	36
	5.1.6	Yasadışı Yayınlar	36
	5.1.7	Yaşanan Problemler ve Çözüm Yöntemleri	37
	5.1.7.1	Elde Edilen Delillerin Hukuki Durumu	38
	5.1.7.2	Delillerin Elde Edilmesi	38
	5.1.7.3	Uluslararası Polis İşbirliği	38
	5.1.7.4	Uluslararası Suçun Tanımlanması	39
	5.2	Sonuç	39
6		VERİ MADENCİLİĞİ	40
	6.1	Giriş	40
	6.2	Veri Madenciliğine Genel Bakış (Tarihçe)	42
	6.3	VM Çekirdek Sistemi (VMÇS)	42
	6.4	VTBK ile Makine Öğrenimi Arasındaki İlişki	43

6.5	VTBK ile İstatistik Arasındaki İlişki	43
6.6	VM ile Veri Tabanı Arasındaki İlişki	43
6.7	Veri Madenciliğinde Karşılaşılan Problemler	43
6.7.1	Veri Tabanı Boyutu	44
6.7.2	Gürültülü Veri	44
6.7.3	Boş Değerler	45
6.7.4	Eksik Veri	45
6.7.5	Artık Veri	46
6.7.6	Dinamik Veri	46
6.8	Veri Madenciliği Algoritmaları	46
6.8.1	Hipotez Testi	47
6.8.2	Sınıflama Algoritması	47
6.8.3	Kümeleme Algoritması	47
6.8.4	İlişkilendirme Algoritması	47
6.8.5	Zaman Serileri Arasındaki Bağımlılıklar	48
6.8.6	Sıra Örüntüler	48
6.9	Sonuç	48
7	TEZ KAPSAMINDA KULLANILAN VERİLER	49
7.1	Aylara Göre Yasal ve Suçlu Oranları	49
7.2	Haftanın Günlerine Göre Yasal ve Suçlu Oranları	50
7.3	Günlere Göre Yasal ve Suçlu Oranları	50
7.4	Zamana Göre Yasal ve Suçlu Oranları	51
7.5	Gönderilen Tutara Göre Yasal ve Suçlu Oranları	51
7.6	Gönderilen Kişiye Göre Yasal ve Suçlu Oranları	52
7.7	Gönderilen IP'ye Göre Yasal ve Suçlu Oranları	53
7.8	Gönderilen Bankaya Göre Yasal ve Suçlu Oranları	53
7.9	Gönderilen Şubeye Göre Yasal ve Suçlu Oranları	54
7.10	Sonuç	54
8	MATERYAL VE YÖNTEM	55
8.1	Materyal	55
8.2	Yöntem	55
8.2.1	Tez Kapsamında Kullanılan Veri Madenciliği Algoritmaları	55
8.2.1.1	Karar Ağaçları	55
8.2.1.1.1	ID3 ve C4.5 Karar Ağaçlarının Kurulması	56
8.2.1.1.1.1	ID3'ün Temeli	57
8.2.1.1.1.2	Tanımlamalar	58
8.2.1.1.1.3	Kazanç Oranlarının Kullanımı	59
8.2.1.1.1.4	C4.5 Algoritması	60
8.2.1.1.1.5	Karar Ağaçlarının Budanması	60
8.2.1.2	Saf Bayes Sınıflandırması	61
8.2.1.2.1	Bayes Teoremi	61
8.2.1.2.2	Saf Bayes Sınıflandırması	62
8.2.1.2.3	Örnek olarak Saf Bayes Sınıflandırması Kullanarak Bir Sınıf Üyeliğinin Bulunması	63
9	TEZ KAPSAMINDA KULLANILAN İNTERNET BANKACILIĞINDA DOLANDIRICILIK TESPİTİ	65
9.1	Tez Kapsamında Oluşturulan Dolandırıcılık Tespit Sistemi	66

9.1.1	Verilerin Müşteri Veritabanından Çekilmesi	66
9.1.2	Müşterinin Genel Özelliklerinin Belirlenmesi	66
9.1.3	Müşteri Grup Bilgilerinin Oluşturulması	66
9.1.4	Müşterinin Müşteri Grubu Olarak Adlandırılması ve Verinin Bölümlemesi	71
9.1.5	C4.5 ve Saf Bayes Sınıflandırıcıların Bölümlere Uygulanması	71
9.1.5.1	C4.5 Sınıflandırıcısının Bölümlere Uygulanması	71
9.1.5.1.1	C4.5 Algoritmasına Göre Sınıflandırma Sonuçları	73
9.1.5.2	Saf Bayes Sınıflandırıcısının Bölümlere Uygulanması	74
9.1.5.2.1	Bölümlerin Saf Bayes Sınıflandırmasına Göre Sonuçları	78
9.1.6	Sınıflandırma Sonuçlarının İşlenmesi	78
9.1.6.1	Giriş ve Çıkış Veri Sonuçları	79
9.1.7	Sonuçların Saf Bayes Sınıflandırıcıya Uygulanması	79
9.1.7.1.1	Girdi Veri Tipleri	79
9.1.7.1.2	Saf Bayes Sınıflandırıcı İçin Çıkan Değerler	79
10	SONUÇ ve ÖNERİLER	90
10.1	Tez Çalışmasının Özeti	90
10.2	Çalışmanın Getirileri, Sağladığı Katkılar	90
10.3	Gelecekte Yapılabilecekler	90
10.4	Sonuç	91
11	KAYNAKLAR	92

KISALTMALAR

VM : Veri Madenciliđi
MÇS : Veri Madenciliđi Çekirdek Sistemi
VTBK : Veri Tabanı Bilgi Keşfi
VTYS : Veri Tabanı Yönetim Sistemleri
MÖ : Makine Öğrenimi
EFT : Electronic Fund Transfer
HB : Hazine Bonosu
DT : Devlet Tahvili
EB : Euro Bond
ATM : Automated Teller Machine
IT : Information Technologies
BK : BİLGİ KEŞFİ
VT : Veri Tabanı
TCK : Türk Ceza Kanunu

1 GİRİŞ

1.1 Problemin Tanımı

Bilgi ekonomisinin hızla yaygınlaşması ve bilginin geleceğin anahtarı konumuna yükselmesi, artan globalleşme eğilimleriyle birlikte rekabet olgusunu yaşamın her alanına taşımıştır. Özellikle sanayi toplumundan bilgi toplumuna dönüşümün çok hızlı gerçekleşmesinin temel nedeni, yeni teknolojilerin gelişme hızı ve bilgiye verilen önemin artmasından kaynaklanmaktadır.

Bunun nedeni, bir tarafta bilişim teknolojisindeki olağanüstü gelişmeler, diğer tarafta ise geçmişte sırayla birinci derecede önemli şirket varlığı sayılan insan gücü, makine gücü veya finans gücünün yerini günümüzde artık bilginin gücünün almış olmasıdır. Bu çerçevede bilgi yönetimi ve gerekli teknolojik araçlar büyük önem taşımaya başlamışlardır.

Teknolojinin yoğun olarak yaşandığı finans sektöründe, özellikle 1990'lı yıllardan sonra büyük değişimler yaşanmıştır. Sermaye piyasası da bu değişimlerden etkilenmiştir. İnternet üzerinden sermaye piyasası işlemlerinin 1994 yılının sonlarında başlamasına rağmen, tahmin edilenden daha büyük bir büyüme hızı göstermiş ve günümüzde, sermaye piyasası işlemlerinin önemli bir kısmı internet üzerinden yapılı hale gelmiştir.

Bununla birlikte internet üzerinden yapılan işlemlerin, borsalara, aracı kurumlara, yatırımcılara ve hatta ülke ekonomisine sağladığı yararlar bulunmaktadır. Öncelikle, çevrimiçi işlemler, işlem hacmini arttırmış ve işlem maliyetlerini düşürmüştür. Çevrimiçi işlemin üstünlükleri, birçok yatırımcıyı özellikle, küçük yatırımcıyı sermaye piyasasına çekmiştir. Çevrimiçi işlemler, ülkeler ve ülkelerin sermaye piyasaları arasındaki sınırları ortadan kaldırmış, uluslararası yatırımların ve borsa birleşmelerinin önünü açmıştır.

İnternet üzerinden yapılan işlemlerin artması beraberinde bir çok sorunu da getirmiştir. Bunlardan finans sektörünü en çok baltalayan internet üzerinden dolandırıcılık işlemleridir. Dolandırıcılık yapan kişiler öncelikle kişinin internet bankacılığı şifresini belli yöntemlerle ele geçirip o kişiyi gibi parasal işlemler gerçekleştirmektedir. Bunun yıllık maliyeti milyon dolarlar ile ifade edilmektedir.

İnternet gibi teknolojik gelişmeler dolandırıcılık işlemlerini daha da kolay hale getirmiştir. Suçlulara daha az cezanın verilmesi ve toplumda bu gibi kişilere kötü gözle bakılmaması sorunun artmasında etkili olmuştur.

Dolandırıcılık tespiti esnasında veri madenciliği için bazı teknik ve pratik problemler ortaya çıkmaktadır. En önemli teknik problem sınırlandırma ve zayıf özellikli verilerdir. Genelde veriler başka programlardan toplanmaktadır. Veri madenciliği için özellikle tasarlanmamışlardır. Bunun için veri madenciliğinin ihtiyaç duyduğu verileri bazen karşılamamaktadır.

Tez kapsamında İnternet Bankacılığı hakkında genel bir bilgi ve orada yapılacak işlemler detaylı bir şekilde anlatılacaktır. Bu işlemlerden sonra İnternet Bankacılığının güvenlik unsurları

ve dolandırıcı kişilerin müşteri numarası ile şifreleri nasıl elde ettikleri hakkında bilgiler verilecektir. Daha sonra dolandırıcılığın tanımı ve bilişim dolandırıcılığı anlatılacaktır. Bu bilgilerden sonra dolandırıcılık tespit sisteminde kullanılacak İnternet Bankacılığı verileri ve veri madenciliği metotları detaylı bir şekilde anlatılacaktır. Bu genel bilgilerden sonra asıl olan Dolandırıcılık Tespit Sisteminin çalışması anlatılıp, elde bulunan verilere uygulanacaktır. Bu uygulamadan sonra oluşan sonuçlar incelenecektir.

Her yıl binlerce kişi dolandırıcılık yüzünden bir çok maddi ve manevi zarar görmektedir. Tezde İnternet Bankacılığında yapılan dolandırıcılık işlemlerinin tespitini sağlayan yapı anlatılacaktır. Bu yapı ile İnternet Bankacılığında yapılan her türlü parasal işlem incelemeye alınıp, işlemin yasal ve suçlu olarak sınıflandırılması sağlanacaktır.

1.2 Amaç

Bu tez çalışmasında İnternet Bankacılığını kullanan müşterilerin şifrelerinin bir başkası tarafından kullanılması halinde bile onların maddi ve manevi yönden zarar görmelerini önleyici bir dolandırıcılık tespit sistemi geliştirilmiştir.

Bu sistemde müşterinin daha önceki işlemlerine bakılarak o müşteriye özel bir yapı oluşturulmuştur. Daha sonra onun yaptığı işlemlerde o müşteri olup olmadığı belirlenerek gerekli tedbirler alınmıştır. Bu sistemdeki asıl amaç her bir müşteri için müşteri modeli tanımlayıp müşterileri modellere atamaktır. Her suçlu mutlaka bir delil bırakır sözü ile hareket edilirse dolandırıcı yaptığı işlemlerle gerçek müşteri gibi davranmayacaktır, böylece yapılan işlemin gerçek müşteriye ait olmadığı belirlenerek yapılan işlem iptal edilebilecektir.

Müşteri gruplarının belirlenmesi bu gruplardan özel desenlerin oluşturulması için C4.5 ve Saf Bayes Sınıflandırıcıları kullanılmıştır.

2 LİTERATÜR ARAŞTIRMASI

(Von Altrock,1995) Optimum eşik değerini kullanan dolandırıcılık hesaplama poliçesini içeren Bulanık Mantık Sistemi kullanmıştır. Çıkışlar, dolandırıcı olabilme ihtimalini göstermiştir ve sahte olanların nedenleri ile açıklamıştır. 1200 adet sigorta işlemine uygulanıp , tecrübeli denetçiden daha iyi tahminde bulunan bir sistem geliştirilmiştir.

(Cox ,1995) İki farklı yaklaşma kullanan bulanık mantık sistemi ; keşfedici model ve bulanık farklı-sorgulama modelini araştırmıştır. Veri içerisindeki doğal bağlantıları öğrenmek ve önemli kümelemeleri oluşturmak için birincil model denetimsiz sinir ağları kullanmıştır. Neuro-Fuzzy sınıflandırma sistemi kümelerdeki desenleri tanımlamış, ikincisi bulanık model üretmek için Wang-Mendel Algoritması kullanmıştır.

(Maes at al ,2002) Bayes Ağlarında ve Yapay Sinir Ağlarında çeşitli karşılaştırmalar yapmıştır. Bu karşılaştırma sonucuna göre Bayes Ağlarının daha hızlı ve daha doğru eğitildiğini ama yeni örneklere uygulandığında yavaş olduğunu belirlemiştir. Yapay Sinir Ağlarının ,Bayes Ağlarının tam aksine daha zor eğitildiğini, ama yeni örneklerde güzel sonuçlar verdiğini bulmuştur. Bankacılıkta da bu sistem etkili bir şekilde kullanılabilir.

(Chan et al ,1999) Sonuçta oluşan geniş veri kümelerini, sınıflandırma yapabilmek için küçük alt kümelerine ayırmıştır. Burada farklı algoritmalar kullanmıştır, yasal/suçlu eğitim örnekleri ile eğitmiş ve maliyetin azalması açısından birleştirilmiş çoklu model oluşturmak için stacking yapmıştır.

(Weatherfor,2002) Advanced Security for Personal Communications Technologies(ASPECT) araştırma grubu yapay sinir ağları ve tamamen denetimsiz öğrenme ile şimdiki ve geçmişe ait kullanıcı bilgilerini içeren kullanıcı profillerini eğitmiştir. Bu eğitimden sonra eğer şimdiki kullanıcı profili ile geçmiş arasında çok fazla fark varsa dolandırıcı olma ihtimali vardır sonucunu çıkarmıştır.

(Cahill et al,2002) Adapte Dolandırıcılık Tespit Sistemini geliştirmiştir. Dolandırıcılık olduğunu bulmak için dolandırıcılık puanı atamıştır. Geniş veritabanlarında çeşitli dolandırıcılık tiplerini bulmak için kurallar kullanmıştır. Bu sistem telsiz ve kablolu sistemleri kullanan 2 milyondan fazla müşteriler üzerinde uygulanmıştır. Adapte Dolandırıcılık Sistemi her bir kullanıcıya has özellikte kural tabanını otomatik olarak oluşturmuştur.

(Andreas L. Prodromidis ve Salvatore Stolfo,1999)Tümevarımsal öğrenme ve sınıflandırma teknikleri birçok problemlerde uygulanılır. Bu araştırmada tümevarımsal öğrenme ve meta-öğrenme metotlarını birleştirerek dolandırıcılığı tespit eden bir sistem yapılmıştır. Tümevarımsal öğrenme algoritması dağıtık data kümeleri içerisinde alışılmışın dışındaki verileri saptamak için kullanılır ve meta öğrenme metotları toplu bilgilerini daha yüksek sınıflandırma modellerinde veya meta-sınıflandırıcıda birleştirir. Değiş tokuş veya verilerdeki sınıflandırıcı vekillerini destekleyerek, finans sektöründe dolandırıcıdan korunma mekanizmasını gerçekleştirmiştir.

(R. Brause, T. Langsdorf, M. Hepp,1999) Kredi kartı dolandırıcılığını öğrenme, tahmin etme teknikleri için önemli bir uygulamadır. Yapay sinir ağları kullanmadaki en büyük engel ; bin adet işlemden yalnızca biri geçersizdir ve de %99.9 tahmin yeteneğine sahip bir kabul edilebilirlik yoktur. Burada veri madenciliği teknikleri ve yapay sinir ağları düşük hatalı alarm verecek şekilde birleştirilmiştir. Yapay sinir ağları ile eğitim çok etkili olmasına rağmen, eğitim süresinin uzun sürmesinden dolayı bu yöntem tez de kullanılmamıştır.

(Eric Altendorf, Peter Brende, Josh Daniel, Laurent Lessard,2005)Çevrimiçi alışverişlerde gittikçe yaygınlaşmakta ve bununla birlikte dolandırıcılıkta önemli biçimde artmaktadır. Şuan ki dolandırıcılığı engelleyici teknikler ise kara listeler, kurallar ve kişisel deneyimlerdir. Bunlar güzel sonuç elde etmesine rağmen yine de birçok dolandırıcılık işlemi devam etmektedir ve insan uzmanlara güvenmek zorunda bırakılmaktadır. Buradaki amaç dolandırıcılık tespitinin özelliklerini artırmak ve insana olan gereksinimi azaltmaktır. Bunun için sınıflandırıcılar kullanılmıştır. Böylece insana olan gereksinim belli miktar azaltılmıştır.

(Philip K. Chan,Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo,1999)Kredi Kartı işlemleri gittikçe artmakta ve bunun sonucunda hırsızlık, dolandırıcılıkta artmaktadır.Bundan dolayı bankalar sahtecilik için erken uyarı sistemleri kurmaktadırlar. Alışveriş sistemlerinde muazzam işlem yapılmakta ve bu bilgilerin üzerinde sahtecilik araştırması olurken zaman da önemli bir problem olarak karşımıza çıkmaktadır. Önerilen birleşmiş çoklu öğrenmiş sahtecilik araştırmacıları metotları genel ve kullanışlıdır. Deneysel sonuçlara bakıldığında sahtecilik modellerinin dağıtık veri madenciliğinde kullanıldığında dolandırıcılık azalmıştır.

(John Hogden ,1997)Maximum Likelihood Continuity Mapping(MALCOM) yeni zaman-serisi analiz tekniğidir. Uygulama olarak ta sağlık sigortası ödeme poliçesi üzerinde sahtecilik araştırmasıdır. Verilen eğitim veri kümeleri karıştırılmış tipik sıralıdır, MALCOM , Continuity Map adı verilen sıralı nesil modeli üretir. CM, eğitim örneklerinde verilen model sabitlerinde sıranın muhtemelliğini maksimum yapar. CM eğitim kümesi içinde bulunmayan sırasal verilerin olasılığını hesaplayabilir. Anormal arama ve sıra tahmininde kullanılır. MALCOM kategorik veri sıralarında kullanır, ve de veri tabanı arama araçları için potansiyel yerleşime sahiptir. MALCOM hastaların tıbbi tarihlerinin olasılığında kullanılırdı. Tıbbi Tarih hastaların yapmış olduğu işlemleri belirtmektedir. MALCOM doktorların(12 tane doktorun) hastaları üzerinde denenip iyi sonuçlar alınmıştır.

3 İNTERNET BANKACILIĞI

İnternet Bankacılığı, müşterilerin banka şubelerinden yapabileceği bankacılık işlemlerinin pek çoğunu istenilen yerde ve zamanda yapmalarını sağlayan bir sistemdir. İnternet erişimi olan herhangi bir kullanıcı, bilgisayar aracılığıyla bankacılık işlemlerini gerçekleştirebilir. Bu şekilde şubeye gitmeye gerek kalmadan bankacılık işlemleri yapılmış olur.

Teknolojinin yardımıyla en hızlı gelişen ve hizmet sunumunu çeşitlendiren sektörlerden biri de bankacılık ve finans sektörüdür. İnternetin getirdiği olanakları da bu gelişme doğrultusunda etkili bir araç olarak kullanan neredeyse tüm bankalar, hem İnternet bankacılığı hizmetlerinde servis alanını yaygınlaştırmakta hem de müşterilerini İnternet Bankacılığını kullanma konusunda teşvik etmektedir.

İş yaşamında zaman faktörünün çok değerli olduğu herkesin ortak fikridir, firmaların faaliyetlerinin devamı için vazgeçilmez bir unsur olan bankacılık hizmetleri, ayrı bir mesai yaratmayı zorunlu kılmaktadır. Hem zaman kaybını önlemek hem de İnternet olanağı olan her yerden günün her saati finansal işlemleri gerçekleştirebilmek firmalar için büyük bir olanaktır. Bunun farkında olan bankacılık sektörü, sadece bireysel müşterileri için değil, kurumsal müşterilerine yönelik kurumsal İnternet Bankacılığı hizmetlerini de genişletmektedir.

Şube bankacılığının aksine İnternet Bankacılığında, zaman ve mekandan bağımsız işlem yapabilme avantajı büyük kolaylık sağlamaktadır. EFT, havale, kredi ödeme, döviz, borsa, fon gibi yatırım araçlarını kullanabilme, vergi, fatura ödemelerini yapabilme konularında şubeye bağımlılığı ortadan kaldırmaktadır. Güvenlik açısından oldukça etkili bir sistem olan SSL güvenlik ve şifreleme protokolünün uygulandığı İnternet Bankacılığının, güvenlik altyapısı anlamında şube bankacılığından pek bir farkı bulunmamaktadır.

Yılın 365 günü ve 24 saat kesintisiz hizmet vermesi de, mesai sınırlaması olan şube bankacılığına göre ayrı bir üstünlüktür. Bunun yanında bankaların bireysel ya da kurumsal müşterilerine sunduğu İnternet Bankacılığı hizmetleri, banka politikalarına göre değişen ek kolaylık ve avantajlarla cazibesini gittikçe artırmaktadır. Örneğin ücretsiz havale ve EFT olanakları, e-mail yoluyla ücretsiz portföy bildirimleri, İnternet şubesi kullananlara yönelik kampanya ve puan hediyeleri vs. gibi avantajlar bunlardan bazılarıdır.

3.1 İnternet Bankacılığında Yapılabilecek İşlemler

Bu kısımda müşterinin İnternet Bankacılığında yapabileceği işlemler detaylı şekilde anlatılmıştır. Tez kapsamında İnternet Bankacılığı kullanılarak yapılan işlemler Dolandırıcılık Tespit Sistemine girdi olarak verilip belli sonuçlar elde edilmiştir.

3.1.1 Hesaplar

3.1.1.1 Varlıklar

Varlıklar sayfasından vadesiz, vadeli ve yatırım hesaplarınızın o an itibariyle bakiyelerini ve kullanılabilir YTL ve döviz bakiyelerini, kredinizin tutarını ve kalan borcunuzu ve tanımlı olan kredi kartlarınızı görüntüleyebilirsiniz. Ayrıca vadesiz hesaplarınızın IBAN bilgilerini de görüntüleyebilirsiniz. IBAN ülke ,banka, şube ve hesap bilgisini içeren tek bir koddur. Varlıklar 5 alt gruptan oluşmaktadır:

1. Grupta vadesiz YTL ve döviz hesaplarınızı, bakiyelerini ve kullanılabilir bakiyelerini, IBAN bilginizi
2. Grupta vadeli YTL ve döviz hesaplarınızı ve bakiyelerini,
3. Grupta yatırım hesaplarınızı, bakiyelerini ve kullanılabilir bakiyelerini,
4. Grupta bireysel kredi hesaplarınızı, kredi tutarlarını ve kalan borç tutarlarını,
5. Grupta kredi kartlarınızı görüntüleyebilirsiniz.

Ürün tanımı yukarıdaki gruplara girdiği halde görülmeyen hesap veya kartlarınızı tanımlatmak için, bankanıza ait telefonları arayabilir veya şubenize başvurabilirsiniz.

3.1.1.2 Hesap Hareketleri

Vadesiz YTL ve döviz hesaplarınızı ve yatırım hesaplarınızın hareketlerini 1'er aylık periodlar halinde en fazla 6 ay geçmişe kadar inceleyebilirsiniz.

3.1.1.3 Yatırım Hesapları

Yatırım hesaplarınızın, anlık olarak nakit durumunu, menkul durumunu ve toplam portföy değerlerini görüntüleyebilirsiniz.

Şubelerden talimat verdiğiniz takdirde, sizin belirleyeceğiniz tutar kalmak kaydı ile vadesiz hesabınızda bıraktığınız 250 YTL üzerindeki paranız, saat 15:00 itibariyle otomatik şekilde repo olarak değerlendirilmektedir.

Repo yapılan mevduatınızı, repo dönüş tarihinizde 07:00 itibariyle kullanabilirsiniz.

3.1.1.4 Kredi Hesapları

Bireysel kredilerinizin ödeme planını, alınan ve kalan borç tutarınızı görüntüleyebilirsiniz.

3.1.1.5 İnternet İşlemleri

Seçtiğiniz tarih aralığında yaptığınız tüm parasal işlemleri görüntüleyebilir, dekontunu alabilirsiniz.

3.1.1.6 Özel Hesap İşlemleri

3.1.1.6.1 Özel Hesap Tanımlama

Özel Hesabınızın otomatik B tipi likit fon alıŖ satıŖ özelliğini aktif hale getirmek için Özel Hesap ile Özel Yatırım hesabınızı ilişkilendirmeniz gerekmektedir. Bu adımda ilk olarak kredili mevduat (Özel Hesap) hesabınızı, ikinci olarak Özel Yatırım hesabınızı seçmeniz istenecektir. Vadesizde hesapta kalacak alt bakiyeyi belirledikten sonra devam tuşuna basarak, otomatik B tipi likit fon alıŖ/satıŖı aktifleştirmiş olacaksınız.

Otomatik (fatura, kredi kartı, vb.) ve düzenli ödemeleriniz sırasıyla önce hesaptaki bakiyenizden, bakiyeniz yetersiz ve yatırım fon bakiyesiniz varsa fonunuzu bozarak, ikisi de yetersizse kredili mevduat hesabınızdan gerçekleştirilir.

Özel Hesap'ta minimum 100 YTL bırakmanız gerekmektedir. Bu tutar istenirse gün içerisinde kullanılabilir. Ancak, saat 01:00'de ve 18:30'da fon bozulma saati geldiğinde, minimum 100 YTL veya belirlediğiniz tutar kadar vadesiz bakiye kalacak şekilde fon bozumu gerçekleştirilecektir. Özel Hesabınızdaki mevcut kredi limitinizden kullandığımız takdirde, mevcut kredinizi kapatmadan Özel Hesap deęişiklięi yapılamayacaktır.

3.1.1.6.2 Günlük Ödeme Bilgileriniz

Günlük ödeme bilgilerinizin görüntüledięi adımdır. Sistem tarafından gün içinde 2 defa otomatik fon alım/satım işlemi yapılacaktır. Saat 01:00'de sizin belirlediğiniz minimum tutar vadesiz hesapta kalacak şekilde fon alım/satımı gerçekleştirilecek olup, hesabınızdan verdiğiniz talimatlardan sırasıyla havale, EFT ve düzenli ödemeleriniz yapılacaktır. Saat 18:30'dan sonra da yine sizin belirlediğiniz minimum tutar vadesiz hesapta kalacak şekilde fon alım/satımı gerçekleştirilecek ve otomatik ödemeleriniz yapılacaktır. Sizin vermiş olduğunuz otomatik ödeme ve düzenli ödeme talimatları zamanında hesap bakiyeniz yeterli deęilse ve yatırım fonunuz varsa otomatik olarak fon bozarak, her ikisi de yeterli deęilse kredili mevduat hesabınızdan ödeme gerçekleştirilir.

Özel Hesap bir YTL hesabı olacaęından, yabancı para talimatlar için otomatik fon satılmayacaktır. Örneğin USD havale gibi.

Özel Hesap kapsamında EFT ve havale talimatlarınızın gerçekleştirilebilmesi için en geç saat 00:00'a kadar talimat girişinizi yapmanız gerekmektedir. Gün içinde gerçekleşmiş olan talimatlarınız Günlük Ödeme Bilgileriniz adımında gözükmeyecektir. Gerçekleşen talimatlarınızı hesap hareketlerinden takip edebilir.

3.1.1.6.3 Özel Hesap Görüntüleme/Güncelleme

Özel Hesapta otomatik fon alım/satımını bu adımdan açıp/kapatılabilir, vadesizde bırakmak istediğiniz alt limiti değiştirebilirsiniz.

3.1.1.6.4 Özel Hesap Günlük İşlem Bilgileriniz

Özel Hesap dahilinde verdiğiniz talimatlarınızı ve bunların doğrultusunda otomatik gerçekleştirilmiş fon alım/satışlarınızı istediğiniz tarih aralığında görüntüleyebilir, ödemelerinizle ilgili tüm detaylara ulaşabilirsiniz.

3.1.1.7 Karta Hesap Bağlama

Debit ve kredi kartınıza vadesiz hesap ekleme ve çıkarma işlemlerini yapabilirsiniz. Debit kartınıza en fazla 4 tane, kredi kartınıza en fazla 3 tane vadesiz hesap bağlayabilir, dilediğiniz hesabı çıkarabilirsiniz. Her iki kartınıza bağlı hesaplarınızdan 1 tanesi ana hesap olmak zorundadır ve ana hesabınız silinemez.

3.1.1.8 Hesap Açılışı

Bankanızın istediğiniz şubesinde, istediğiniz para biriminde vadesiz hesap veya Özel Hesap (0 limitli kredili mevduat hesabı) açılışı gerçekleştirebilirsiniz.

Açtırmak istediğiniz hesabın tipini, para birimini, ilini ve hangi şubede açılmasını istediğinizi seçerek işleminizi gerçekleştirebilirsiniz. Özel Hesap özelliklerinden biri olan kredili mevduat hesabı olma özelliği ilk hesap açılışında kapalı olup, kullanılabilmesi için gerekli belgeler ile hesabın açıldığı şubeye başvurmanız gerekmektedir. Vadesiz hesap açılışı ekranlarını kullanarak dilediğiniz kadar hesap açabilirsiniz.

3.1.1.9 Portföy

Portföy Raporu adımımdan vadeli ve vadesiz hesaplarınızın o an itibarıyla durumunu öğrenebilir ve bakiyelerini, kullanılabilir YTL, USD veya EURO bakiyeleri olarak görebilirsiniz. Ayrıca sahip olduğunuz yatırım araçlarının durumunu ve size olan getirisinin ne kadar olduğunu para birimi ve yüzde olarak takibini yapabilirsiniz.

Varlıklar sayfası 5 ana gruptan oluşmaktadır:

1. Grupta Vadesiz YTL, Vadesiz Döviz ve Özel Hesaplarınız.
2. Grupta Vadeli YTL ve Vadeli Döviz hesaplarınızı ve her iki grubun altında da toplam kullanılabilir bakiyeleri .
3. Grupta yapmış olduğunuz repolar ve vade sonunda size getirisi.
4. Grupta almış olduğunuz fon çeşitleri ve bu gün itibarıyla size kazancı.
5. Grupta hazine bonusu,devlet tahvili ve eurobondlarınızın bakiyelerini görüntüleyebilirsiniz.

Vadesiz hesaplarınızda; hesaplarınızın sadece vadesiz bakiyeleri gösterilmiştir. Portföy raporunda "bakiye" sütunu dikkate alınmıştır. YTL bakiye ve YTL kullanılabilir bakiye alanları, bankanızın güncel alış-satış kuru ortalaması alınarak hesaplanmaktadır.

Vadeli hesaplarınızda; hesaplarınızın vade sonundaki tutarı baz alınarak hesaplamalar yapılmıştır. Vade sonu potansiyel YTL tutar alanı, bankanızın güncel alış-satış kuru ortalaması alınarak hesaplanmaktadır. Sadece İnternet Şubesinde görüntülediğiniz hesaplarınız baz alınmıştır.

Repo hesaplarınızda; hesaplarınızın vade sonundaki tutarı baz alınarak hesaplanır. Sadece İnternet Şubesinde görüntülediğiniz hesaplarınız baz alınmıştır.

Fon hesaplarınızda; sadece İnternet Şubesinde görüntülediğiniz hesaplarınız baz alınmıştır.

HB/DT/EB Hesaplarınızda; hesaplarınızın vade sonundaki tutarı baz alınarak hesaplanır. Sadece İnternet Şubesinde görüntülediğiniz hesaplarınız baz alınmıştır. YTL Genel Toplam alanı, internet şubesinin güncel alış-satış kuru ortalaması dikkate alınarak hesaplanmaktadır.

3.1.2 Çek ve Senet İzleme

3.1.2.1 Tahsil Teminat Çekleri

Teminata/Tahsilata verilen onaylanmış, tahsil edilmiş veya iade olmuş çeklerinizi gözlemleyebilirsiniz.

3.1.2.2 Senetler

Teminata/Tahsilata verilen onaylanmış ödenmiş, protestolu, iade veya bekleyen senetlerinizi gözlemleyebilirsiniz.

3.1.2.3 Çek Karnesi

Bankanız tarafından verilen her türlü çeklerinizi gözlemleyebilirsiniz.

3.1.3 Döviz İşlemleri

3.1.3.1 Döviz Alış

Bankanızdaki vadesiz YTL ve döviz hesaplarınızın bakiyelerini, kullanılabilir bakiyelerini görüntüleyebilir ve döviz alabilirsiniz.

Döviz alış yapabilmek için tutarın çekileceği vadesiz YTL hesabınızın bakiyesi yeterli olmalıdır.

3.1.3.2 Döviz Satış

Bankanızdaki vadesiz YTL ve döviz hesaplarınızın bakiyelerini, kullanılabilir bakiyelerini görüntüleyebilir ve dövizinizi satabilirsiniz.

Döviz satışı yapabilmek için tutarın çekileceği vadesiz döviz hesabınızın bakiyesi yeterli olmalıdır.

3.1.4 Kredi Kartları

3.1.4.1 İzleme

Bankanızdan aldığımız kredi kartlarınızın dönem içi hareketlerini, gelecek dönem taksitlerinizi, kart bilgilerinizi, limit bilgilerinizi ve ekstrenizi görüntüleyebilirsiniz.

3.1.4.2 Borç Ödeme

Bankanızdaki vadesiz YTL ve döviz hesaplarınızdan istediğiniz hesabı seçerek, İnternet Bankacılığında tanımlı kredi kartınızın borcunu ödeyebilirsiniz.

3.1.4.3 Kart No ile Borç Ödeme

Bankanızdaki vadesiz YTL ve döviz hesaplarınızdan istediğiniz hesabı seçerek, herhangi bir banka kredi Kartının borcunu ödeyebilirsiniz.

3.1.4.4 Nakit Avans

Bankanız Kredi Kartınızdan Bankanızdaki vadesiz YTL hesabınıza para aktarabilir ve acil nakit sıkışıklığınızı giderebilirsiniz.

3.1.4.5 Ekstre Talimatı

Kredi kartınızın ekstresinin istediğiniz bir e-mail adresine ve posta yoluyla iş adresinize ya da ev adresinize gönderilmesini isteyebilirsiniz.

3.1.4.6 Otomatik Ödeme Talimatı

Kartınızın veya başka bir kişiye ait Kartın YTL ve USD bazında borç ödemelerini otomatiğe bağlayabilirsiniz.

Otomatik ödeme talimatları, kredi kartı borcunuzun son ödeme tarihinde seçtiğiniz vadesiz hesabınızda yeterli bakiye olması durumunda gerçekleştirilir. Kendi kartınız ve otomatik ödeme talimatı verdiğiniz diğer kartların ödemeleri belirli bir sıra olmaksızın tahsil edilmektedir. Sizin ve talimat verdiğiniz diğer kartların ödeme tarihinin aynı olması durumunda, hesabınızda yeterli bakiye olmalıdır. Borcunuzun son ödeme tarihinde saat 19:00'a kadar verdiğiniz talimatlar, mevcut ekstre döneminizi de kapsamaktadır.

3.1.4.7 Şifre Alma / Değiştirme

İşlem yapmak istediğiniz kredi kartınızı seçtikten sonra, kartınıza ilk defa şifre belirlemek için "ilk şifre", kart şifrenizi değiştirmek için "şifre değiştir" kısmı kullanılır.

İlk defa şifre belirlemek için 4 haneli şifrenizi "yeni şifreniz" ve "yeni şifreniz tekrar" alanlarına yazınız

Mevcut şifrenizi değiştirmek için "eski şifreniz" alanına kullanmakta olduğunuz şifreyi, "yeni şifreniz" ve "yeni şifreniz tekrar" alanlarına da almak istediğiniz şifreyi yazınız.

Şifrenizi, doğum tarihiniz ve kolay tahmin edilecek ardışık sayılardan oluşturmamaya dikkat ediniz.

Şifrenizi unuttuysanız banka telefon yetkilisini arayarak şifrenizi oluşturabilirsiniz

3.1.4.8 Telefonla Uyarı

Seçtiğiniz kredi kartınızı internet işlemlerinde kullanabilmek amacıyla telefonla uyarı işlemlerine açabilir ve kapatabilirsiniz. Bu işlemler sırasında kartınızın telefonla uyarı için açmak istediğiniz limiti YTL ve USD bazında belirleyebilir, tarih aralığı ile sınırlandırabilirsiniz. Karşılaşacağınız herhangi bir sorun hakkında banka telefon yetkilisini arayarak banka telefon yetkilisinden yardım alabilirsiniz.

3.1.4.9 Kart Başvurusu

Bankanızdan aldığınız kredi kartlarınız için ek kart başvurusunda bulunabilirsiniz. Ek kart bağlamak istediğiniz kredi kartınızı seçip ek kart sahibinin bilgilerini girerek asıl kart limitinin ne kadarının ek kart hamili tarafından kullanılacağı belirlenir. Ek kartınız iş veya ev adresinize gönderilir.

3.1.4.10 Görüntüleme/Güncelleme

Kişisel bilgilerinizi, ev ve iş adres bilgilerinizi, iletişim bilgilerinizi görüntüleyebilir ve bu bilgilerinizde değişiklik varsa güncelleyebilirsiniz.

Kişisel bilgilerinizde bazı alanlar, aynı zamanda güvenlik sorusu olarak sorulan bilgiler olduğundan değiştirilemez. Bu alanlardaki değişiklikleriniz için banka telefon yetkilisini arayabilir ya da şubeniz ile irtibata geçebilirsiniz.

3.1.4.11 İşlem ve Saat Limitleri

İnternet Bankacılığını kullanarak yapabileceğiniz işlemler için alt ve üst limitleri, günlük toplam ve kalan limitinizi, işlem saatlerini ve bu işlemlerin anlık yapılabilirlik durumunu görüntüleyebilirsiniz.

3.1.5 Tanımlamalar

3.1.5.1 Parola Deęiřtirme

İnternet Bankacılıęına giriřte kullandığınız parolanızı deęiřtirebilirsiniz. Parolanız en az 6, en fazla 8 karakterden oluřmalı, rakam ve harfleri birlikte içermeli (örneęin; tez2007) ve Türkçe karakter(ö,ř,ę,ı,ü,ç) içermemelidir.

3.1.5.2 Şifre Deęiřtirme

İnternet Bankacılıęına giriřte kullandığınız şifrenizi deęiřtirebilirsiniz. Şifreniz 6 rakamdan oluřmalı, ardışık rakamlardan veya aynı rakamlardan oluřmamalı (örneęin; 234567 veya 333333) ve müşteri numaranızdan farklı olmalıdır.

3.1.5.3 Güvenlik Ayarları

3.1.5.3.1 Zaman Ayarları

Bu seçenekte İnternet Bankacılıęının güvenlięini arttırmak amacı ile İnternet Bankacılıęını kullanmak istediğiniz gün ve saat aralıęının seçimini yaparak seçim yapmış olduęunuz gün ve saatler haricinde İnternet Bankacılıęı kullanımını engellemiş olacaksınız.

3.1.5.3.2 IP Aralık Belirleme

Bu güvenlik adımını kullanarak İnternet Bankacılıęına sadece sizin belirlediğiniz üç farklı IP aralıęından girilebilmesini saęlayabilirsiniz.

3.1.5.3.3 Tatil Tanımlama

Bu seçenekte İnternet Bankacılıęını kullanmayacaęınız tarih aralıęını seçerek iki tarih arasında İnternet Bankacılıęı giriřini engelleyebilirsiniz.

3.1.5.3.4 Para Transferini Kapama/Kısıtlama

Bu adımda İnternet Bankacılıęını kullanarak yapılacak Havale/EFT ve Swift işlemlerine kısıtlama getirebilir ve günlük işlem limitlerinizi tanımlayabilirsiniz. Limitleri “0” olarak belirlemeniz durumunda ise İnternet Bankacılıęı ile yapılan tüm para transferi işlemlerini kapatabilmeniz mümkündür.

3.1.5.3.5 Para Transferi Uyarısı Tanımlama

Bu seçeneęi kullanarak İnternet Bankacılıęında sizin belirlemiş olduęunuz işlemler ve limitlerin üstünde bir para çıkışı olması durumunda e-mail adresinize uyarı maili gelmesini saęlayabilirsiniz.

3.1.5.3.6 Hesap ayarları

Bu seçenek ile İnternet Şubesinde görüntülenmesini istemediğiniz hesaplarınızı belirleyebilirsiniz.

3.1.5.3.7 Güvenlik Sorusu

İnternet Bankacılığında yaptığımız işlemlerin daha güvenli ortamda gerçekleşmesi için sizin tarafınızdan belirlenecek olan onay kelimesidir. İnternet Bankacılığında para çıkışı gerektiren işlemlerde, güvenlik tanımlamalarınızı veya kişisel bilgilerinizi değiştirmek istediğinizde sizden bu soruyu yanıtlamanız istenir.

3.1.5.3.8 Güvenlik Sorusu Değiştirme

Güvenlik ayarları menüsüne kendi belirlemiş olduğunuz güvenlik sorusu ile giriş yapıp isterseniz soruyu değiştirmeniz mümkündür.

3.1.5.3.9 Durum İzleme

İnternet Bankacılığında yaptığımız kişisel güvenlik ayarlarını görüntüleyebileceğiniz adımdır.

3.1.5.4 Telefon Bankacılığı Şifre Değiştirme

Telefon bankacılığınızı kullanıma açabilir ya da kapatabilir, şifre belirleyebilirsiniz. Telefon bankacılığını kapalı statüsüne getirdiğinizde telefon bankacılığı şifreniz silinecektir. Tekrar kullanabilmek için statünüzü açık hale getirmeniz ve şifre belirlemeniz gerekmektedir.

3.1.5.5 Hesap Rumuzu Tanımlama

Bankanızda bulunan vadesiz YTL ve döviz hesaplarınıza birer rumuz vererek isimlendirebilirsiniz (örneğin: maaş hesabım, fatura hesabım). Bu özellik fazla hesabı olan ve bu hesaplarını kullanarak sık işlem yapan müşterilerimiz için hesaplarını isimlendirerek, rahat görüntülenmesini sağlar.

3.1.5.6 Renk Seçimi

Bu menü altında verilen renk gruplarından seçiminizi yaparak İnternet Bankacılığını istediğiniz renklerle kullanabilirsiniz.

3.1.5.7 Şifre Üretici İşlemleri

3.1.5.7.1 Şifre Üreticisini Kullanıma Açma

Kurye ile tarafınıza ulaştırılan şifre üreticini kullanabilmek için aktifleştirmeniz gerekmektedir. Aktivasyon işleminizi banka telefon yetkilisini arayarak gerçekleştirebilirsiniz.

3.1.5.7.2 Şifre Üreticisini Kullanarak İnternet Bankacılığına Giriş

Şifre üreticisini aktif hale getirdikten sonra İnternet Bankacılığı girişlerinizde şifre üreticinizin ürettiği şifreleri kullanmaya başlayabilirsiniz. İnternet Bankacılığına girişlerde, sizden öncelikle müşteri numaranız, parolanız ve İnternet Bankacılığına girişte daha önceden kullanmakta olduğunuz şifreniz istenecektir. Bu bilgileri doğru girdikten sonra sizden istenen, Şifre üreticiniz yazan bölüme şifre üreticinizin o anda ürettiği 6 haneli şifreyi girmenizdir. Bu şifre olmadan İnternet Bankacılığına girmeniz mümkün olmayacaktır.

Şifre üreticinizi aktifleştirdikten sonra, İnternet Şubesi işlemlerinizi için tanımladığınız güvenlik sorusunun yerine şifre üreticinizde üretilen şifreyi kullanmanız gerekmektedir. Ancak şifre üreticiniz tek kullanımlık şifreler ürettiği için, gerek İnternet Bankacılığı girişinde gerekse güvenlik teyidi gerektiren alanlarda ikinci kez aynı şifre kullanılamayacaktır. Bu yüzden yeni üretilen şifrenin beklenmesi ve ondan sonra kullanılması gerekecektir.

3.1.5.7.3 Şifre Üreticinin Ürettiği Şifrenin Yanlış Girilmesi

Şifre Üreticinizin ürettiği şifreyi 3 defa yanlış girmeniz durumunda İnternet Bankacılığı girişiniz engellenecektir. Yeniden giriş yapabilmek için banka telefon yetkilisini arayarak blokenizi kaldırabilirsiniz.

3.1.5.7.4 Şifre Üreticinin Kaybolması veya Çalınması

Şifre üreticiniz kaybolur ya da çalınırsa, en kısa zamanda banka telefon yetkilisini arayarak ya da İnternet Bankacılığı içindeki şifre üretici menüsünden iptal talebinizi yapmanız gerekmektedir. İnternet Bankacılığı içerisinden yapılacak olan talepler mesai saatleri içerisinde olmak zorundadır.

3.1.5.7.5 Şifre Üreticini Kullanıma Kapatma

Şifre üreticinizi kullanıma kapatmak isterseniz, yine İnternet Bankacılığı içindeki şifre üretici kısmından ya da banka telefon yetkilisini arayarak iptal talebinizi yapmanız gerekmektedir. İnternet Bankacılığı içerisinden yapılacak olan talepler mesai saatleri içerisinde olmak zorundadır.

Şifre Üretici ile ilgili bilmeniz gereken önemli noktalar;

- Güvenliğiniz açısından şifre üreticinizi kimseyle paylaşmayınız ve sürekli yanınızda bulundurunuz.
- Şifre üreticinizi aktif hale getirmek için cihazınızın o anda ürettiği şifreyi banka telefon yetkilisine söylemeniz gerekir. Cihazınızı aktif hale getirdikten sonra, şifre üreticinizin ürettiği şifreleri, bankamız personeli de dahil olmak üzere, hiç kimseye söylemeyiniz.
- Şifre üreticiniz çalınırsa ya da kaybolursa hiç zaman kaybetmeden banka telefon yetkilisini arayınız.

- İnternet Bankacılığına giriş yaparken, şifre üreticinizin ürettiği şifreyi doğru girdiğinizden emin olmanıza rağmen giriş yapamamanız halinde banka telefon yetkilisini arayınız.
- Şifre üreticinizin arkasındaki tarih şifre üreticinizi son kullanma tarihidir. Bu tarihten sonra cihazınız kullanılamayacaktır. Bu durumda, şifre üretici talebinizi yine İnternet Bankacılığından yapmanız gerekir.

3.1.6 Kur ve Oranlar

3.1.6.1 Döviz Kurları

Bankanız Döviz Kurlarını son iş günü itibariyle veya istediğiniz tarihte görüntüleyebilir, hesap makinesiyle döviz/YTL çevirme işlemlerini yapabilirsiniz.

3.1.6.2 Repo Faiz Oranları

Bankanız tarafından verilen repo faizlerini görüntüleyebilir, istenilen vade ve tutar için net kazancınızı hesaplayabilirsiniz.

3.1.6.3 Vadeli Mevduat Faiz Oranları

YTL ve döviz bazında vadeli ve kırık vadeli mevduat faiz oranlarını görüntüleyebilir, istenilen vade ve tutar için net kazancınızı hesaplayabilirsiniz.

3.1.6.4 Bireysel Krediler Faiz Oranları

Bankanız tarafından verilen bireysel kredi tiplerinden istediğinizi seçerek aylık faiz oranlarını görüntüleyebilir, istenilen bilgileri girerek aylık taksit tutarını ve geri ödeme toplamını hesaplayabilirsiniz.

3.1.6.5 Kıymet Fiyatları

Kıymet Fiyatları; bankamızda bulunan kıymetlerin güncel alış/satış oranları, temiz/kirli fiyat ve stopaj durumları gösterilmektedir.

Stopaj; stopajlı kıymetlerden elde edilen faiz geliri ve alım satım kazancı üzerinden stopaj kesintisi yapılmaktadır.

Kıymet; uluslararası kullanılan menkul kıymet tanımlama kodudur.

Örn:

TR B 041006 T16 --> Koyu renk ile belirtilen kısım kağıdın vadesini göstermektedir.

TR T 061206 T12 --> Koyu renk ile belirtilen kısım kağıdın türünü göstermektedir.

Türü; İşlem yaptığınız devlet borçlanma kağıdının devlet tahvili mi yoksa hazine bonosu mu olduğunu gösterir.

T: Devlet Tahvili

B: Hazine Bonosu

Temiz Fiyat; Son kupon ödeme tarihinden valör tarihine kadar olan süre içinde birikmiş olan kupon faizini içermeyen fiyattır.

Kirli Fiyat; Birikmiş kupon faizinin üzerinde olduğu fiyattır.

3.1.7 Ödemeler

3.1.7.1 Fatura Ödeme

Bazı kurum ve kuruluşlara ait faturaların anlık durumunu sorgulayarak borç bilgilerinizi görüntüleyebilir, hızlı ödeme seçeneği ile daha önce ödemesini yapıp kaydettiğiniz abone numaralarına ait borç bilgisini hızlıca sorgulayabilir, isterseniz vadesiz YTL hesabınızdan ödeme yapabilirsiniz.

3.1.7.2 Fatura Ödeme Talimatı

Bazı kurum ve kuruluşlara ait faturalarınızın düzenli olarak ödenmesi için otomatik ödeme talimatı verebilirsiniz.

3.1.8 Para Transferleri

3.1.8.1 Havale ve EFT

Para transferi talimatınızı İnternet Bankacılığında yapabilirsiniz. Öncelikle işleminizin gerçekleştirileceği hesabınızı seçmeniz gerekmektedir.

Bir hesaba ilk defa transfer yapacaksanız ya da daha önce “çok kullandıklarım” listesine eklemediğiniz bir hesaba transfer yapacaksanız, yeni alıcıya seçeneğini işaretlemelisiniz.

Havale yapmak istiyorsanız “banka adı” alanında Bankanızı, EFT yapmak için ise karşı bankayı seçmelisiniz.

Parayı transfer edeceğiniz hesabın bulunduğu şubenin ilini “il adı” bölümünden seçiniz. Şube adını ise bir sonraki ekrandan seçeceksiniz. EFT talimatlarınız “transferin yapılacağı tarih” alanında girdiğiniz günün başlangıcı olan 00:00’dan saat 16:35’e kadar yapılmaktadır. İstenilen bilgileri girdikten EFT talimatı işleminize devam edebilirsiniz.

Bilgilerinizi son kez kontrol edip havale işleminizi tamamlamış olursunuz.EFT işlemleri sadece YTL para cinsinden yapılabilmekte olup, Bankanız hesapları arasında havalelerde ise

gönderici ve alıcı hesap türü aynı para cinsinden olmak koşuluyla tüm para türlerinden para transferinizi yapabilirsiniz.

Havaleler, talimat gününde karşı hesaba anında geçmektedir. EFT ise talimat gününde hesabınızdan anında gönderilmekte olup, karşı hesaba geçmesi zaman alabilir.

3.1.8.2 Hesaplarınız Arasında Transfer

Bankanız da bulunan ve İnternet Bankacılığında tanımlı vadesiz YTL ve döviz hesaplarınız arasında para transferi yapabilirsiniz.

3.1.8.3 Başka Banka KK Ödeme

Bankanızda bulunan vadesiz YTL hesaplarınızdan başka bankaların kredi kartlarına para transferi yapabilirsiniz.

Bir kredi kartı hesabına ilk defa transfer yapacaksanız ya da daha önce “çok kullandıklarım” listesine eklemediğiniz bir kredi kartına transfer yapacaksanız, yeni alıcıya seçeneğini işaretlemelisiniz.

16:35'ten sonra verilen kredi kartı borç ödeme talimatları EFT süresinin dolması nedeniyle aynı gün yapılamamaktadır. Ancak verdiğiniz talimatı bir sonraki iş günü için kaydedebilirsiniz.

3.1.8.4 Toplu Para Transferi

Bankanızdaki vadesiz YTL ve döviz hesaplarından daha önce “çok kullandıklarım” listesine eklediğiniz banka hesaplarınıza ve kredi kartlarınıza tek seferde para transferi yapabilirsiniz.

İşlem yapmak istediğiniz vadesiz YTL veya döviz hesabını seçip, havale veya EFT yapmak istediğiniz hesap numarasını ve/veya kredi kart numaralarını, “işlemin yapılacağı tarih” alanında istediğiniz tarihi seçiniz. “E-maile bildir” seçeneği sadece ileri tarihli işlemler için seçilebilir. Bilgilerinizi girdikten sonra işleminiz gerçekleştirilir.

3.1.8.5 Düzenli Ödeme

Bankanızdaki vadesiz YTL ve döviz haftalık ve aylık bazda düzenli olarak yapılmak üzere, para transferi talimatı verebilirsiniz. Bu menü haftalık ya da aylık bazda düzenli olarak fazla miktarda para transferi veya ödeme yapmak durumunda olan ve bu işlemleri her seferinde tekrarlamak istemeyen müşterilerimiz için çok kullanışlıdır.

3.1.8.6 Talimat İzleme

Seçtiğiniz tarih aralığında talimatlarınızı ve para transferlerinizi durumuna göre görüntüleyebilirsiniz.

İleri tarihli bir talimatınızı kontrol edecekseniz, bu talimatın gerçekleşmesi için yazdığınız tarihi de içeren bir aralıkta sorgulama yapmanız gerekmektedir.

İleri tarihli EFT talimatınız, hesabınızda yeterli bakiye olması durumunda saat 09:00'da gerçekleşecektir. Hesabınızda yeterli bakiye olmaması durumunda ise; aynı gün içinde saat 09:10 ile 16:20 arasında hesabınız sürekli kontrol edilerek talimatınızın gerçekleştirilmesine çalışılacaktır. 16:20'den sonra hesabınızda yeterli bakiye olsa bile talimatınız yapılamamış ve iptal edilmiş olacaktır.

İleri tarihli havale talimatınız, hesabınızda yeterli bakiye olması durumunda saat 05:00'de gerçekleşecektir. Hesabınızda yeterli bakiye olmaması durumunda ise; aynı gün içinde saat 05:00 ile 17:00 arasında hesabınız sürekli kontrol edilerek talimatınızın gerçekleştirilmesine çalışılacaktır. 17:00'den sonra hesabınızda yeterli bakiye olsa bile talimatınız yapılamamış ve iptal edilmiş olacaktır.

İleri tarihli vadesiz hesabınızdan yatırım hesabınıza havale talimatınız, hesabınızda yeterli bakiye olması durumunda saat 09:15'de gerçekleşecektir. Hesabınızda yeterli bakiye olmaması durumunda ise; aynı gün içinde saat 09:15 ile 11:10 arasında hesabınız sürekli kontrol edilerek talimatınızın gerçekleştirilmesine çalışılacaktır. 11:10'dan sonra hesabınızda yeterli bakiye olsa bile talimatınız yapılamamış ve iptal edilmiş olacaktır.

İleri tarihli yatırım hesabınızdan vadesiz hesabınıza havale talimatınız, hesabınızda yeterli bakiye olması durumunda saat 09:07'de gerçekleşecektir. Hesabınızda yeterli bakiye olmaması durumunda ise; aynı gün içinde saat 09:07 ile 12:05 arasında hesabınız sürekli kontrol edilerek talimatınızın gerçekleştirilmesine çalışılacaktır. 12:05'den sonra hesabınızda yeterli bakiye olsa bile talimatınız yapılamamış ve iptal edilmiş olacaktır.

3.1.8.7 Çok Kullandıklarım

Sıklıkla havale, EFT ve kredi kartı borç ödeme için verdiğiniz transfer talimatları sırasında girdiğiniz hesap numaralarını çok kullandıklarına kaydedebilir, bu hesaplara isim verebilir ve bu hesaplara tekrar para transferi yapmak istediğinizde alıcı bilgilerini yazmadan talimatınızı verebilirsiniz.

“Hesaba para transferleri” başlığı altında EFT, havale yaptığınız hesapları; “kredi kartına para transferleri” başlığı altında ödeme yaptığınız kredi kart numaralarını görüntüleyebilirsiniz.

3.1.8.8 Döviz Transferi(SWIFT)

Döviz transferi adımı ile yurtiçi ve yurtdışındaki bankalara döviz transferi işlemlerinizi gerçekleştirebilirsiniz.

3.1.8.8.1 Giriş

Döviz transferi işlemini yapabilmemiz için öncelikle bir döviz hesabınızın bulunması gerekmektedir. Bankanın bulunduğu ülkeyi seçtikten sonra, transferi gerçekleştireceğiniz bankanın ilk iki harfini ve transferi gerçekleştirmek istediğiniz bankanın/şubenin bulunduğu

şehrin ilk iki harfini girmeniz gerekecektir. Yurt içindeki bankalara döviz transferi yapılacak ise dikkat edilmesi gereken nokta başlangıcında Türkiye bulunan bankalara (Türkiye İş Bankası vb) transfer yapılacağı zaman bankanın ilk iki harfinin girilmesi istenen kısma “tu” girilmesi gerekecektir

Bu girişleri yaptıktan sonra belirlediğiniz kriterlere uyan ve Döviz transferi sistemine tanımlı banka şubeleri listelenecektir. Buradan diğer gönderim bilgilerini girerek işleminizi tamamlayabilirsiniz. Döviz transferi işlemleri hafta içi 09:00 – 16:00 arasında yapılabilmektedir. Döviz transferi işlem girişinizi gün içinde saat 12:30'dan önce yapmanız durumunda para aynı gün, 12:30'dan sonra yapmanız durumunda ise 1 iş günü valörlü karşı bankadaki hesaba gönderilecektir.

3.1.8.8.2 İptal

Yapmış olduğunuz Döviz transferi işlemini iptal ettirmek istiyorsanız banka telefonunu arayarak taleplerinizi iletebilirsiniz. Ancak karşı banka bu işlemde dolayı masraf talep edebilir. İptal işleminden kaynaklanan masraflar, döviz transferi işleminin yapıldığı hesabınızdan alınacaktır.

3.1.8.8.3 İşlem Ücret ve Limiti

İnternet Bankacılığında veya telefonda gerçekleştirilen döviz transferi işlemleri için 3000 \$'a kadar olan kısımdan komisyon alınmamakta olup sadece alınması zorunlu olan 25 YTL +BSMV= 26.25 YTL karşılığı USD yasal vergi alınmaktadır. 3000 \$ ve üzeri işlemlerde masraf haricinde binde 5 komisyon alınacaktır. İşlem günlük limiti alt limit 1000 \$, üst limit ise 10.000 \$ veya aynı miktarda Euro'dur.

3.1.8.8.4 Önemli Noktalar

İnternet Bankacılığında döviz transferi işlemleri sadece serbest transferler için gerçekleştirilecektir. Eğer işleminiz ticari amaçlı (ithalat-ihracat amaçlı transferler, ödemeler) bir işlem ise işleminizi şubeniz aracılığı ile yapmanız gerekmektedir.

İşleminiz, girişinizi yaptıktan kısa bir süre sonra gerçekleştirilecektir. İşlem açıklamanız serbest transferler için uygun değilse işleminiz iptal edilecektir. İşlemin hangi aşamada olduğunu İnternet Bankacılığında takip edebilirsiniz.

Gerçekleşmiş olan bir döviz transferi işleminizdeki bilgi eksiklikleri (örneğin, karşı bankadaki alıcı ismi ile alıcı hesap numarasının tutmaması) nedeni ile gerçekleştirilemeyebilir. Bu durumda transferi gerçekleştirdiğiniz banka, bankanızdan işlem ile ilgili bilgilerde düzeltme isteyecektir. Bu bilgilerin tamamlanması amacıyla girdiğiniz telefon numarasından aranarak bilgilerde düzeltme yapmanız talep edilecektir. Karşı banka işlemde yapacağı güncellemeler için ücret talep edebilir. Bu işlem ücreti işlemi gerçekleştirdiğiniz şubede bulunan hesaplarınızdan kesilecektir.

3.1.8.9 Hızlı Gönder

Hızlı para transferi adımını kullanarak para transferi işlemlerinizi hızlı bir şekilde gerçekleştirebilirsiniz. Son yaptığınız 10 adet EFT/havale/hesaplarım arasında havale işlemi görüntülenecektir. Buradan istediğiniz işlemi yeniden seçerek onaylamanız gerekecektir. Dilerseniz buradan meblağ ve şube değişikliklerini gerçekleştirebilirsiniz.

3.1.9 Yatırım İşlemleri

3.1.9.1 Repo

Bankanızdaki yatırım hesaplarınızın, anlık olarak nakit durumunu, menkul durumunu görüntüleyebilir vadesiz hesabınızdan repo bağlayabilirsiniz.

Repo işlem tutarı 250.00 – 5.000.000.00 aralığında YTL veya YTL karşılığı olmalı ve vadesiz hesabınızda yeterli bakiye olmalıdır.

Repo başlangıç tarihinde girdiğiniz tarih o gün yada sonraki bir tarih olmalı ve iş gününe denk gelmelidir. Geçmiş tarih için repo bağlayamazsınız.

Repo başlangıç tarihi alanında istediğiniz tarihi seçip “tamam” butonuna basınız. Repo başlangıç tarihi, bulunduğunuz güne denk geliyorsa o günkü repo faiz oranlarını görüntüleyebilirsiniz. Bankanızda vadesiz hesaplarınız olduğu halde görülmeyen hesaplarınızı tanımlatmak için, bankanıza ait telefonları arayabilir veya şubenize başvurabilirsiniz.

3.1.9.2 Repo İzleme

Bankanızdaki vadesiz hesaplarınızın anlık olarak nakit durumunu, menkul durumunu görüntüleyebilir; repo emirlerinizin gerçekleşip gerçekleşmediğini görüntüleyebilir ve verdiğiniz repo emirlerini durumuna göre sorgulayabilirsiniz. Vermiş olduğunuz repo talimatlarını, vadesiz hesabınızın bulunduğu şubeden saat 15:00’a kadar iptal ettirebilirsiniz.

Bankanızda vadesiz hesaplarınız olduğu halde görülmeyen hesaplarınızı tanımlatmak için, bankanıza ait telefonları arayabilir veya şubenize başvurabilirsiniz.

3.1.9.3 Vadeli Hesap İşlemleri

Yeni vadeli hesap açabilir ve seçtiğiniz vadeli hesabınızı istediğiniz zaman kapatabilirsiniz.

Vadeli hesap açabilmeniz için vadesiz YTL veya döviz hesabınızın bulunması gerekmektedir. Vadeli hesap açma işlem tutarı 1.00 – 500.000.00 aralığında YTL veya YTL karşılığı olmalıdır.

Vadeli hesap açılışları mesai günlerinde saat 15:00’a kadar aynı gün, 15:00’dan sonra ve diğer günlerde bir sonraki iş günü valör ile açılmaktadır.

Vadeli hesabınızı bozabileceğiniz üst sınır 100.000 YTL veya YTL karşılığıdır. Daha üst limitler için işlem yapılamayacaktır. Vadeli hesabınız, vadesi dolmadan bozulduğu takdirde, geçen günler için faiz ödemesi yapılmayacaktır.

3.1.9.4 Fon İşlemleri

A tipi değişken, B tipi likit, B tipi tahvil bono ve B tipi değişken fon alım/satımı yapılmakta, portföy görüntüleme, fon fiyatı görüntüleme, emir takibi ve fon hareketleri görüntülenmektedir.

3.1.9.5 Fon Alım/Satımı

İnternet Bankacılığında Bankanız A Tipi Değişken Fonu, Bankanız B Tipi Likit Fonu, Bankanız B Tipi Tahvil Bono Fonu ve Yatırım B Tipi Değişken Fonu alıp/satabilirsiniz.

Fon Tipi	İşlem Saati	İşlemin Gerçekleşeceği Tarih	
		Alış	Satış
A Tipi Değişken Fon	09:00 - 12:00	1 iş günü sonra	1 iş günü sonra
	12:00 - 24:00	2 iş günü sonra	3 iş günü sonra
B Tipi Likit Fon	09:00 – 24:00	aynı gün	aynı gün
B Tipi Tahvil ve Bono Fonu	09:00 - 13:40	1 iş günü sonra	1 iş günü sonra
	13:40 - 24:00	2 iş günü sonra	2 iş günü sonra

3.1.9.6 Fon Fiyatları

İşlem gören yatırım fonlarının güncel alış / satış fiyatlarını görüntüleyebilirsiniz.

3.1.9.7 Fon Portföy

Yatırım hesabınızda bulunan nakit bakiyenizi, fon bakiyenizi ve fon adedinizi fiyatıyla beraber görebilirsiniz.

3.1.9.8 Fon Hareketleri

Seçtiğiniz tarih aralığında yatırım fonu alım satım hareketlerinizi görebilir, dekontunu alabilirsiniz. İleri tarihli gerçekleşmiş fon emirlerinizin de dekontunu bu adımdan alabilirsiniz.

3.1.9.9 Fon Emir Listesi

Verdiğiniz fon emirleri görüntülenmektedir.

3.1.9.10 Hazine Bonosu/Devlet Tahvili/Eurobond

Hazine bonusu; 1 yıla kadar olan devlet borçlanma kağıdıdır.Devlet tahvili; 1 yıldan daha uzun süreli olan devlet borçlanma kağıdıdır.Eurobond; Eurobondlar kurum/şirket veya devletlerin yurtdışından kaynak sağlamak amacıyla kendi ulusal para birimleri dışında bir para birimi cinsinden yurtdışında çıkardıkları (yurtdışına ihraç ettikleri) uzun vadeli (genelde 2-30 yıl) tahvillerdir.

Kesin alış; bankanızda satışa sunulmuş olan kıymetleri görüntüleyebilir ve kıymetin alış işlemini gerçekleştirebilirsiniz.

Kesin satış; portföyünüzde bulunan kıymetleri görüntüleyebilir kıymetin satış işlemini gerçekleştirebilirsiniz.

Kıymet fiyatları; bankanızda bulunan kıymetlerin güncel alış/satış oranları, temiz/kirli fiyat ve stopaj durumları gösterilmektedir.

Stopaj; stopajlı kıymetlerden elde edilen faiz geliri ve alım satım kazancı üzerinden stopaj kesintisi yapılmaktadır.

Kıymet; uluslararası kullanılan menkul kıymet tanımlama kodudur.

Örn:

TR B **041006** T16 --> Koyu renk ile belirtilen kısım kağıdın vadesini göstermektedir.

TR T 061206 T12 --> Koyu renk ile belirtilen kısım kağıdın türünü göstermektedir.

Türü; işlem yaptığınız devlet borçlanma kağıdının devlet tahvili mi yoksa hazine bonusu mu olduğunu gösterir.

T: Devlet Tahvili.

B: Hazine Bonosu.

Temiz fiyat; son kupon ödeme tarihinden valör tarihine kadar olan süre içinde birikmiş olan kupon faizini içermeyen fiyattır.

Kirli fiyat; birikmiş kupon faizinin üzerinde olduğu fiyattır.

Portföy; "Portföy" adından portföyünüzde bulunan kıymetlerin detaylarını görebilir, kar/zarar bilgisi, kuponlu devlet tahvili ve eurobondlara ait kupon ödemelerini izleyebilirsiniz.

Hesap makinesi; "Hesap makinesi"ni kullanarak dönemsel getiri ve kar/zarar hesaplamaları yapabilirsiniz.

3.1.9.11 Hisse Senedi İşlemleri

Hisse Senedi:

Bir anonim şirketin eşit paylara bölünmüş sermayesinin bir payını temsil eden kıymetli evraktır. Anonim şirketlerin halka açık olan yüzdelerini temsil eden hisse senetlerinin alım-satımı İstanbul Menkul Kıymetler Borsası'nda yapılmaktadır.

İnternet Bankacılığını kullanarak İMKB'de işlem gören halka açık şirketlere hissedar olabilir, tüm hisse senedi işlemlerinizi gerçekleştirebilirsiniz. İnternet Bankacılığında hisse senedi işlemleri yapabilmek için yatırım hesabınızın bulunması gerekmektedir.

3.2 Sonuç

Bu kısımda İnternet Bankacılığında ne gibi işlemlerin yapılabileceği belirtilmiştir. Tez kapsamında bu işlemlerden para transfer işlemleri önem arz etmektedir. Çünkü dolandırıcıların müşteriye maddi yönden zarar vermesi EFT veya havale ile sağlanmaktadır. Dolandırıcı kişi bilgilerini aldığı müşterinin hesaplarındaki parayı, kendine veya bir başkasına ait olan hesap numarasına EFT ya da havale ile göndermektedir. Bir ATM veya banka şubesine giderek parayı alabilmektedir. Tez kapsamında müşterinin para transferi yaparken ne zaman yaptığı, hangi banka,şube ve hesaba ne kadar transfer yaptığı incelenmiştir.

Tez sonunda oluşturulacak Dolandırıcılık Tespit Sistemi, havale veya EFT işlemleri gerçekleştirilmeden önce çalıştırılıp yapılacak para transferi işleminin yasal veya suçlu olup olmadığına karar verecektir. Buna göre işlem onaylanıp onaylanmayacaktır. Burada anlatılan İnternet Bankacılığı işlemleri, tez için eğitim örneklerinin oluşturulmasını sağlamaktadır.

4 İNTERNET BANKACILIĞINDA GÜVENLİK

4.1 İnternet Bankacılığında Güvenlik Unsurları

Bu bölümde İnternet Bankacılığında güvenliği sağlamak için kullanılan yöntem ve araçlar anlatılmıştır.

4.1.1 SSL 128 Bit Şifreleme

İnternet Bankacılığı SSL 3.0, 128 bit şifreleme sistemiyle korunmaktadır. Bu sistem sayesinde sizin bilgisayarınız ile bankacılık sisteminiz arasında son derece güvenli bir hat kurulur. Tüm dünyada yaygın olarak güvenlik amaçlı kullanılan bu sistem sayesinde bilgileriniz ve hesaplarınız güvenlidir.

4.1.2 Şifre Alma Aşamasında Bankamatik Kart Şifresinin Sorulması

İnternet Bankacılığı şifrenizin oluşturulabilmesi için bankamatik kart şifrenizi tuşlamanız gerekmektedir. Banka telefon yetkilisi tarafından kart şifresi verilirken güvenlik teyidinden geçirildiğiniz için şifre oluşturma sürecinde iki aşamalı kontrol sağlanmış olur.

4.1.3 Banka Telefon Yetkilisi Tarafından Sorulan Güvenlik Soruları

Kart şifresi alma işleminde olduğu gibi; İnternet Bankacılığı şifrenizi oluştururken de banka telefon yetkilisi tarafından yapılacak olan güvenlik teyidinden geçmeniz gerekmektedir.

4.1.4 Doğum tarihi ve TC. Kimlik No Kontrolü

İnternet Bankacılığı şifrenizi aldıktan sonra, İnternet Bankacılığı ilk giriş esnasında size sorulacak olan doğum tarihi ve TC. kimlik numaranızı, başvuru formunda vermiş olduğunuz şekilde cevaplamanız gerekmektedir.

4.1.5 Sanal Klavye Kullanımı

Sanal Klavye kötü niyetli kişilerin İnternet Bankacılığı şifresini çalmak için kullandıkları screenloger ve keylogger gibi programları etkisiz hale getiren bir güvenlik katmanıdır.

4.1.6 Şifre Üretici

İnternet Bankacılığına girişte ekstra güvenlik sağlayan, her 60 saniyede, yeni, size özel ve tek kullanımlık şifreler üreten bir cihazdır. İnternet Bankacılığı müşterisi iseniz İnternet Bankacılığındaki tanımlamalar/şifre üretici seçeneğinden başvurunuzu yapabilirsiniz. Şifre üretici; başvurunuzdan kısa bir süre sonra tarafınıza kurye ile imza karşılığında teslim edilir. Şekil 4.1’da bir şifre üretici görülmektedir.



Şekil 4.1 Şifre Üretici(www.sekerbank.com.tr)

4.1.7 Hatalı Parola ve Şifre Girişinin Gösterilmesi

Bu adımdan erişim yaptığınız tarih ve saat bilgilerini kontrol ederek, bilginiz dışında bir erişimin söz konusu olup olmadığını kontrol edebilirsiniz.

4.1.8 Otomatik Oturum Kapatma

Güvenli çıkış işlemini yapmadan İnternet Şubesinin başından ayrıldığınız durumlarda, izinsiz kullanımı engellemek amacıyla İnternet Bankacılığı oturumu 6 dakika sonra otomatik olarak kapatılır.

4.1.9 Güvenlik Sorusu

İzniliniz dışında gerçekleşebilecek para çıkışı ve bilgi değişikliğini önlemek, yaptığınız işlemleri teyit etmeniz amacı ile para transferi ve bankacılık işlemlerinizde kendi belirlediğiniz güvenlik sorusunun rasgele iki karakteri sorulur. 60 günlük periodlar ile sizden güvenlik sorunuzu değiştirmeniz istenecektir. Şifre Üretici kullanarak işlem yapan müşterilerin güvenlik sorusu yerine Şifre Üreticinin anlık olarak ürettiği şifreyi kullanmaları gerekmektedir.

4.1.10 Zaman ve Tatil Ayarları

Bu seçenek ile seçilen gün, saatler veya tarih aralığı haricinde İnternet Bankacılığı kullanımınızı engelleyebilirsiniz. İnternet Bankacılığı kullanmak istediğiniz gün, saat veya tarih aralığını belirlemeniz için İnternet Bankacılığı içindeki Tanımlamalar ve Güvenlik ayarları menüsünden güvenlik sorusunu cevapladıktan sonra gün, saat tercihlerini veya tatil ayarlarını yapmanız gerekir.

4.1.11 IP Aralık Belirleme

Bu adım kullanılarak İnternet Bankacılığına belirlediğiniz üç farklı IP aralığından erişim sağlayabilirsiniz. IP aralığını belirlemek için İnternet Bankacılığındaki Tanımlamalar/Güvenlik

ayarları menüsünden güvenlik sorusunu cevapladıktan sonra kullanmak istediğiniz IP aralığını seçmeniz gerekmektedir.

4.1.12 Para Transferini Kapama ve Kısıtlama

Bu adım ile İnternet Bankacılığı üzerinden yapacağınız havale ve EFT ve döviz transferi işlemlerine kısıtlama getirebilir ve günlük işlem limitlerinizi tanımlayabilirsiniz. Limitlerin "0" olarak belirlenmesi durumunda İnternet Bankacılığı ile yapılan tüm para transferi işlemleri kapatılacaktır. İnternet Bankacılığında para transferi işlemlerini kapama ya da kısıtlama yolu ile güvenliğinizi sağlamak için İnternet Bankacılığındaki tanımlamalar/güvenlik ayarları kısmından güvenlik sorusunu cevapladıktan sonra günlük işlem limitlerini tanımlamanız gerekmektedir.

4.1.13 Para Transferi Uyarısı Tanımlama

Bu seçenek ile İnternet Bankacılığında belirlemiş olduğunuz işlem ve limitlerin üstünde bir para çıkışı olması durumunda e-posta adresinize uyarı maili gönderilir. Kendi belirlediğiniz limitlerin üzerinde para transferi olduğunda uyarı almak için İnternet Bankacılığındaki tanımlamalar ve güvenlik ayarları kısmından güvenlik sorusunu cevapladıktan sonra para transferi uyarısı almak istediğiniz ürünü seçmeniz ve uyarı almak istediği tutarı belirlemeniz gerekmektedir. Belirlenen tutarın üstündeki işlemlerde belirttiğiniz e-posta adresine bilgi mesajı gönderilmektedir.

4.1.14 Hesap Ayarları

Bu adım ile İnternet Bankacılığında görüntülenmesini istemediğiniz hesaplarınızı belirleyebilirsiniz. Bu sayede seçilen hesaplar İnternet Bankacılığının hiç bir menüsünde görüntülenmez ve olası herhangi bir müdahaleye karşı güvenlik sağlanır. İnternet Bankacılığında hesap ayarlarını yaparak kişisel güvenlik sağlamak için İnternet Bankacılığındaki tanımlamalar/güvenlik ayarları kısmından güvenlik sorusunu cevapladıktan sonra İnternet Bankacılığında görüntülenmesini istemediğiniz hesaplarınızı belirlemeniz gerekmektedir.

4.2 İnternet Bankacılığına Saldırıları

İnternet bankacılığını suiistimal edip yasadışı yollardan bilgi edinme ve dolandırıcılık yolu ile finansal getiri elde etme amacıyla yapılan dolandırıcılık eylemleri mevcuttur. Son zamanlarda adı sıkça duyulan dolandırıcılık olayları ve internet dolandırıcılığı hakkında bilgilendirmek ve oluşabilecek riskleri en aza indirmek için bilinmesi gereken önemli noktalar bulunmaktadır.

Finansal işlemlerinizi güvenli bir şekilde yapmanız ve bilgi güvenliğinizin sağlanması banka için en önemli konuların başında gelir. Bu konu ile ilgili olarak banka tarafından alınmış olan pek çok güvenlik önlemi vardır. Fakat tek başına banka tarafından önlem alınması yeterli değildir.

Güvenli finansal işlem yapma ve bilgi güvenliği konusunda müşterilerin bazı konularda bilgi sahibi olup yine bir takım önlemleri alıp dikkatli davranması gerekmektedir.

İnternet üzerinden yapılan sahtekarlık ve dolandırıcılık eylemleri sonucunda kredi kartı bilgileri, özlük bilgileri ve mail adresi çalınabilir. Bu dolandırıcılık ve sahtekarlık eylemleri çeşitli yollardan yapılabilmektedir.

4.2.1 Keylogger Saldırıları

Keylogger, klavye ve ekran görüntülerinin kopyalanabilmesini sağlayan, kısaca ekranda görünen ve yapmış olduğunuz her türlü işlemi kayıt etmeye yarayan casus programlara verilen isimdir.

İnternet kullanan banka müşterilerinin veya internet üzerinden finansal işlem yapan kullanıcıların çevrimiçi işlem şifrelerinin çalınması "keylogger", yani klavye tuş girdilerini kayıt eden yazılımlar vasıtasıyla yapılmaktadır. Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden truva atı (trojan) adlı yazılımlar aracılığıyla keylogger yazılımları sisteme yüklenebilir.

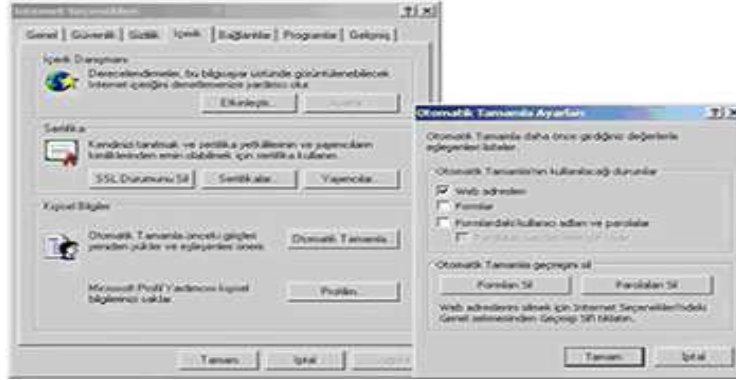
Kötü niyetli ya da korsanlar tarafından kullanıcıların bilgisayarlarına yerleştirilen keylogger adlı yazılım, bilgisayarda yapılan her türlü işlemin bir kaydını tutar, bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar sistemde; .txt (metin) dosyası olarak tutulur veya klavye girdileri e-posta ile saldırgana (Hacker) gönderilir. Bu şekilde müşterilerin önemli bilgileri, şifreleri, kullanıcı adı ve parola bilgileri saldırgana ulaşmış olur.

Keylogger yazılımı bilgisayara, kullanıcı tarafından da, diğer bilgisayar kullanıcılarını kontrol etmek amacıyla (örneğin; ebeveynlerin, çocuklarının girdiği siteler hakkında bilgi edinmesi için) yüklenebilir. Buna "ebeveyn denetimi" de denebilir.

4.2.2 Keylogger Saldırılarından Korunma

1. İşletim sisteminizi belli aralıklarla güncellenmeli.
2. Bankacılık ve her türlü finansal işlemlerinizi güvenli olmayan bilgisayarlardan yapılmamalı.
3. Kullandığınız bilgisayarın internet tarayıcısı (web browser)'nın otomatik tanımlama özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmın işaretli olmasına dikkat edilmeli ve "Formlarda kullanıcı adları ve parolalar" bölümündeki düzenleme aşağıdaki şekilde yapılmalıdır.

* İnternet Explorer 6.0 için (Araçlar->İnternet Seçenekleri->İçerik->Otomatik Tamamla)



Şekil 4.2 Otomatik Tanımlama

4.2.3 Olta(Phishing) Saldırıları

Phishing, İngilizce "password" (şifre) ve "fishing" (balık avlamak) kelimelerin birleşmesiyle meydana gelmiş bir kelime olup, illegal yollarla bir kişinin şifresini veya kredi kartı detaylarının öğrenilmesine denir. "Phisher" diye tanımlanan şifre avcıları, genelde e-posta vb. yollarla şahıslara ulaşır ve onların kredi kartı vb. detaylarını sanki resmi bir kurummuş gibi isterler. Bu "av" a karşılık veren kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınabilir.

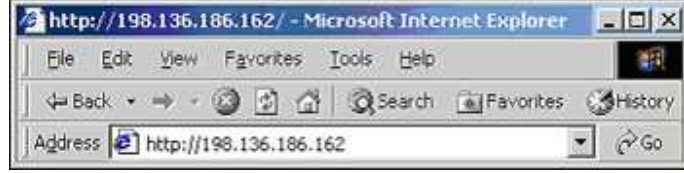
Olta saldırıları internet üzerinde en çok kullanılan dolandırıcılık yöntemlerinden biridir. Son zamanlarda bu tarz saldırıların sayısı oldukça artmıştır.

Olta saldırıları kapsamında; çeşitli banka ve finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş izlenimi veren sahte e-postalar internet aracılığıyla yayılmaktadır. Bu e-postalarda verilen linkler ile banka müşterilerinden, kart bilgileri, kart şifreleri, internet şubesi şifreleri ve kişisel bilgileri istenmektedir. Bu eylem açık bir dolandırıcılık girişimidir. Bankalar, e-posta yoluyla hiç bir şekilde şifre işlemleri yaptırmamaktadır, gizli kişisel bilgiler istememektedir.

Sahtekarlığı gerçekleştirecek kişi/kişiler, bir banka, kart şirketi veya bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. E-posta'nın konusu, müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve ilgili kurumların sayfalarının bire bir kopyası şeklinde görünen internet sayfalarına giden link'lerden oluşmaktadır. Bir başka tuzak ise; "tarafınıza X adlı kişiden 500 YTL para transferi yapılmıştır. Lütfen aşağıdaki linke tıklayın ve internet bankacılığınıza giriş yaparak bilgilerinizi kontrol ediniz" gibi olabileceği gibi yine yukarıdaki olaydaki gibi bir mailde "Eğer internet bankacılığına girerek işlemi onaylamazsanız para transferi gerçekleştirilmeyecektir" gibi tuzağa düşürücü ibareler bulunabilmektedir.

Maile gelen link ile açılan sayfa birebir bankanızın internet sayfası görünümünde olabilir. Bu nedenle bu tür e-postalardaki linklerin açtığı sayfalarda kesinlikle şifrenizi ya da kişisel bilginizi girmemelisiniz.

Bazı müşteriler, bu tarz tehlikelerin farkında olmadan, istenilen bilgileri doldurularak e-postalara cevap verirler veya mail içindeki linke tıklayıp şifre, parola gibi bilgilerini girerler. Bunun sonucunda, müşteri kişisel bilgileri ve şifreleri dolandırıcılar tarafından çalınmış olur. Bu tür mailler üzerinden gelen saldırılar sonucu girilen internet sitesinin web adresleri genelde rakamlardan veya alan adındaki ufak değişikliklerden oluşmaktadır.



Şekil 4.3 rakamlardan oluşan bir site yapısı

Sahtekarlığı gerçekleştirecek kişi/kişiler olta yöntemi ile ele geçirdikleri finansal bilgileri kullanarak karmaşık yöntemlerle hesabınızdaki paraları ele geçirme imkanına sahiptirler. Paranın hesaptan çekilmesi aşamasında, kimliklerinin tespit edilmesini engellemek için, saldırganlar şüphelenilmeyecek üçüncü kişileri kullanırlar. Bu üçüncü kişilere ulaşmak içinde internet üzerinden sahte iş ilanları yayınlırlar. Bu ilanlarda çaba harcamadan kolay para kazanılacağı şeklinde bilgi verilmektedir. Bu ilana başvuruda bulunan kişilerin hesap bilgilerinin isterler. Daha sonra üçüncü kişinin hesapları kullanılarak olta yöntemi ile ele geçirilen hesaplardan kendi hesaplarına para transferi yaparlar. Böylece sahtekarlığı gerçekleştiren kişi/kişiler kimliğini gizli tutmuş olur ve ilan aracılığı ile başvuran üçüncü kişilere suçu atmış olur.

Özetle, belirli bir parayı alıp, komisyon karşılığında başka bir yere transfer etmek şeklindeki iş ilanları konusunda çok dikkatli olunması gerekmektedir. Bu şekilde kara para aklanmış olup, sonucu kanuni takibata kadar varabilecektir.

4.2.4 Olta(Phising) Saldırılarından Korunmak İçin

1. Gönderilen e-posta'nın kimden geldiğinden ve doğruluğundan mutlaka emin olunmalı. Gönderen kişiyi yabancı ise maillerdeki linkleri tıklamamalı veya gönderilen dosyaları açmamalıdır.

2. Banka veya ticari kurumlardan gelmiş gibi gösterilen ve şifre, kullanıcı adı, müşteri numarası, kredi kartı numarası, kimlik numarası gibi bilgileri talep eden e-postaları dikkate almamalı ve hemen silinmelidir.

3. E-postalarda bulunan linkler üzerinden herhangi bir bankanın İnternet bankacılığına girilmemelidir.

4. Adres barında gözükken ismi sayılardan oluşan internet bankacılığı sitelerine girilmemelidir ve girmek istenilen sitenin adını müşteri kendi yazmalıdır.. Örneğin: <http://www.bankanizinismi.com.tr> doğru bir kullanımdır. Bunun yanında <http://198.136.186.162> yanlış bir kullanımdır. Çoğu kurum ya da kuruluş web adresi olarak isim kullanmaktadır.

5. İnternet tarayıcısının üst kısmındaki adres çubuğunda bulunan adresin "https" ile başladığı kontrol edilmelidir, "https" in son kısmında yer alan "s" harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırıldığını belirtir. Bunlara ek olarak, internet tarayıcının sağ alt kısmında yer alan kapalı kilit işareti, yine güvenli ve şifrelenmiş bir sayfada işlem yaptığınızı gösterir.



Şekil 4.4 Kapalı kilit işareti (www.sekerbank.com.tr)

6. Olta saldırısından şüphelenilen bir e-postaya cevap verilmişse önce kart ve internet şubesi şifreleri değiştirilmelidir. Banka çağrı merkezini arayarak konu hakkında bilgi verilmelidir.

4.2.5 Casus Yazılımlar ve Diğer Saldırıları

Keylogger ve olta saldırılarının dışında saldırganlar (hacker) tarafından finansal bilgilerinizin çalınması için uygulanan pek çok yöntem bulunmaktadır. Bir saldırının öncelikli amacı bilgisayara casus program yükleyebilmek ve bilgilere ulaşmaktır.

Bir bilgisayarı ele geçirmek için en kolay yol bir dosyanın içine virüs programı saklamaktır. Saldırgan bu hedefine ulaşabilmek için; öncelikli olarak güveni sağlamak isteyebilir. Bu amaçla kendi mail adresini aşına olunan bir mail adresi (resmi kurumlar, yakınlar vs.) gibi göstererek güvenilmesini sağlar. Saldırganlar, bunun dışında çok cazipmiş gibi görünebilen bir dosya veya link yollar. Bu dosya bilgisayara kopyalandığında (veya e-posta ekinde açıldığında) ve çalıştırıldığında, virüs bilgisayara bulaşmış olacaktır.

Bilgisayara girmesi muhtemel virüsler genellikle uygulama (.EXE) dosyalarında saklanabilmektedir. Ancak macro virüsü ofis programlarının içinde de saklanabilmektedir. (.DOC, .XLS ve .PPT dosyaları). İki virüs tipi de sisteminize zarar verebilir veya bilgisayarınızdaki ya da ofis ağınızdaki gizli bilgilerinizin kopyalanmasına neden olabilir.

Kısaca, bir saldırının yolladığı mailde ya bir link ya da açmanız için bir dosya bulunur. Bu linke tıkladığında veya yollandığında dosya açıldığı takdirde artık saldırgan bilgisayara hakim olabilir demektir. Bu şekilde bilgisayara casus yazılımlar (trojan, worm, spyware, keylogger, solucan, vs.) yüklenmiş olur. Saldırgan bu yolları kullanarak kötü amacına ulaşabilir. Bu tehlikeden korunmanın en iyi yolu yüzde yüz güvenilmeyen sitelerden program indirmemek, bu programları kullanmamak ve yabancı kişi veya kurumlardan gelen e-postalar da ekli olan dosyaları açmamaktır.

Bunların dışında, bilgisayarınıza aktif web içeriği kullanarak ulaşmak ta mümkündür. ActiveX ve Java normalde interaktif içerik sağlamak için kullanılan teknolojiler olmakla birlikte

bazen kötü amaçlı olarak da kullanılabilirler. Tarayıcının ayarları yapılarak bu içeriğin kişisel bilgisayara veya bilgisayar ağına zarar verme ihtimalini ortadan kaldırılabilir.

Son olarak değinilmesi gereken bir konu ise; şifre hırsızlığının ve dolandırıcılık eylemlerinin müşterilerin tanıdıkları kişiler tarafından yapılabilme riski bulunmasıdır. Maalesef bu şekilde müşterilerin tanıdıkları (eşi, çocukları, arkadaşı, akrabası vs.) tarafından dolandırılmaları seyrek de olsa gerçekleşmekte ve müşteriler mağdur olmaktadır. Bu dolandırıcılık eylemi "sosyal saldırı" (Social Hack) olarak bilinmektedir. Sosyal dolandırıcılığın engellenebilmesi için müşterinin şifre, kullanıcı adı ve parola gibi önemli bilgileri kimseye vermemesi veya not etmemesi, kendi adlarına yakınlarının işlem yapmalarını istememeleri gerekmektedir.

4.2.6 Alınması Gereken Önlemler

Yukarıda anlatılmış olan saldırıların dışında güvenliğinizi açısından aşağıdaki konulara da dikkat etmeniz gerekmektedir.

1. Bankanız, mail yoluyla bilgilerinizi güncellemeniz konusunda sizlerden talepte bulunmamaktadır.

2. Kimlik bilgileriniz, adres bilgileriniz ve her türlü kişisel bilgilerinizi talep eden maillere asla cevap yazmayınız. Bu mailler tanıdığınız kişilerden bile gelmiş gibi gözükebilir.

3. Kredi Kartı numaranızı, kartın son kullanma tarihini ve kartın arka yüzündeki CVV2 numarasını kimseye paylaşmamalı bir yere not edilmemelidir.

4. Bilgisayara e-mail vasıtasıyla gelen veya internette rasgele bulunan programları yüklememeli ,çünkü bu programlar korsan ya da ele geçirme amaçlı çeşitli tuzaklar içerebilir.

5. Kredi kartı kullanılan ya da kişisel bilgilerin yazıldığı bilgisayarın güvenli olmasına dikkat edilmeli. (Kullanılan web sitesi <http://> yerine <https://> olmalıdır).

6. Düzenli olarak hesaplar ve harcamalar kontrol edilmeli, aylık kontrolü (ekstre) beklenmemelidir.

7. Bilgisayarda güncel bir virüs koruma programı olmasına dikkat edilmeli ve belirli periyotlarla virüslere karşı bilgisayarlar taratılmalıdır. Bunun dışında virüs programının engelleyemeyeceği veya bulup yok edemeyeceği bazı casus programlar ve virüsçükler olabilir. Bunlar; solucanlar (worm), casus (spy) yazılımlar, trojanlar, vs.'dir. Bu tarz casus program ve virüsçükleri etkisiz hale getirmek için özel olarak hazırlanmış olan programlardan faydalanılmalıdır.

8. Bilgisayarın güvenlik duvarı (firewall) her zaman aktif ve güncel tutulmalıdır. İnternet bankacılık işlemleri güvenliğinden emin olunmayan bilgisayarlardan yapılmamalıdır. Bu amaçla internet kafe gibi halka açık yerlerdeki bilgisayarları kullanmaktan kaçınılmalıdır. Bu gibi alanlarda İnternet Bankacılığı kullanmak mecburiyetinde kalınırsa her zaman sanal klavye

kullanılmalı ve İnternet bankacılığında çıktıktan sonra bilgisayardaki geçici internet dosyalarını temizlenmelidir. (Temporary İnternet Files)

9. Genelde İnternet Bankacılığına giriş sanal klavye ile 2 şekilde hazırlanır. Birincisi harf ve rakamların üzerine tıklayarak giriş, diğeri ise harf ve rakamların üzerinde bekleyerek (fotoğraf çekerek) giriştir.

10. Bankalar tarafından verilen veya müşterinin belirlemiş olduğu kullanıcı adı, şifre, parola gibi bilgiler kimseyle paylaşılmamalı ve bir yere not edilmemeli ve tahmin edilebilir sayı veya kelimelerden oluşturulmamalıdır.

11. İnternet bankacılığına girişte şifre veya parola yazarken veya güvenlik sorunuzun cevabının sorulduğu yerlerde sanal klavye kullanmaya özen gösterilmeli ve yazılan rakam ve numaraların " * " olarak gözüktüğünden emin olunmalıdır.

12. İnternet Bankacılığı girişten sonra gelen ilk sayfada son işlem tarihi ve son başarısız şifre/parola giriş tarihi bilgileri kontrol edilmelidir.

13. İnternet Bankacılığı işlem yaparken bilgisayarın başından ayrılmamalı ve işlemlerin bittiğinde, çıkmak için bankanın belirlediği yerden oturumu kapatılmalıdır.

4.2.7 İnternet Explorer ve Güvenlik

İnternette gezinti yapmak, bilgisayarınızın fiziksel olarak internet ortamı ile temasa geçmesi olarak açıklanabilir. Bu durumda her zaman bilgisayarınıza ve kayıtlı bilgilerinize dışarıdan ulaşılma olasılığı vardır. İnternette güvenlik, size gönderilen ve sizin dışarıya gönderdiğiniz bilgilerin güvenli bir şekilde aktarılabilmesi ve alınabilmesinden ibarettir.

Bilgisayarınızı zararlı içeriklerden korumanın anlamı, ziyaret ettiğiniz sitelerdeki zararlı içeriği etkisiz kılmak veya en azından bir tehde karşı sizi uyarmaktır. Tarayıcınızda farklı güvenlik seviyeleri tanımlayabilirsiniz. Bu güvenlik alanları sayesinde aktif içerik kullanımı ve güvendiğiniz sitelerden dosya indirme konusunda problem yaşamazsınız ve kesintisiz olarak internette gezinebilirsiniz.

Bazı web sitelerini ziyaret ettiğinizde sizin hakkınızda bilgi toplar ve bu bilgileri bilgisayarınızda bir text dosyasında tutarlar. Bu dosyalara çerezler (cookie) denir. Bu dosya, sizin hangi siteleri ziyaret ettiğiniz ve bu sitelerde doldurduğunuz formlardaki bilgilerden oluşur.

Çerezler virüs yaymak için kullanılamazlar. Ancak siz bu tür bilgilerin bilgisayarınızda tutulmasını istemiyor olabilirsiniz. Bunun yanında internette dolaştığınız sürece bazı gereksiz dosyalar geçici internet dosyaları(temporary internet files) bilgisayarınızda depolanmaya başlar. Bu dosya ve çerezleri silbilmek için: Araçlar (Tools) altındaki İnternet Seçenekleri (İnternet Options) penceresinden Genel (General) yolundan; Çerezleri Sil (Delete Cookies), Tüm Dosyaları Sil (Delete All) altından Tüm Çevrimdışı İçeriği Sil (Delete All Offline Content) kutucuğu işaretlenip Tamam (Ok) onaylandığı zaman temizleme işlemini gerçekleştirebilirsiniz.

Ayrıca, ziyaret ettiğiniz web sitelerinde var olan çerez kullanımını güvenlik ayarları vasıtasıyla kontrol edebilirsiniz. Güvenlik ayarlarınızı Araçlar (Tools) altındaki İnternet Seçenekleri (İnternet Options) penceresinden Gizlilik (Privacy) ve Güvenlik (Security) seçeneklerinden ayarlayabilirsiniz. Bu ayarların en azından orta (medium) seviyesinde tutulması lazım olup düşürülmesi önerilmemektedir.

İnternet kullanırken karşılaşılabileceğiniz bazı güvenlik açıklarını kapatmak ve bilgisayarınıza gelebilecek saldırılara karşı sisteminizi koruyabilmek için bazı yardımcı programların sisteminizde kurulu olması gerekmektedir. Bu programlar; sayesinde virüs veya virüsçüklerden etkili bir şekilde korunmuş olursunuz fakat şunu unutmamalısınız ki, hiçbir program %100 güvenlik sağlamamaktadır. Asıl amaç riskleri en aza indirebilmek olmalıdır. Bu bağlamda virüs programınız aktif ve güncel olmalı, güvenlik duvarınız (firewall) sürekli aktif durumda kalmalıdır.

4.3 Sonuç

Bu bölümde dolandırıcılık işlerini yapanların bu işleri ne gibi yollarla yaptığını ve bunlardan kaçınmanın yolları anlatılmıştır. Tez kapsamında incelediğimiz İnternet Bankacılığında oluşabilecek dolandırıcılık işlemleri bu anlatılan yöntemlerle yapılmaktadır. Bu tez çalışmasında amaçlanan yukarıdaki kurallara uyulması halinde bile gerçekleştirilen dolandırıcılık işlemlerinin önüne geçebilmektir.

5 DOLANDIRICILIK

Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamak amacıyla yapılan hareketlere dolandırıcılık denir.

5.1 Bilişim Dolandırıcılığı

Gelişen teknolojiler akıl almaz bir hızla ilerleyerek insan hayatını her geçen gün biraz daha kolaylaştırmaktadır. Bilgisayar ve iletişim teknolojilerindeki gelişmeler günümüzde insanlık tarihi açısından çok önemli bir devrim olarak kabul edilmekte hatta sanayi devrimi ile mukayese edilmektedir. Eğitimden ticarete, devlet sektöründen özel sektöre, eğlenceden alış-verişe kadar bir çok alanda klasikleşmiş anlayışları değiştirmiş ve insanlara yeni bir anlayış yeni bir hayat tarzı kazandırmıştır. Bununla birlikte insanın bulunduğu her yerde suça rastlanıldığı gibi bu alanda da yeni suç tipleri ortaya çıkmış ve suçlular da teknolojinin getirdiği yenilik ve kolaylıkları kullanmaya başlamıştır. Günümüzde bilgisayar kavramı sadece hayatımızı kolaylaştıran bir devrim olmaktan çıkmış suç kavramı ile birlikte anılan bir araç haline de gelmiştir.

(Abagnale,2001)Dolandırıcılığın artmasına, internet gibi teknolojik gelişmelerin dolandırıcılık işlemlerini daha da kolay hale getirmesi , suçlulara daha az cezanın verilmesi ve toplumda bu gibi kişilere kötü gözle bakılmaması neden olmuştur.

Bu tür suçlar özellikle dijital ortamdaki değerlere yapılan saldırılardır ve genellikle bankalardaki finans kayıtları, hastane kayıtları, askeri bilgiler v.b. bu saldırılara maruz kalma potansiyeli taşımaktadır. Bilgisayar üzerinden daha ucuz ve kolay suç işleme olanağı ileride bu suç tipleri ile daha çok karşılaşacağımız ve bildiğimiz klasik suç tiplerinin; hırsızlık, soygun, terörizm, sabotaj, kaçakçılık ve bir çoğunun dijital ortamda yerini alacağı anlamına gelmektedir. Hatta ülkeler arasındaki sanayi, teknoloji ve strateji casusluğu dijital ortamda yapılmakta ve ülkeler bundan dolayı büyük zararlara uğratılabilmektedir. Bununla birlikte banka hırsızları artık klasik yöntemler yerine iletişim sistemlerini kullanarak bankalardaki hesap kayıtlarını rahatça değiştirilebilmektedirler.

5.1.1 Bilişim Suçlarının Kapsamı, Tanımlamaları ve Sınıflandırılması

Suçlarda teknolojinin kullanılması kaçınılmazdır. Bir bilgisayar, internet uzayı, bir kredi kartı, elektronik bir cihaz veya cep telefonu ile de bu suçlar işlenebilmektedir. Bu yüzden bilgisayar suçlarının kapsamı çok geniştir. Tanımlamalar da bu yüzden hep değişik olmuştur. En basit tabiriyle bilgisayar suçları olarak tanımlayabildiğimiz gibi; siber suçlar, dijital suçlar, İnternet suçları, bilişim suçları, ileri teknoloji suçları vs. tanımlamaları ile de karşılaşmaktayız. Diğer ülkelerde yapılan tanımlarda ise; Computer Crimes, Cyber Crimes, IT Crimes(Information Technologies – Bilgi Teknolojileri), Crime of Networks vb. aslında tüm bunlar ile bu suçların bir kısmı tanımlanması yapılmaktadır. Ancak türkçemize bilişim teknolojileri suçları olarak geçen IT crime (Information Technologies) bu suçların alanı açısından tanım olarak daha iyi uymaktadır. Bu yüzden daha kısa ve yalın bir ifade ile “Bilişim Suçları” olarak kullanılması daha uygun olacaktır.

Bilişim Suçları kapsamına giren suçların tanımlanması ve sınıflandırılmasının yapılması daha sonra yapılacak çalışmalara hazırlık teşkil edecek ve her bir suç tipi daha rahat anlaşılabilir olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken “suçun işlenmesindeki amaç” olmalıdır. Bu tür suçlar hangi yöntemle işleniyor olsa da, hangi amaca hizmet ettiğine bakmak lazımdır. Örneğin; bir bilgisayar sistemine girmek için bir çok yöntem bulunabilir; bir virüs veya trojan kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Ancak burada amacın “sisteme girme” eylemi olduğuna dikkat etmek lazımdır. Burada kullanılan yöntemler ancak suçun ağırlaştırıcı sebeplerini oluşturabilir. Mesela bir sisteme girerken başka sistemlere de sızmış olması gibi. Aşağıda tanımlanması yapılan suç tipleri gerek Avrupa Birliği, gerek Avrupa Konseyi ve gerekse diğer Avrupa ülkelerince yapılan tanımlamaların ülkemize uyarlanmış halidir. Benzer tanımlamalarla İngilizce tabirleri ile karşılaşmak mümkündür. “Unauthorized Acces, Computer Sabotage, Computer Fraud” gibi. Bu suç tiplerine bakacak olursak;

5.1.2 Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme

Anayasamızda belirtilen “Özel Hayatın Gizliliği” maddesine aykırı olarak teknolojik dinlemelerin yapıldığına güncel olarak karşılaşmaktayız. Günümüzde daha modern bir yapıya ulaşan iletişim kavramı artık bilgisayarlar üzerinden yapılmakta ve hatta kişilere ait önemli bilgiler bu ortamda iletilebilmektedir. Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerini tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır. Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır. İşte bu noktada gizlilik gerektiren bilgilere yetkilisi haricinde yapılan erişimler bu suç tipine girmektedir. Erişim haricinde haberleşme amacıyla kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de aynı şekilde değerlendirilmektedir. İletişimin dinlenmesi; sadece bilgisayar başındaki iki kişinin birbiri ile görüşmesi olarak düşünülmemelidir. Birbirine bilgi gönderen ve uyum içinde çalışan bilgisayarların ağ içinde göndermiş oldukları bilgilerin dinlenmesi de dinleme olarak değerlendirilmelidir.

5.1.3 Bilgisayar Sabotajı

Bilgisayar sabotajı yetkisiz erişimin ikinci safhası olarak değerlendirilebilir. Çünkü; yetkisiz erişimde bulunan birisi sadece pasif bir davranışta bulunup özel hayatın gizliliğini bozmuş olur. Ancak bilgisayar sabotajı erişimden sonra elde ettiği bilgilerin silinmesini ve değiştirilmesini içerir. Bu suç tipi iki şekilde karşımıza çıkmaktadır. Birincisi; yine bilgisayar teknolojileri kullanılarak erişilen bilgilerin silinmesi, yok edilmesi ve değiştirilmesidir. İkincisi ise bilgisayar teknolojileri kullanılmadan direk olarak bilgilerin tutulduğu bilgisayarı ve/veya bilgisayarları fiziksel olarak zarara uğratmaktır. Burada önemli olan mala karşı değil de, bilgisayarın içindeki bilgilere karşı yapılmış bir hareket olarak algılamak lazımdır. Çünkü bu bilgiler bilgisayarın kendisinden daha değerli olabilir.

5.1.4 Bilgisayar Yoluyla Dolandırıcılık

Klasik olarak bildiğimiz ve karşılaştığımız dolandırıcılık suçunun bilgisayar ve iletişim ortamları üzerinden yapıyor olmasıdır. Bilgisayar yoluyla dolandırıcılık en çok kredi kartlarının kullanımıyla yapılmaktadır. Bunun için üretilmiş birçok “(Kart Üretici)Cart Generator” programı bulunmaktadır. Bunlar sayesinde internet üzerinden alışveriş yapılırken, istenilen kredi kartı şirketi için mantıksal olarak olası kredi kartı bilgileri üretilmekte ve bu olaydan kredi kartı sahibinin haberi bile olmamaktadır. Bununla beraber yine finans bilgilerinin tutulduğu programlarda yapılan değişiklikler ile istenilen kişinin hesabına istenildiği kadar para aktarılması yapılabilmektedir.

5.1.5 Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Fikir ve Sanat Eserleri Kanununda eser olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılmasıdır. Bilgisayar yazılımları satın alınırken üzerinde gelen lisans sözleşmesine göre bir yazılımın bir adet kopyası ancak satın alan şahıs tarafından yapılacağı ve bu yazılımın başka bir kişi tarafından kopyalanmayacağı ve kiralanmayacağı belirtilmektedir. Bir çok yazılım şirketinin yazılım korsanlığına karşı hukuki işlemlerini yürüten BSA'nın (Business Software Alliance, Kurumsal Yazılım Anlaşması) verdiği rakamlara göre ülkemizde lisanssız yazılım kullanımının %80'lerin üzerinde olduğu belirtilmektedir.

5.1.6 Yasadışı Yayınlar

Yasadışı yayınlar karşımıza üç şekilde çıkmaktadır. Bunlardan birincisi; vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet sayfalarıdır. Özellikle terör örgütleri tarafından hazırlanan bu sayfalarda Türkiye içerisinde yayınlamadıkları bölücü fikirlerini internet ortamında çok rahat teşhir edebilmektedirler. Bununla birlikte; halkın ar ve haya duygularını incitecek şekilde genel ahlaka aykırı pornografik görüntüler içeren internet sayfaları da yayınlanabilmektedir. Yurtdışındaki diğer ülkelerde genel itibarıyla çocuk pornografisi üzerine yoğunlaşmış ve ona göre çalışmalar yapılmıştır. Ülkemizde ise; çocuk veya büyük pornografisi şeklinde bir ayırım yapılmadığından bütün pornografik yayınlar yasaklanmış durumdadır. İnternet sayfaları ile işlenebilecek diğer bir suç türü ise; bir kişiye karşı yapılan hakaret ve sövme suçudur.

Hukuki açıdan bakıldığında adı geçen suç tiplerini iki şekilde kategorize edebiliriz. Aşağıdaki tabloda da gösterildiği şekliyle birincisi; geleneksel suçların bilgisayar yolu ile işlenmesi, diğeri ise yeni teknolojiler ile birlikte ortaya çıkan suç tipleridir.

Hukuki Olarak	Suç Tipi	Kanundaki Yeri
Geleneksel Suçların Bilgisayar Yoluyla İşlenmesi	Bilgisayar Yoluyla Dolandırıcılık	TCK 503-507 : Dolandırıcılık ve İflas
	Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı	5846'nolu Fikir ve Sanat Eserleri Kanunu (FSEK)
	Yasadışı Yayınlar	<ul style="list-style-type: none"> ■TCK 125-200 : Devletin Şahsiyetine karşı cürümler ■TCK 480-490 : Hakaret ve Sövme Cürümleri ■TCK 426-427 : Halkın ar ve haya duygularını inciten veya cinsi arzuları tahrik eden ve istismar eder nitelikte genel ahlaka aykırı: ve diğer anlatım araç ve gereçleri
Teknolojinin İlerlemesi ile Ortaya Çıkan Suç Tipleri	Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme	TCK 525 a,b,c ve d “Bilişim Alanında Suçlar Babı”
	Bilgisayar Sabotajı	

Tabloda da görüldüğü gibi her suç tipinin hukukumuzda karşılığı bulunmaktadır. Teknolojinin ilerlemesi ile ortaya çıkan suçların hukukumuzdaki karşılığı 1991 yılında TCK’ a eklenen 525-a,b,c,d maddeleri ile yapılmıştır. Ancak teknolojinin hızla ilerlemesiyle birlikte suçlarda hızla ilerleyecek ve yeni suç tipleri ile karşılaşılacaktır. Suçların teknik olarak engellenmesinin mümkün olmayacağı bu noktada; teknolojik suçlarla mücadelede hukukun tartışılmaz üstünlüğü ortaya çıkmaktadır. Bu yüzden en iyi çözüm hukuki bazda yapılacak değişimlerdir.

Ayrıca bu suçlardan bazıları takibi şikayete bağlı suçlar olup mağdur olanların bizzat şikayette bulunmaları gerekmektedir. Ancak; Türkiye’de bakıldığında buradaki mağdurların bu konuda nasıl bir müracaatta bulunacaklarını ve hangi kanunlarla korunduklarını bilemediklerinden kendi yöntemleri ile mağduriyetlerini giderme cihetine gitmektedirler. Bunlar ise; genel itibariyle “sen benim bilgilerimi sildin bende seninkileri silerim” türünden davranışlar olmaktadır.

5.1.7 Yaşanan Problemler ve Çözüm Yöntemleri

Görüldüğü üzere suç tipleri tanımlanmış ve bu suç tiplerinin kanunlarımızda karşılığı bulunmaktadır. Mücadelede yaşanan problemler ve problemlerin çözüm yöntemleri aşağıda açıklanmıştır.

5.1.7.1 Elde Edilen Delillerin Hukuki Durumu

Suçluların bulunmasında en etkili yöntem delillerin toplanmasıdır. Toplanan her delil soruşturma süresince polise ışık tutacak ve mahkeme aşamasında önemli sonuçlar ortaya koyacaktır. Bilgisayar suçlarında delil niteliği teşkil eden bilgiler ise; yine bilgisayar ortamında tutulmuş olan kayıtların olacağı da aşikardır. Bu kayıtların delil niteliği teşkil edebilmesi için sağlam ve değiştirilemez bir yapıya sahip olması gerekmektedir. Ancak bilgisayarın kullanıcısı tarafından belirlenen yöntemlerle kaydedilen bilgiler yine bilgisayarın kullanıcısı tarafından değiştirilebilme ihtimali taşımaktadır. Böyle olunca sağlam bir delil olmaktan çıkmaktadır. Kanunlarımızda faks çıktıları dahi delil olarak nitelendirilmediği göz önünde bulundurulacak olursa, bilgisayar kayıtlarının ne kadar delil teşkil edip etmeyeceği gözükecektir. Bilişim Suçlarında delil niteliği olan sadece bu kayıtlı bilgiler olduğundan dijital delillerin hukuki durumu tartışılması en önemli konulardan biri olmalıdır.

5.1.7.2 Delillerin Elde Edilmesi

Ülkemizde dijital kayıtların delil niteliğinin düzenlenmiş olduğunu varsayacak olursak, bu sefer delillerin elde edilmesi problemi karşımıza çıkmaktadır. İnternete bağlanmak için ya bulunduğunuz kurumun bilgisayar ağına bağlı olmanız, ya bir İnternet Servis Sağlayıcıdan hizmet almanız veya bir İnternet kafeye gitmeniz gerekmektedir. Tabi bilgisayar üzerinden bir suç işlemeniz içinde bu yerlerden servis olarak internete bağlanmanız gerekir. Böyle olunca suçu işleyen kişiye ait bilgiler sadece buralardan bulunabilir. Ancak ülkemizdeki İnternet Servis Sağlayıcıları ve özellikle de İnternet kafeler düzenli kayıt tutma işleminin masraflı olmasından dolayı bu sistemleri kurmamaktadırlar. Bu yüzden emniyet tarafından takip edilen bir soruşturma da kayıtların elde edilmesi aşamasında problem yaşamaktadır. Bu da; suçların yaygınlaşmasında önemli bir rol oynamaktadır. Bu yüzden bu türden internet servisi veren yerlere en kısa zamanda devlet tarafından belli standartların getirilmesi ve bu konuda sorumluluklar verilmesi gerekmektedir.

5.1.7.3 Uluslararası Polis İşbirliği

Ülkemizde gerek delillerin hukuki niteliği, gerekse de İnternet Servis Sağlayıcılardan delillerin elde edilmesi konusunda her türlü düzenleme yapılmış olsa da, uluslararası polis işbirliğine gidilmeden sağlıklı bir sonuç elde edilmesi afaki kalacaktır. Çünkü; özellikle internet üzerinde işlenen suçlarda birden fazla geçiş noktası bulunabilmektedir. Bu noktalarda genelde birden fazla ülke üzerinde bulunabilmektedir. Böyle olunca bir olayın soruşturmasında olayın yurt dışındaki bir servis sağlayıcı üzerinden yapıldığı bulunursa ilgili ülke polis teşkilatı ile irtibata geçip gerekli bilgilerin elde edilebilmesi gerekmektedir. Aksi takdirde olayın soruşturması bir noktadan sonra kesilecektir. Bu amaçla ülkeler bu konuda aralarında ikili polis işbirliğine gitmelidir.

5.1.7.4 Uluslararası Suçun Tanımlanması

Şu ana kadar sayılan tüm problemler halledilmiş olsa da, eğer soruşturmadaki bir suç diğer ülkede suç niteliği teşkil etmiyorsa o ülkeden gerekli bilgiler alınamayacaktır. Bu amaçla İnterpol, Avrupa Birliği ve Avrupa Konseyinde uluslararası suçun tanımının yapılmasına dair çalışmalar bulunmaktadır. Ülkemizde de bu çalışmalar özenle takip edilmeli ve kanunlarımızdaki eksiklikler giderilmeye çalışılmalıdır.

Bilişim Suçları olgusu teknolojiyi kullanan ve kullanacak bütün ülkelerin ortak problemi haline gelmiş ve özellikle A.B.D ve Avrupa ülkelerinde bu alandaki hukuki ve idari yapılanmaların düzenlenmesi için birçok çalışmalar başlatılmıştır. Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde milli sınırları aşmış, bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmıştır. Teknolojik gelişmeler ile globalleşen dünyamızda; tüm ülkelerin işbirliği ile bu tip suçlara karşı mücadele etme gereği ortaya çıkmıştır.

5.2 Sonuç

Gerçek hayatta güncel olarak rastladığımız suç tiplerini artık dijital ortamda da sıkça görmekteyiz. Pornografik ve yasadışı yayınlar, kredi kartı dolandırıcılığı, telif hakları ile korunan bilgisayar yazılımlarının kopyalanması v.b. suç tipleri İnternet ve özellikle bilgisayarlar üzerinde aktüel olarak işlenmektedir. Ayrıca yüksek teknoloji suçları bilinen suç tiplerinden farklılık arz etmektedir. Bu yüzden bu tip suçlara polisler ve suçun soruşturulması esnasında görevli olan herkes daha farklı yaklaşmalıdır. Çünkü elektronik cihazlar, bilgisayarlar ve diğer yüksek teknoloji ürünleri kullanılarak daha kolay ve ucuz suç işlenebilmektedir. Bu da; ileride bu suçlar ile daha çok karşılaşacağımız anlamına gelmektedir. Bu yüzden Türkiye'nin bilişim suçları üzerine ciddi olarak eğilmesi gerekmektedir.

Bu bölümde belirtilen suçlar kapsamına İnternet Bankacılığı suçları da girmektedir. Tez kapsamında bu konun anlatılması ile işlenen suçun cezası ve takip edilebilirliği araştırılmıştır. Yapılan para transferi eğer Dolandırıcılık Tespit Sisteminde suçlu olarak görülüyorsa işlem iptal edilecek ve eldeki verilerle(hesap numarası,IP bilgisi vs.) dolandırıcılık yapan kişilere ulaşılabilecektir.

6 VERİ MADENCİLİĞİ

6.1 Giriş

Bu bölümde veri madenciliğinden, veri tabanında bilgi keşfinden, kısaca veri madenciliği algoritmalarından, veri madenciliği ön veri işlemeden ve veri madenciliğinde karşılaşılan sorunlardan bahsedilecektir.

Bilgisayar teknolojisi gün geçtikçe daha ucuz ve daha hızlı olmaya başlıyor (Alpaydın, 1999). Eskiye nazaran daha hızlı ve daha fazla veri saklayabilir hale geliyor. Bunun yanında bilgisayar ağlarındaki ilerleme ile bu veriye başka bilgisayarlardan da hızla ulaşabilmek mümkün olabilmektedir. Bilgisayarların daha ucuza elde edilmesi ile ona olan istek ve kullanım yaygınlaşıyor. Veri doğrudan sayısal olarak toplanıyor ve saklanıyor. Bunun sonucu olarak da ayrıntılı ve doğru bilgiye ulaşabiliyoruz.

Önceden süper marketlerde basit dört işlem yapan kasalar mevcuttu. Müşterinin yaptığı alış veriş işlemlerinde sadece toplam tutarı gösteriyordu. Ancak şuan bu kasaların yerine satış noktası terminalleri konularak müşteri hareketlerinin detayları saklanabilmektedir. Saklanan bu binlerce malın ve binlerce müşterinin hareket bilgileri sayesinde her malın zaman içindeki hareketlerine ve eğer müşteriler bir müşteri numarası ile kodlanmışsa bir müşterinin zaman içindeki verilerine ulaşmak ve analiz etmek mümkün olabilmektedir. Bütün bunlar marketlerde kullanılan barkot, bilgisayar destekli veri toplama ve işleme cihazları sayesinde mümkün olmaktadır.

Market, ticari, tıp, askeri, iletişim, vb. birçok alanda benzer teknolojilerin kullanılması ile veri hacminin yaklaşık olarak her yirmi ayda iki katına çıktığı tahmin edilmektedir (Frawley, 1991).

Verilerin çokluğunun ve incelenmesinin en zor olduğu açıkça görülen kurum NASA olmaktadır (Fayyad, 2000). NASA'nın kullandığı uyduların sadece birinden, bir günde terabayt'larca veri gelmektedir.

Veri tek başına bir anlam ifade etmez fakat, bu veri bir amaca yönelik üzerinde işlem yapılırsa bilgi olur. Verinin, bilgiye dönüştürülmesine bilgi keşfi denir. Bu tanımda keşif sözcüğünün kullanılmasının amacı, gizli olan ve daha önceden bilinmeyen örüntülerin bulunmasından kaynaklanmaktadır. Bilgi, bir soruya yanıt vermek için veriden çıkardığımız anlam olarak da tanımlanabilir. Veri sadece sayılar veya harfler değildir; veri, sayı ve harfler ve onların anlamıdır. Veri hakkındaki bu veriye üst veri diyoruz.

Veri hacminin hangi boyutlara ulaşabileceği ve bunların işlenmesinin ne kadar güç olduğu kolayca anlaşılabilir. Süper market örneği incelendiğinde, veri analizi yaparak her mal için bir sonraki ayın satış tahminleri çıkarılabilir; müşteriler satın aldıkları mallara bağlı olarak gruplanabilir; yeni bir ürün için potansiyel müşteriler belirlenebilir; müşterilerin zaman içindeki hareketleri incelenerek onların davranışları ile ilgili tahminler yapılabilir. Binlerce malın ve müşterinin olabileceği düşünülürse bu analizin gözle ve elle yapılamayacağı, otomatik olarak yapılmasının gerektiği ortaya çıkar. Veri madenciliği burada devreye girer:

Veri madenciliği büyük miktarda veri içinden gelecekle ilgili tahmin yapmamızı sağlayacak bağıntı ve kuralların bilgisayar programları kullanarak aranmasıdır.

Geleceğin, en azından yakın geleceğin, geçmişten çok fazla farklı olmayacağını varsayarsak geçmiş veriden çıkarılmış olan kurallar gelecekte de geçerli olacak ve ilerisi için doğru tahmin yapmamızı sağlayacaktır.

Büyük miktarlarda verinin VT'lerde tutulduğu bilindiğine göre bu verilerin VM teknikleriyle işlenmesine de veri tabanında bilgi keşfi denir (VTBK). Büyük hacimli olan ve genelde veri ambarlarında tutulan verilerin işlenmesi yeni kuşak araç ve tekniklerle mümkün olabilmektedir. Bundan dolayı bu konularda yapılan çalışmalar güncelliğini korumaktadır. Bazı kaynaklara göre; VTBK daha geniş bir disiplin olarak görülmektedir ve VM terimi sadece bilgi keşfi (BK) metotlarıyla uğraşan VTBK sürecinde yer alan bir adımdır (Fayyad et al., 1996a) Prof. Dr. Usama Fayyad'a göre VTBK sürecinde yer alan adımlar şu şekilde sıralanmaktadır (Fayyad et al., 1996b):

- 1. Veri Seçimi:** Bu adım veri kümelerinden problemin çözümüne yönelik verilerin seçimidir. Sonuçta eğitim kümesi oluşur.
- 2. Veri Temizleme ve Ön işleme:** Oluşan eğitim kümesinde yer alan hatalı kayıtların silindiği ve eksik nitelik değerlerinin değiştirildiği kısımdır. İşlem sonucunda verinin kalitesi artar.
- 3. Veri İndirgeme :** Verilere bu işlemler yapılarak kullanılan veri madenciliği sorgusunun çalışma zamanını iyileştirilir.
- 4. Veri Madenciliği:** VM sorgularının(sınıflandırma,kümeleme, eşleştirme, vb.) oluşan veri üzerine uygulanması aşamasıdır.
- 5. Yorumlama:** Yukarıdaki tüm işlemlerden sonra oluşan verinin geçerlilik,yenilik,yararlılık ve basitlik açısından yorumladığı kısımdır.

VM için yapılan diğer tanımlardan bazıları da şunlardır:

1. VM, büyük veri kümesi içinde saklı olan genel örüntülerin bulunmasıdır.(Holsheimer ve Siebes, 1994).
2. VM, önceden bilinmeyen ve potansiyel olarak faydalı olabilecek, veri içindeki gizli bilgilerin çıkarılmasıdır (Frawley et al., 1991).

VMÇS'ni oluşturan diğer disiplinlerle VTBK arasındaki ilişki izleyen bölümde anlatılacaktır.

6.4 VTBK ile Makine Öğrenimi Arasındaki İlişki

Makine öğrenmesi, VTBK'de yoğun biçimde kullanılmaktadır. Kullanım sebepleri ise; örneklerden öğrenme, düzenli örüntülerin keşfi, gürültülü ve eksik verilerin öğrenilmesi sayılabilir.

VTBK'nın makine öğreniminden en büyük farkı aşağıda sıralanmıştır:

- VTBK veri ambarları gibi çok büyük veri kümeleriyle çalışabilir.
- VTBK gerçek yaşamda oluşan büyük veriler üzerinde araştırma yapmaktadır.

Veri görselleştirmede kullanılan yöntemler, VTBK sistemi ile elde edilen örüntülerin, kullanıcıya grafikler aracılığıyla sunumunu sağlar.

6.5 VTBK ile İstatistik Arasındaki İlişki

İstatistik ile VTBK arasında oluşan ilişki veri modelleme ve verideki gürültüyü azaltmadan kaynaklanmaktadır. İstatistiğin VTBK'de kullanılan tekniklerinden bazıları aşağıda sıralanmıştır:

- Özellik seçimi (Corinna, 1995),
- Veri bağımlılığı (Zhong and Ohsuga, 1994; Shapiro and Matheus, 1992),
- Veri özeti (Shapiro and Matheus, 1992),
- Eksik değerlerin tahmini (Elder-IV and D. Pregibon, 1995),
- Sürekli değerlerin ayrımı (Zhong and Ohsuga, 1994; Fayyad and Irani, 1993), vb.

6.6 VM ile Veri Tabanı Arasındaki İlişki

VT eldeki verileri VM sorgularına giriş değeri olarak tutmaktadır. VM faydalanacağı sorgular VT üzerinden çalıştırılmaktadır. Özellikle ilişkilendirme sorgusunda fazla miktarda VT sorgusu yapmak gerekmektedir.

VM, VT'den farklıdır, çünkü VT'de bir keşfetme olayı yoktur var olanlar üzerinde sorgular çalıştırılmaktadır ama VM'deki sorgular genelde keşfe dayalı ve ortada olmayan örüntüleri keşfetmeye dayalıdır.

6.7 Veri Madenciliğinde Karşılaşılan Problemler

Yukarıda MÖ ile VM arasındaki farklar VM'nin büyük ve gerçek veriler ile çalışması olduğu belirtilmiştir. Bunun böyle olması beraberinde bir çok problemi de getirmiştir. Bu gerçek veriler üzerinde eksik, boş değerli ,gürültülü, artık ve dinamik veriler oluşabilir. Bunun

sonucunda sistem yanlış çalışabilir. Bundan dolayı bu problemlerin çözümlenmesi gerekmektedir.

6.7.1 Veri Tabanı Boyutu

Veri tabanı boyutu bazı uygulamalarda yavaş , NASA örneğinde olduğu gibi de büyük boyutlara ulaşmaktadır (Fayyad et al., 2000). VT'de yer alan veriler ,yatay ve dikey olarak artmaktadır :

- Yatay Boyut: VT'de yer alan nesnelere özellik(veri tabanına yeni bir alan vs eklenmesi) sayılarıyla genişlemektedir.
- Dikey Boyut: Bu boyutta nesnelere yer alan kayıtlar adet olarak genişlemektedir.

Bu şekilde verilerin artmasıyla bunların işlenmesinde bir çok sorunu da beraberinde getirmektedir. Bu sorunlara farklı çözümlerin bazıları :

- Eğitim kümesinin yatay ve dikey boyutta indirgenmesi,
 - o Yatay indirgeme: Nitelik değerleri genelleştirilerek var olan nitelik değeri bu genelleştirilen değere göre günlendir. Mükerrer kayıtlar çıkarılır yani artık bir niteliğin değer sayısı mesela gün 24 saat ile ifade edilirken 3 parçaya bölünüp eski değerler bunlara göre günlenebilir.
 - o Dikey indirgeme: Artık niteliklerin indirgenmesi işlemidir.
- VM yöntemleri sezgisel/buluşsal bir yaklaşımla arama uzayını taramalıdır, vb.

Eğitim kümesinin geniş olması bulunacak örüntülerin kalitesi açısından çok faydalı olmasına rağmen, bu büyük kümeyle uğraşma zorluğu da o kadar artmaktadır.

6.7.2 Gürültülü Veri

Veri girişi veya veri toplanması esnasında oluşan sistem dışı hatalara gürültü denir. Ölçümden kaynaklanan hatalar ,veri toplanması esnasında oluşan hatalar kategorisine girmektedir. Bu hataların sonucu olarak VT'de birçok niteliğin değeri yanlış olabilir. Günümüz ticari ilişkisel veri tabanları bu tür hataların ele alınması için az bir destek sunmaktadır. Hatalı verilere sahip gerçek dünya verilerinde VM işlemleri yapmak ciddi bir problemdir. Bu sebepten dolayı VM tekniklerinin gürültülü verilere karşı daha az duyarlı olması gerekir.

Sistemin gürültülü veriye daha az duyarlı olmasında belirtilmek istenen, sistem tarafından gürültülü verilerin belirlenip, ihmal edilmesidir.

(Chan ve Wong,1991), gürültünün tespit edilmesi için istatistiksel yöntemler kullanmıştır. Sınıflama üzerinde bir çok çalışmalar yaptığı bilinen Quinlan'nın gürültünün sınıflama üzerine dezavantajları konusunda yaptığı çalışmada; denetimli öğrenmede denetim üzerindeki gürültünün öğrenme algoritmasının performansını doğrudan etkileyerek düşürdüğünü tespit etmiştir (Quinlan, 1986).

6.7.3 Boş Değerler

VT'de boş değer birincil anahtar ve boş olmaması önceden istenen veriler dışında her alanda olabilir. Boş değerın genel tanımını, kendisi de dahil olmak üzere hiç bir değere eşit olmayan değer demektir. Eğer VT'de bir nitelik değeri boşsa o nitelik bilinmeyen ve uygulanamaz bir değere sahiptir.

Bir uygulama için VT tasarlanırken genel yapılar kurulmaya çalışır. Mesela oluşturulan bilgisayar isimli tablo her tür bilgisayarın kayıtlını alabilecek durumda olmalıdır; eğer bilgisayarın ses kartı yoksa oraya boş değer girilebilmelidir.

Veri kümelerinde var olan boş değerleri için çeşitli çözümler söz konusudur (Quinlan, 1986):

- Boş değerli kayıtlar işlemde göz ardı edilebilir,
- Boş değerli kayıtlar istenen bir değerle değiştirilebilir. Bu değiştirme için çeşitli yöntemler söz konusudur:
 - Boş değer yerine o nitelikteki en fazla frekansa sahip bir değer veya ortalama bir değer konulabilir,
 - Boş değer yerine varsayılan bir değer konulabilir,
 - Boş değerın bulunduğu kaydın diğer özelliklerine göre, boş değerın kendine en yakın değerle günlenmesi sağlanabilir, vb.

6.7.4 Eksik Veri

VM işlemlerini gerçekleştirebilmek ve istenen problemin çözümüne ulaşabilmek için gereken eğitim kümesindeki yatay ve dikey boyutların eksik olmaması gerekir. Bu boyuttaki eksiklikler şu şekilde olabilir:

- Yatay boyutta: Yatay boyuttaki eksiklik, eğitim kümesinde olması gereken nitelik veya niteliklerin olmamasıdır. Örneğin: eğer insanların yaşlarıyla alakalı bir hastalığın neye bağlı olduğu bulunmaya çalışılıyorsa, niteliklerden yaş bilgilerinin tanımlı olması gerekir(kolon bazında yaş diye bir kolonun olması) bulunması gerekir.
- Dikey boyutta: Dikey boyuttaki eksiklik eğitim kümesindeki kayıtların eksik olmasıdır. Örneğin bir süper markette yaş 25 ve 30 yaşındaki kişiler her yaptıkları alışverişte bir ürünü sürekli alıyorsa, bu örüntünün keşfedilmesi için eğitim kümesinde yeterli sayıda 25-30 yaş aralığına giren kayıtların bulunması gerekir. Eğer eğitim kümesinde bu kayıtlara yer verilmezse bununla ilgili gerçek dünya örüntüsü bulunamaz.

6.7.5 Artık Veri

Artık veri, problemin çözümünde hiç kullanılmayan eğitim kümesi içerisindeki veridir.

Artık nitelikleri bulmak için kullanılan algoritmalar, özellik seçimi olarak adlandırılır. Özellik seçimi arama uzayını küçültür ve sınıflama işleminin kalitesini de artırır (Deogun et al., 1995; Kira and Rendeli, 1992; Almuallim and Dietterich, 1991; Pawlak, 1986).

6.7.6 Dinamik Veri

Her an veri girişi yapılan veri tabanlarıdır. Bunlara örnek İnternet Bankacılığı çevrimiçi veri tabanları gösterilebilir. Bir veri tabanındaki içeriğin sürekli değişmesi VM uygulamalarının uygulanabilmesine önemli ölçüde zorlaştırıcı etki yapmaktadır. Bu sorunlardan bazıları şunlardır:

- Ortaya çıkan VM örüntülerinin sürekli değişim halinde olan verilerden hangisini ifade ettiğinin tespitinin zorluğu ve bu üretilen sonuçların zaman içinde eski üretilen sonuçlardan farkının tespiti ve gereken yerlerin güncellenmesi zorluğu,

- VM algoritmalarının çalışabilmesi için verilerin üzerine okuma kilidi konulması gerektiğinden, bu verilerin başka uygulamalar tarafından değişime açık olmaması ve uygulamaların çalışmasını engellemesi,

- VM algoritmalarının ve çevrimiçi VT uygulamalarının aynı anda uygulanmasından kaynaklanan ciddi performans düşüşlerinin olması, vb.

6.8 Veri Madenciliği Algoritmaları

Veri madenciliği algoritmaları verilerde var olan gizli bilgiyi ortaya çıkartmaya yarayan metotlardır.

Veri madenciliği algoritmaları genel olarak iki ana gruba ayrılır (Simoudis, 1996):

Doğrulamaya dayalı algoritmalar; kullanıcı tarafından ispatlanmak istenen bir hipotez ortaya sürülür ve VM algoritmalarıyla bu hipotez ispatlanmaya çalışılır. Çok boyutlu analizlerde ve istatistiksel analizlerde tercih edilen metottur. Hipotez testi buna güzel bir örnektir.

Keşfe dayalı algoritmalarda herhangi bir ispatlanmak istenen bir hipotez yoktur. VT keşfedici olarak araştırılarak , gizli olan bilgiler açığa çıkarılır. Doğrulamaya dayalı algoritmaların tersine bu algoritmalarda ortada ispatlanması istenen hipotezler yoktur. Tam tersine bu algoritmalar otomatik keşfe dayanmaktadır. Keşfe dayalı algoritmaların birçok kullanım alanı vardır: istisnai durumların keşfi, karar ağacı, kümeleme gibi algoritmalar bu yaklaşıma göre kurulmuştur.

VM algoritmalarından önemli olanlarına değinilecektir.

6.8.1 Hipotez Testi

Hipotez testi algoritmaları doğrulamaya dayalı algoritmalarıdır. Doğrulanacak hipotez VT üzerindeki verilerle belli doğruluk ve destek değerlerine göre sınılanır. mesela X ve Y birer mantıksal ifade olmak üzere eğer X ise Y'dir, ifadesi VT'de araştırılır.

Sınama işlemi uzman tarafından aşağıdaki ihtiyaçlardan dolayı yapılır:

- Bir varsayımın; kural olarak ortaya çıkarılmak istendiğinde,
- Ortaya çıkarılmış bir kuralın budanması veya genişletilmesinde.

6.8.2 Sınıflama Algoritması

Sınıf olmak için her kaydın belli ortak özellikleri olması gerekir. Ortak özelliklere sahip olan kayıtların hangi özellikleriyle bu sınıfa girdiğini belirleyen algoritma, sınıflama algoritmasıdır.

Sınıflama algoritması, denetimli öğrenme kategorisine giren bir öğrenme biçimidir. Denetimli öğrenme, öğrenme ve test verilerinin hem girdi hem de çıktığı içerecek şekilde olan verileri kullanmasıdır.

Sınıflama sorgusuyla, bir kaydın önceden belirlenmiş bir sınıfa girmesi amaçlanmaktadır (Weiss and Kulikowski, 1991). Bir kaydın önceden belirlenmiş bir gruba girebilmesi için sınıflama algoritması ile öğrenme verileri kullanılarak hangi sınıfların var olduğu ve bu sınıflara girmek için bir kaydın hangi özelliklere sahip olması gerektiği otomatik olarak keşfedilir. Test verileriyle de bu öğrenmenin testi yapılarak ortaya çıkan kurallar optimum sayısına getirilir.

Sınıflama algoritmasının kullanım alanları sigorta risk analizi, banka kredi kartı sınıflaması, sahtecilik tespiti, vb. alanlardır.

6.8.3 Kümeleme Algoritması

Kümeleme algoritması denetimsiz öğrenme kategorisine giren bir algoritmadır. Kümeleme algoritmasındaki amaç verileri alt kümelere ayırmaktır (Michalski and Stepp, 1983). Sınıflama algoritmasında olduğu gibi ortak özellikleri olan veriler bir kümeye girer. Alt kümelere ayrılmak için keşfedilen kurallar yardımıyla bir kaydın hangi alt kümeye girdiği kümeleme algoritması sayesinde bulunur.

Kümeleme algoritması genelde astronomi, nüfus bilimi, bankacılık uygulamaları, vb. uygulamalarda kullanılır.

6.8.4 İlişkilendirme Algoritması

İlişkilendirme algoritması denetimsiz öğrenme kategorisine giren bir algoritmadır. Eşleştirme algoritması sınıflama algoritmasının benzeridir (Seidman, 2000). Sınıflama algoritmaları ile eşleştirme algoritmaları arasındaki fark, eşleştirmede sınıflandırmada olduğu

gibi bir sınıfa sokulması amaçlanmaz. Eşleştirmedeki amaç eğitim kümesindeki nesnelere nitelikleri arasındaki ilişkilerin saptanmasıdır.

Nitelikler arasındaki bütün kombinasyonlar çıkarılarak bütün niteliklerin farklı kombinasyonlarındaki farklı değerleri deneyerek örüntüler keşfedilmeye çalışılır (Agrawal et al., 1993). Bu, ilişkilendirme algoritmasının sınıflandırma algoritmasından farklıdır. Her bir ilişkilendirme kuralı farklı ifadeleri verecek şekilde ortaya çıkar.

6.8.5 Zaman Serileri Arasındaki Bağımlılıklar

Zaman serilerindeki örüntü belli bir periyotta, belli bir sıklıkta gerçekleşen olaylardır. Belli frekansla tekrarlanan bu olaylar zaman serileriyle yapılan VM algoritmaları sayesinde keşfedilir. Örneğin, müşteriler e-ticarette yazın yazlık ürünlere, kışın da kışlık ürünlere rağbet gösteriyorsa bu 6 ay periyotla tekrarlanan bir örüntüdür. Bu örüntüye göre stok bilgilerini o dönem periyotlarına göre ayarlayabilirler.

6.8.6 Sıra Örüntüleri

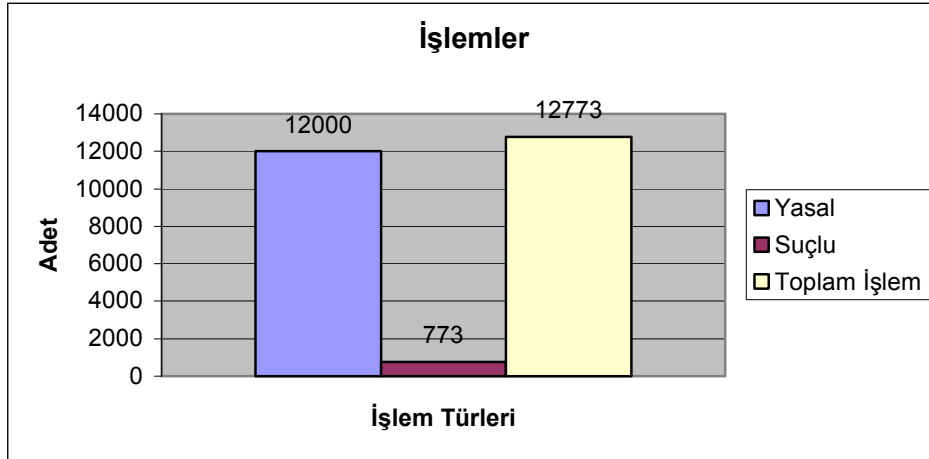
Ardışık örüntü keşfi, bir zaman aralığında sıklıkla gerçekleşen olaylar kümelerini bulmayı amaçlar (Agrawal ve Sri kant, 1995). Bir ardışık örüntü örneği şöyle olabilir: Bir yıl içinde A yazarının "X" romanını satın alan insanların %70'i B yazarının "Y" adlı kitabını da satın almıştır. Bu tip örüntüler perakende satış, telekomünikasyon ve tıp alanlarında yoğun biçimde kullanılmaktadır.

6.9 Sonuç

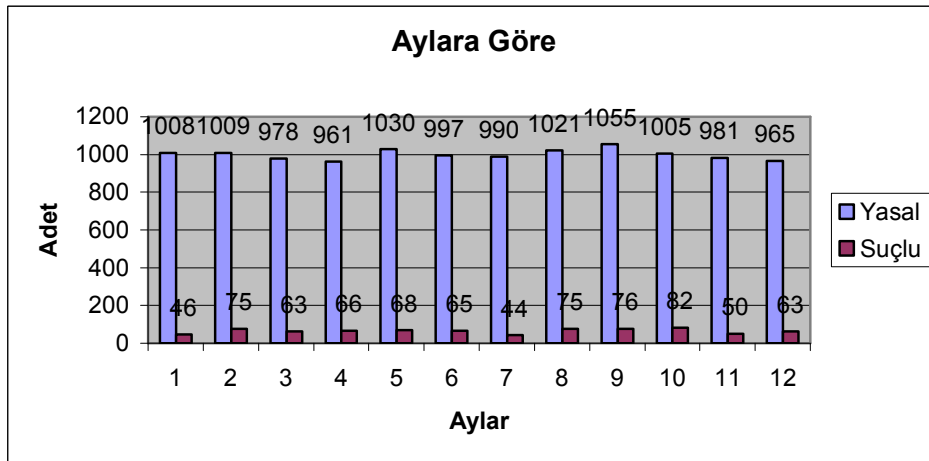
Bu bölümde VM ile ilgili genel bir bilgi verilmiştir. Tez kapsamında, bu bölümde anlatılan VM algoritmalarından sınıflandırma ve kümeleme algoritmaları, Dolandırıcılık Tespit Sisteminde kullanılmıştır.

7 TEZ KAPSAMINDA KULLANILAN VERİLER

İnternet Bankacılığında olması gereken özellikler de dikkate alınarak veriler sanal olarak üretilmiştir. İnternet Bankacılığında 01/01/2004 ile 01/01/2007 tarihleri arasındaki 571 adet müşteriye ait 12773 adet parasal işlem incelemeye alınmıştır. 12773 işlemden 12000 'ü yasal , 773 tanesi suçludur.

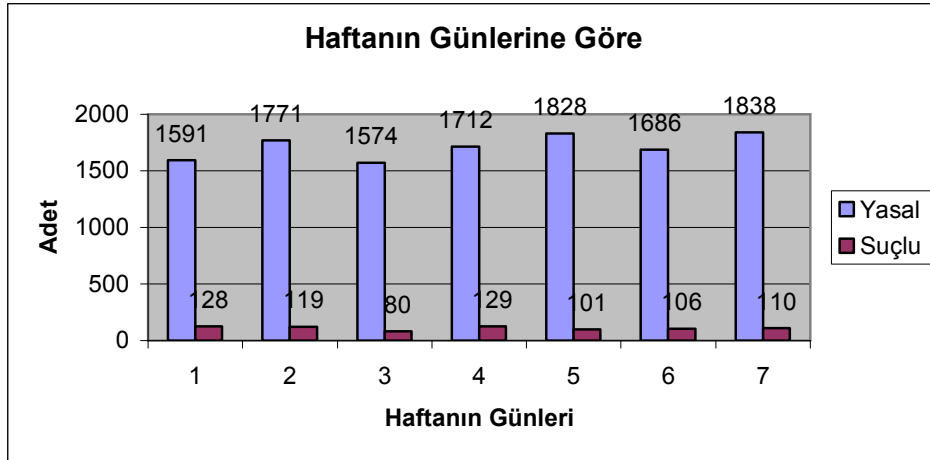


7.1 Aylara Göre Yasal ve Suçlu Oranları



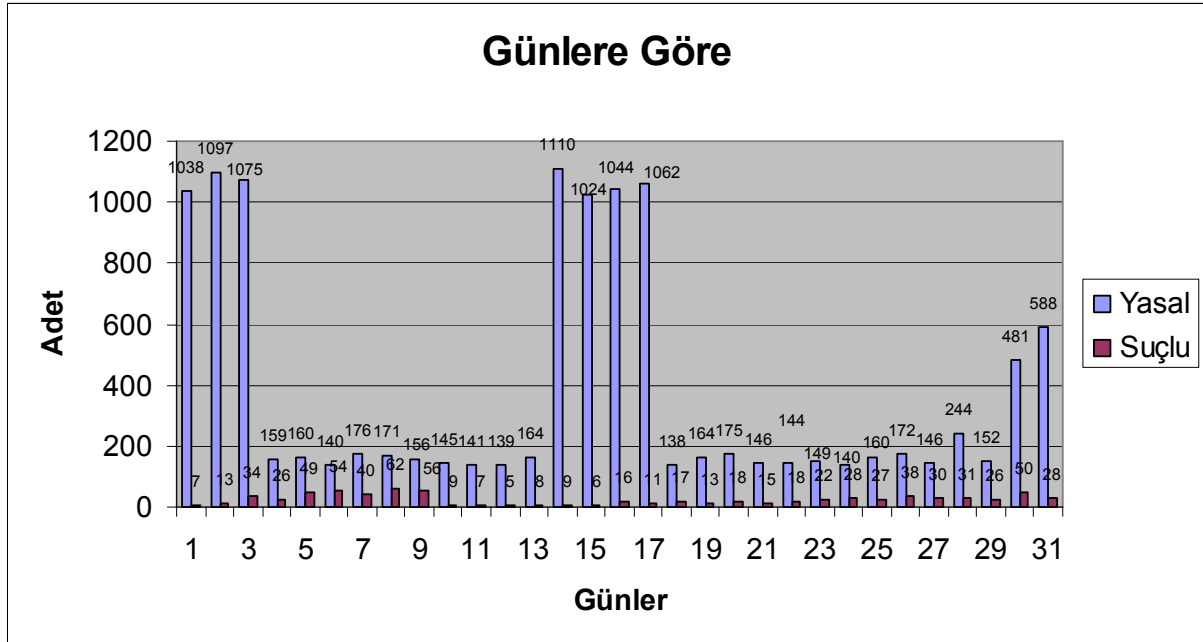
Aylar rakam olarak sıralanmıştır. Ocak(1), şubat(2) , mart(3) , nisan(4), mayıs(5), haziran(6) , temmuz(7), ağustos(8), eylül(9), ekim(10), kasım(11) , aralık(12). Ocak ayından başlayıp aralık ayına kadar yapılan yasal ve suçlu işlem miktarını göstermektedir. Burada aylara yaklaşık olarak yapılan yasal ve suçlu işlemleri aynı miktardadır.

7.2 Haftanın Günlerine Göre Yasal ve Suçlu Oranları



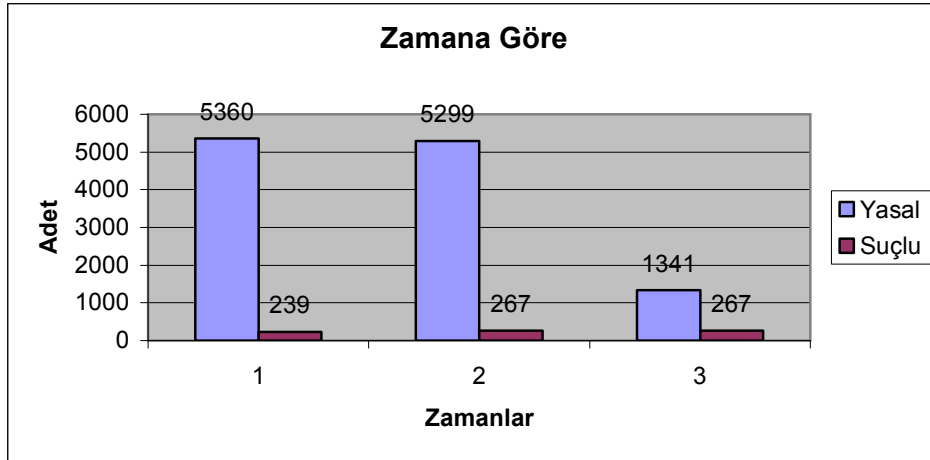
Günler rakam olarak sıralanmıştır. Pazartesi(1), salı(2),çarşamba(3),perşembe(4), cuma(5), cumartesi(6),pazar(7). Pazartesi gününden başlayıp pazar gününe kadar yapılan yasal ve suçlu işlem miktarını göstermektedir. Burada günlere göre yaklaşık olarak yapılan yasal ve suçlu işlemleri aynı miktardadır.

7.3 Günlere Göre Yasal ve Suçlu Oranları



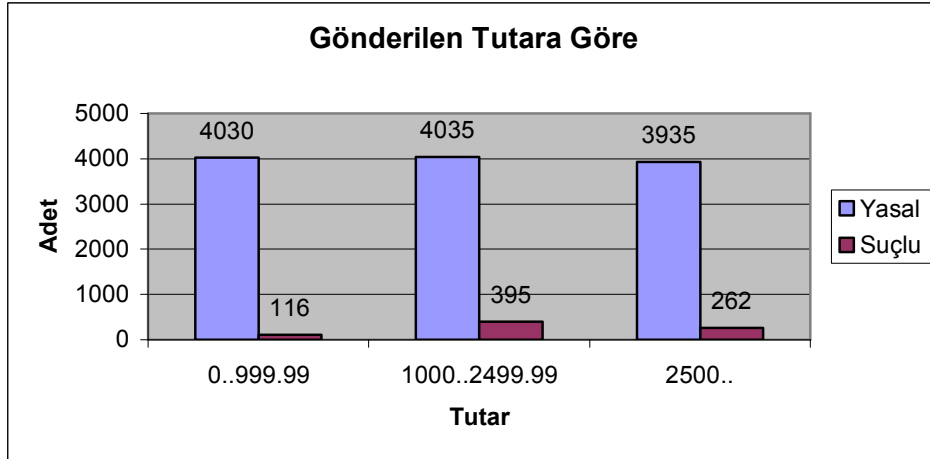
Ayın 1. gününden başlayıp ayın 31. gününe kadar yapılan yasal ve suçlu işlem miktarını göstermektedir. Burada günlere göre yaklaşık olarak yapılan yasal işlemler 1-3 , 14-17,30-31 arasındaki günlerde diğer günlere göre çok işlem yapılmaktadır.

7.4 Zamana Göre Yasal ve Suçlu Oranları



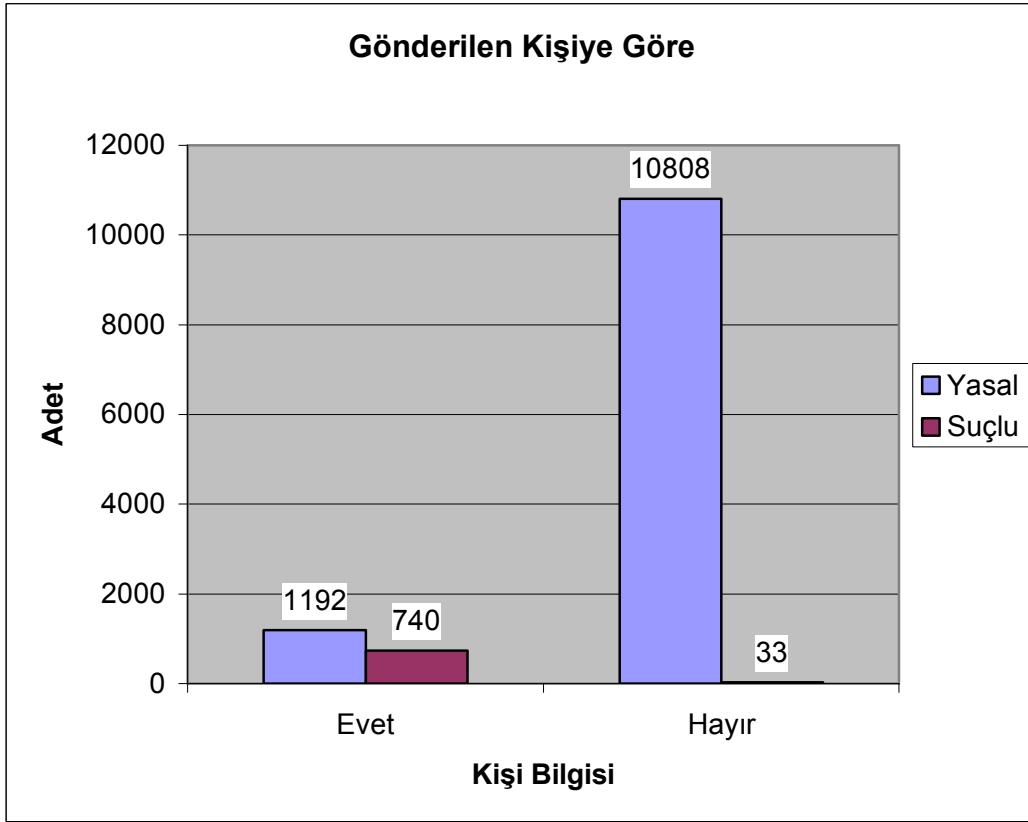
Gün içindeki para transfer saatleri gruplandırılmıştır. Zaman1 saat 08:00:00 ile 13:59:59, zaman2 saat 14:00:00 ile 19:59:59 ve zaman3 saat 20:00:00 ile 07:59:59 arasındadır. Bu saat aralıklarının bölünmesi suçlu ve yasal işlemlerin zaman bilgilerine göre belirlenmiştir. Yasal veriler genel de zaman1 ile zaman2 aralıklarında daha çok gerçekleşirken, suçlu kayıtlar her zaman diliminde hemen hemen aynı oranda gerçekleşmiştir.

7.5 Gönderilen Tutarı Göre Yasal ve Suçlu Oranları



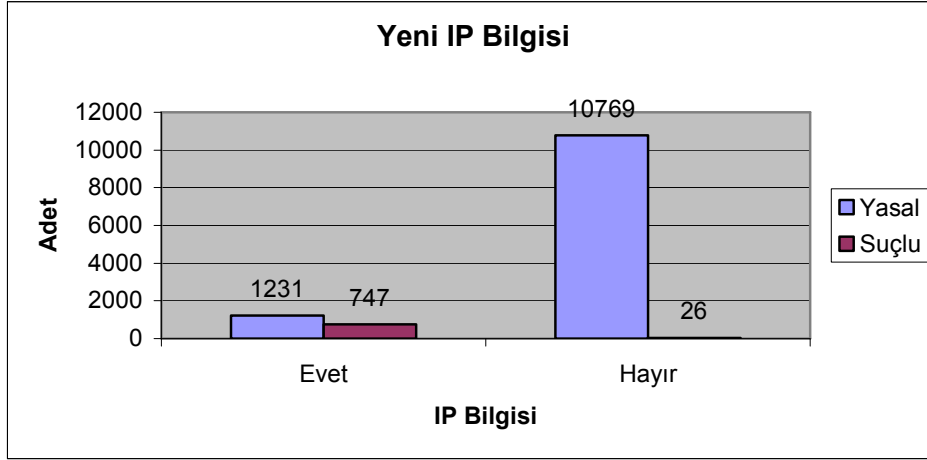
Yasal ve yasadışı olarak gönderilen miktarlar 3 gruba ayrılmıştır. Bunlar sırası ile 0 ile 999.99 YTL, 1000 ile 2499.99 YTL ve 2500 YTL den fazla olmak üzere 3 gruptur. YTL dışında yapılan diğer para birimleri YTL'ye çevrilmiştir. Suçlu kayıtlardan en fazlası 1000 ile 2499.99 YTL arasında para transferi yapılan kayıtlardır. En az ise 1000 YTL'den az para transferi yapılan kayıtlar gelmektedir.

7.6 Gönderilen Kişiyeye Göre Yasal ve Suçlu Oranları



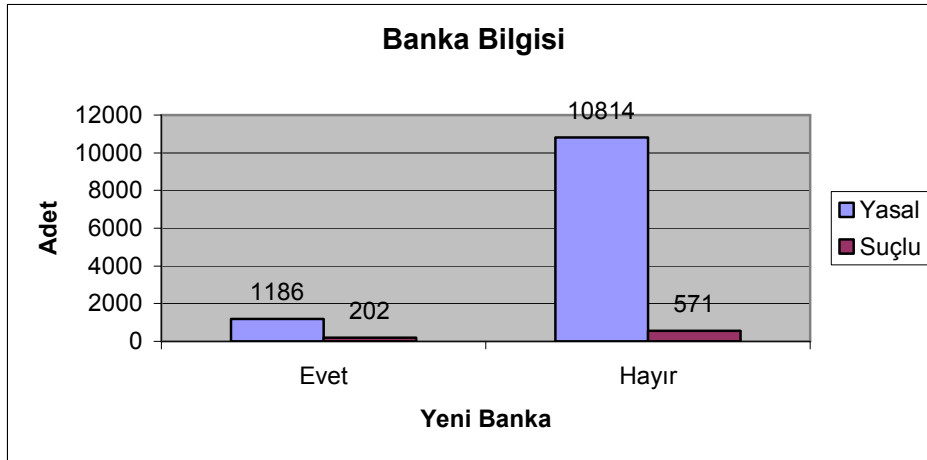
Müşterinin yeni bir kişiyeye(daha önceden para transferi yapılmamış) para transferi yapıp yapmadığını belirtmektedir. Yasal kayıtlarda yeni bir kişiyeye gönderim az iken suçluda tam aksine daha fazladır.

7.7 Gönderilen IP'ye Göre Yasal ve Suçlu Oranları



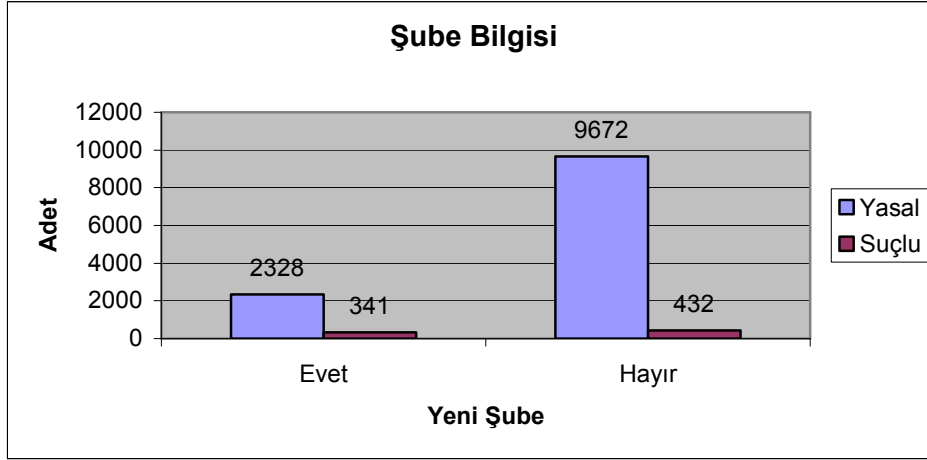
Müşterinin yeni bir IP numarasından para transferi yapıp yapmadığını belirtmektedir. Yasal kayıtlarda yeni bir IP numarasından gönderim az iken suçluda aksine daha fazladır.

7.8 Gönderilen Bankaya Göre Yasal ve Suçlu Oranları



Müşterinin yeni bir bankaya para transferi yapıp yapmadığını belirtmektedir. Yasal kayıtlarda yeni bir bankaya gönderim azdır.

7.9 Gönderilen Şubeye Göre Yasal ve Suçlu Oranları



Müşterinin yeni bir şubeye para transferi yapıp yapmadığını belirtmektedir. Yasal kayıtlarda yeni bir şubeye gönderim azdır.

7.10 Sonuç

Bu bölümde tez kapsamında kullanılan veriler hakkında grafiksel olarak bilgiler verilmiştir. Bu veriler Dolandırıcılık Tespit Sistemine giriş olarak kullanılmıştır. Bu verilerin işlenmesi sonucunda oluşan sonuçlar ilerleyen bölümde anlatılacaktır.

8 MATERYAL VE YÖNTEM

8.1 Materyal

Uygun test ortamını oluşturabilmek için veritabanı, java kurulu bilgisayar ve gerekli yazılımlar gereklidir.

Veritabanı olarak Oracle veritabanı seçilmiştir. Oluşturulan veya işlenen veriler buraya aktarılmıştır. Uygulama ise Java1.4 ile geliştirilmiştir. Geliştirme editörü olarak IntelliJ IDEA kullanılmıştır.

8.2 Yöntem

Bu bölümde, tez kapsamında kullanılan veri madenciliği metotları anlatılmıştır .

8.2.1 Tez Kapsamında Kullanılan Veri Madenciliği Algoritmaları

Burada tez kapsamında kullanılan Veri Madenciliği algoritmalarından Karar Ağaçları ve Saf Bayes Sınıflandırıcı anlatılacaktır.

8.2.1.1 Karar Ağaçları

Karar Ağaçları, verileri belli nitelik değerlerine göre sınıflandırmaya yarar. Bunun için algoritmaya girdi olarak verilerin belirlenen belli nitelikleri, çıktı olarak da verilerin belli bir niteliği verilir ve algoritma bu çıktı niteliğindeki değerlere ulaşmak için hangi girdi nitelik değerlerinin olması gerektiğini ağaç veri yapıları kullanarak keşfeder.

Karar ağacı, gürültülü veride etkili çalışır ve sınıfların ayırıcı özelliklerini keşfeder. Karar ağacı algoritmalarını bir probleme uygulayabilmek için aşağıdaki koşulların sağlanması gerekir.

1. Olayların özelliklerle ifade edilebilmesi gerekir. Nesnelerin belli sayıda özellik değerleriyle ifade edilebilmesi gerekir. Örneğin; soğuk, sıcak,...vb.

2. Sınıfları belirleyebilmek için gereken ayırıcı özelliklerin olması gerekir.

Karar Ağaçları makine öğrenme tekniğidir, bağımlı ve bağımsız özelliklerin kümesini gösterir, ağaç şeklinde yapıyla karar kümelerini oluşturur(Witten and frank,1999).Karar ağaçları akış şemasına benzer ağaç yapılarıdır. Her bir nitelik bir düğüm tarafından temsil edilir. Dallar ve yapraklar ağaç yapısının elemanlarıdır. En son yapı yaprak, en üst yapı kök ve bunların arasında kalan yapılar ise dal olarak adlandırılır Karar ağaçları sınıflandırma algoritmalarını uygulayabilmek için uygun bir yapıdır.

8.2.1.1.1 ID3 ve C4.5 Karar Ağaçlarının Kurulması

Karar ağaçları olarak da adlandırılan ID3 ve C4.5 algoritmaları, sınıflandırma modellerini işlemek için (Quinlan ,1993) tarafından geliştirilmiştir. C4.5, ID3'ün geliştirilmiş halidir. C4.5 eksik nitelik değerlerini ele alabilmekte, karar ağacının budanması ve kural çıkarımı gibi işlemleri yapabilmektedir. Karar ağacının kurulması için kullanılacak girdi olarak bir dizi kayıt verilirse bu kayıtlardan her biri aynı yapıda olan birtakım nitelik/değer çiftlerinden oluşur. Bu niteliklerden biri kaydın hedefini belirtir. Problem, hedef-olmayan nitelikler kullanılarak hedef nitelik değerini doğru kestiren bir karar ağacı belirlemektir. Hedef nitelik çoğunlukla sadece {evet, hayır}, veya {başarılı, başarısız} gibi ikili değerler alır. Örnek : Golf oynamak isteyen kişiler için hava koşulları kayıtlarıyla ilgilenilsin. Hedef nitelik olan golf oynama durumu iki değer alabilsin. Bunlar oynanabilir ve oynanamaz olsun. Tablo 8.2'deki veriler bu örnek için verilmiş nitelik ve bunların alabileceği olası değerler olsun.

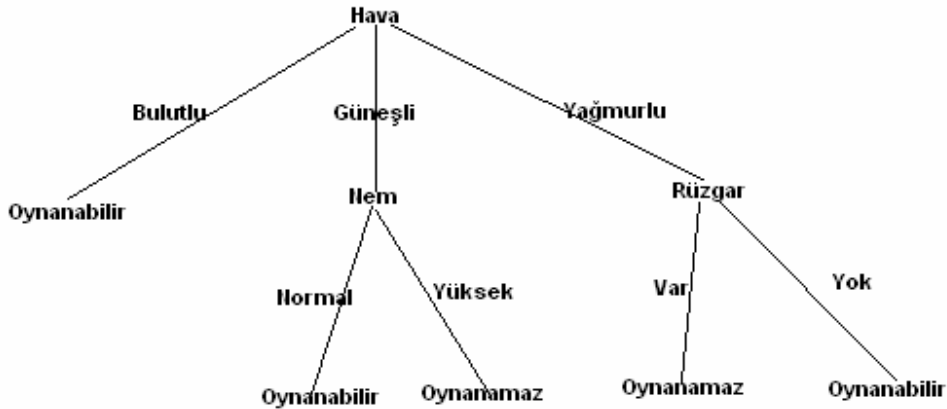
Nitelik	Olası Değerler
Hava durumu	Güneşli, Bulutlu , Yağmurlu
Sıcaklık	Sıcak,Normal,Soğuk
Nem	Yüksek,Normal
Rüzgar	Var , Yok

Tablo 8.2 Golf örneği için hedef-olmayan nitelikler

Hava durumu	Sıcaklık	Nem	Rüzgar	Golf oynama durumu
Güneşli	Sıcak	Yüksek	Yok	Oynanamaz
Güneşli	Sıcak	Yüksek	Var	Oynanamaz
Bulutlu	Sıcak	Yüksek	Yok	Oynanabilir
Yağmurlu	Normal	Yüksek	Yok	Oynanabilir
Yağmurlu	Soğuk	Normal	Yok	Oynanabilir
Yağmurlu	Soğuk	Normal	Var	Oynanamaz
Bulutlu	Soğuk	Normal	Var	Oynanabilir
Güneşli	Normal	Yüksek	Yok	Oynanamaz
Güneşli	Soğu	Normal	Yok	Oynanabilir
Yağmurlu	Normal	Normal	Yok	Oynanabilir
Güneşli	Normal	Normal	Var	Oynanabilir
Bulutlu	Normal	Yüksek	Var	Oynanabilir
Bulutlu	Sıcak	Normal	Yok	Oynanabilir
Yağmurlu	Normal	Yüksek	Var	Oynanamaz

Tablo 8.3 eğitim verileri

Tablo 8.2 'deki nitelikler ve hedef nitelikle tablo 8.3'deki eğitim verileri kullanıldığında ortaya şekil 8.1 deki karar ağacı çıkar.



Şekil 8.1 Golf örneği için oluşan karar ağacı

Bir karar ağacı ne bildiğimizi (örn., öğrenme verisi) özetlediği için değil, yeni durumların sınıflamasını doğru yaptığı için önemlidir. Sınıflandırma modelleri kurarken hem model kurmak için öğrenme verisi hem de ne kadar iyi çalıştığını belirlemek için test verisi olmalıdır.

8.2.1.1.1 ID3'ün Temeli

Karar ağacında, her bir düğüm hedef-olmayan bir niteliğe, düğümler arasındaki her yay (arc) ise niteliğin olası bir değerine karşılık gelir. Ağacın bir yaprağı, bu yapraktan köke kadar ki yolda tanımlanan kayıtlar için hedef niteliklerin beklenen değerini belirler.

Karar ağacında her bir düğüm kökten başlayarak yol üzerinde henüz dikkate alınmamış olan nitelikler arasından en çok bilgi sağlayan hedef-olmayan nitelikle ilişkilendirilebilir. Bu “İyi” bir karar ağacının nasıl olduğunu gösterir.

Entropi bir düğümün ne kadar bilgi verici olduğunu ölçmede kullanılır. Bu “İyi” ile ne kastedildiğini belirtir. Bu kavram Claude Shannon tarafından ilk kez Bilgi Teorisi içinde tanımlanmıştır.

8.2.1.1.1.2 Tanımlamalar

n tane eşit olasılığa sahip mesaj varsa, her birinin olasılığı $p = 1/n$ ve her mesajın taşıdığı bilgi $-\log(p) = \log(n)$ dir. Burada logaritma iki tabanlıdır. Örneğin, 16 mesaj varsa, $\log(16) = 4$ 'tür ve bu her mesajı ifade etmek için 4 bite ihtiyaç var demektir.

Genelleme yapılacak olursa, olasılık dağılımı $P = (p_1, p_2, \dots, p_n)$ ise, bu dağılımla taşınan bilgi P'nin Entropisi yada ortalama bilgisi olarak anılır.

$$P\text{'nin Entropisi} = I(P) = - (p_1 * \log(p_1) + p_2 * \log(p_2) + \dots + p_n * \log(p_n))$$

Örneğin;

$$P = (0.5, 0.5) \text{ ise } I(P) = 1,$$

$$P = (0.67, 0.33) \text{ ise } I(P) = 0.92,$$

$$P = (1, 0) \text{ ise } I(P) = 0 \text{ 'dır.}$$

Bu örnekten de anlaşılacağı üzere olasılık dağılımı ne kadar homojen olursa, kaynağın entropisi de o oranda artmaktadır. Eğer kayıt kümesi (T), hedef niteliklerin değerleri üzerinden C_1, C_2, \dots, C_k sınıflarına ayrıldığında, bir elemanın sınıfının belirlenmesi için gerekli bilgi $\text{Bilgi}(T) = I(P)$ olur. Burada P, C_1, C_2, \dots, C_k bölmelerin olasılık dağılımıdır:

$$P = (|C_1|/|T|, |C_2|/|T|, \dots, |C_k|/|T|)$$

$$\text{Verilen golf örneği için bilgi: } \text{Bilgi}(T) = I(9/14, 5/14) = 0.94$$

$$\text{Stok market örneği için ise } \text{Bilgi}(T) = I(5/10, 5/10) = 1.00 \text{ şeklindedir.}$$

T , hedef-olmayan özellik X 'in değerine dayalı olarak, T_1, T_2, \dots, T_n dizinlerine bölümlenirse, T 'nin bir elemanının sınıfını belirlemek için gerekli bilgi, T_i 'nin bir elemanın sınıfın belirlenmesinde gerekli bilginin ortalama ağırlığı olur.

Örn.; $\text{Bilgi}(T_i)$ 'nin ortalama ağırlığı:

$$\text{Bilgi}(X, T) = \sum_{i=1}^n \frac{|T_i|}{|T|} \text{Info}(T_i)$$

Golf örneğinde, 'Hava durumu' niteliği için,

$$\text{Bilgi}(\text{Hava durumu}, T) = 5/14 \cdot I(2/5, 3/5) + 4/14 \cdot I(4/4, 0) + 5/14 \cdot I(3/5, 2/5) = 0.694$$

Kazanç (Gain): Bir T elemanını tanımak için gereken bilgi ile X özelliği de kullanılarak T elemanını tanımak için gereken bilgi arasındaki farktır. Bu aynı zamanda , X özelliğine dayalı bilgi kazancı olarak adlandırılır.

$$\text{Kazanç (X,T)} = \text{Bilgi(T)} - \text{Bilgi (X, T)}$$

Golf örneğindeki hava durumu ve rüzgar özelliği için kazanç:

$$\begin{aligned} \text{Kazanç (Hava durumu,T)} &= \text{Bilgi(T)} - \text{Bilgi(Hava durumu, T)} \\ &= 0.94 - 0.694 = 0.246 \end{aligned}$$

$$\text{Kazanç (Rüzgar,T)} = 0.048$$

Buradan hava durumunun rüzgara kıyasla daha fazla bilgi sağladığı söylenebilir. Kazanç nitelikleri sıralamada ve karar ağacının oluşturulmasında kullanılır. Şöyle ki, ağaçta her bir düğüm, kökten başlayarak yol üzerinde henüz dikkate alınmamış nitelikler arasından en büyük kazançlısı seçilerek belirlenir.

Bu düzenlemenin amacı küçük karar ağaçları oluşturmaktır. Böylece bir kayıttın hangi sınıfa girdiği sadece bir kaç sorudan sonra belirlenebilir.

8.2.1.1.3 Kazanç Oranlarının Kullanımı

Örneğin, her bir kayıt için farklı değerleri olan bir D niteliği varsa $\text{Bilgi(D,T)}=0$, bundan dolayı Kazanç(D,T) maksimum demektir. Quinlan (1993), bunu dengelemek için kazanç yerine kazanç oranını kullanmayı önermiştir.

$$\text{KazançOranı(D,T)} = \text{Kazanç(D,T)} / (\text{BilgiBölme(D,T)})$$

BilgiBölme (SplitInfo), D hedef nitelik değerinin temelindeki T'nin bölünmesine dayalı bilgidir. Bu nedenle BilgiBölme(D,T) aşağıdaki gibi tanımlanmıştır.

$$\text{BilgiBölme(D,T)} = I \left(\frac{|T_1|}{|T|}, \frac{|T_2|}{|T|}, \dots, \frac{|T_m|}{|T|} \right)$$

Burada $\{T_1, T_2, \dots, T_m\}$ D değeri tarafından ortaya çıkarılan T'nin bölümleridir.

$$\begin{aligned} \text{Golf örneği için Bilgi Bölme (Hava durumu, T)} &= \\ &= -5/14 * \log(5/14) - 4/14 * \log(4/14) - 5/14 * \log(5/14) = 1.577 \end{aligned}$$

olarak bulunur

$$\text{Hava durumu Kazanç Oranı } 0.246 / 1.577 = 0.156$$

olarak hesaplanır.

$$\text{Bilgi Bölme(Rüzgar, T)} =$$

$$-6/14 * \log(6/14) - 8/14 * \log(8/14) = 6/14 * 0.1.222 + 8/14 * 0.807 = 0.985 \text{ olarak bulunur ve}$$

Rüzgarın KazançOranı $0.048 / 0.985 = 0.049$ olarak hesaplanır.

8.2.1.1.1.4 C4.5 Algoritması

C4.5 ID3 algoritmasının bir uzantısıdır.

Bir karar ağacı kurarken, kazanç hesaplamasıyla eğitim kümesindeki değerler bilinmeden sadece nitelikler bilinerek işlem yapılır.

Bir karar ağacı kullanımında bilinmeyen nitelik değerlerine sahip olan kayıtlar, mümkün olan sonuçların olasılıklarını tahmin ederek sınıflanabilir. Daha önce verilmiş olan golf örneği için, hava durumu güneşli ve nem bilinmiyor koşulu için yeni bir kayıt verilmişse, aşağıdaki süreç sürdürülür:

Hava durumu kök düğümünden nem düğümüne ‘güneşli’ etiketli yay takip edilerek gidilir. Bu noktada eğer nem Normal ise iki tanesi ‘oynanabilir’ olmak üzere iki kayıt vardır, eğer nem Yüksek ise üç tanesi ‘oynanamaz’ olmak üzere üç kayıt vardır. Dolayısıyla, kayıtların olasılıkları oynanabilir ve oynanamaz için sırasıyla 0.4 ve 0.6’dır.

Uygulamamızda C4.5 algoritmasının tercih edilme nedenleri olarak;

- Eksik nitelik değerlerini ele alabilmektedir.
- Karar ağacının budanması ve kural çıkarımı gibi işlemleri yapabilmektedir.
- Yeni durumların sınıflamasını doğru yapabilmektedir.

8.2.1.1.1.5 Karar Ağaçlarının Budanması

Ağacın budanması, bütün bir alt ağacın yerine bir yaprak düğümünün yerleştirilmesiyle yapılır. Yerleştirme ancak bir alt ağaçtaki beklenen hata tek yapraktan daha büyükse ancak yapılır. Örnek: eğer şekil 8.2’de verilen basit karar ağacı; 1 kırmızı başarılı öğrenme kaydı ile 2 mavi başarısız öğrenmeden elde edilir ve sonra Test dizininde 3 kırmızı başarısız ve 1 mavi başarılı bulunursa, şekil 8.2’deki ağaç tek bir Başarısız düğüm ile değiştirilir. Değişimden sonra dört hata yerine yalnızca iki hata yapılmış olunacaktır.

Hedef niteliğin hedef-olmayan bir niteliğe gerçekten bağımlı değilse, hedef-olmayan nitelik karar ağacının geçerli yolunda gözükmeyecektir.

Bir karar ağacından bir kural dizini çıkarmak : kökten yaprağa karar ağacında bulunan her bir yol için bir kural yazılır. Bu kuraldaki sol-taraf, düğümlerin etiketlerinden ve etiketli yaylardan kolayca inşa edilir.



Şekil 8.2 Basit Karar Ağacı

8.2.1.2 Saf Bayes Sınıflandırması

Yaş	Gelir	Öğrenci	Kredi Oranı	Bilgisayar Aldı
<=30	Yüksek	hayır	düşük	hayır
<=30	Yüksek	hayır	yüksek	hayır
31...40	Yüksek	hayır	düşük	evet
>40	Orta	hayır	düşük	evet
>40	düşük	evet	düşük	evet
>40	düşük	evet	yüksek	hayır
31...40	düşük	evet	yüksek	evet
<=30	orta	hayır	düşük	hayır
<=30	düşük	evet	düşük	evet
>40	orta	evet	düşük	evet
<=30	orta	evet	yüksek	evet
31...40	orta	hayır	yüksek	evet
31...40	yüksek	evet	düşük	evet
>40	orta	evet	yüksek	hayır

Tablo 8.4 Saf Bayes Sınıflandırıcı için eğitim örnekleri

“Bayes sınıflandırıcıları nedir?” Bayes sınıflandırıcıları istatistiksel sınıflandırıcılardır. Özel bir sınıfa ait olarak verilen bir olasılık gibi, sınıf üyeliklerine ait olasılıklarını önceden söyleyebilirler.

Sınıflandırma algoritmaları karşılaştırılarak yapılan çalışmalar Saf Bayes Sınıflandırıcı olarak bilinen Saf Bayes Sınıflandırıcıyı bulmuşlardır. Bu sınıflandırıcı karar ağaçları ve yapay sinir ağları sınıflandırıcılar ile karşılaştırılabilecek performans gösterirler. Bunun yanında büyük veri tabanları üzerinde işlem yapan Bayes sınıflandırıcılar yüksek hız ve doğruluk derecesine sahip olduklarını sergilediler.

Saf Bayes, verilen bir sınıf üzerindeki bir özelliğe ait değerlerin etkisinin diğer özelliğe ait değerlerden bağımsız olduğunu farz eder. Bu kabul sınıf koşullu bağımsızlık olarak adlandırılır. Bu ise gerekli hesaplamaları basitleştirir, anlaşılabilirliği kolaylaştırır ve doğal olarak “saf” kelimesi ile ifade edilir.

8.2.1.2.1.1 Bayes Teoremi

X sınıf üyeliği bilinmeyen veri örneği olsun. H ise bu veri örneği X in C sınıfına ait olduğunu öngören bir hipotez olsun.

$$\text{Bayes Teoremi } P(H / X) = \frac{P(X / H)P(H)}{P(X)}, \text{ dir.} \quad (i)$$

Şimdi, Saf Bayes sınıflandırıcı içinde Bayes teoreminin nasıl kullanıldığına bakabiliriz.

8.2.1.2.1.2 Saf Bayes Sınıflandırması

Saf Bayes sınıflandırıcı veya Bayes sınıflandırıcı aşağıdaki gibi çalışır.

1. Her veri örneği n-boyutlu özellik vektörleri ile gösterilir, $X = (x_1, x_2, \dots, x_n)$ her veri örneği n özelliklerden alınan örnek üzerindeki n ölçümler ile tarif edilir, sırasıyla, A_1, A_2, \dots, A_n .

$$P(C_i / X) = \frac{P(X / C_i)P(C_i)}{P(X)}$$

2. $P(C_i) = \frac{s_i}{s}$ olabilmektedir, burada s_i C_i sınıfına ait eğitilen örnek sayısı, ve s ise toplam eğitilen örnek sayısıdır.

3. Bir çok özellik barındıran veri setleri verilirse $P(X / C_i)$ aşırı derece hesap yükü gerektirir. $P(X / C_i)$ işleminde hesap yükünü azaltmak için, sınıf koşul bağımsızlığına ait saf varsayım uygulanır. Bu varsayım, özelliklere ait değerler bir diğerinden şartlı olarak bağımsızdır, örneğe ait verilen sınıf üyeliği, özellikler arasında bağımlılık ilişkisi yoktur.

Bu, $P(X / C_i) = \prod_{k=1}^n P(x_k / C_i)$ Olasılıklar $P(x_1 / C_i), P(x_2 / C_i), \dots, P(x_n / C_i)$ eğitim

örneklerinde tahmin edilebilirler, burada $P(x_k / C_i) = \frac{s_{ik}}{s_i}$ burada s_{ik} A_k için x_k değerine sahip

olan C_i sınıfına ait eğitim seti sayısı ve s_i C_i 'ye ait olan eğitim seti sayısıdır. $P(x_k / C_i) = \frac{s_{ik}}{s_i}$

ifadesinin 0 olmasını engellemek için $P(x_k / C_i) = \frac{s_{ik} + 1}{s_i + a_i}$ ifadesi kullanılır, a_i özellik sayısı

mesala "Gelir" için bu değer 3 tür. Tezde oluşturulan Dolandırıcılık Tespit Sisteminde $P(x_k / C_i)$ bu şekilde hesaplanmıştır.

4. $P(X)$ ifadesi sabit olduğu için hesaplanmaz, çünkü önemli olan birbirlerine göre oransal büyüklükleridir. Bilinmeyen örnek X 'i sınıflandırmak için, her C_i sınıfı $P(X / C_i)P(C_i)$ ifadesi hesaplanır.

$$P(X / C_i)P(C_i) > P(X / C_j)P(C_j)$$

Burada hangisi büyükse o X için geçerli sınıf olur.

8.2.1.2.1.3 Örnek olarak Saf Bayes Sınıflandırması Kullanarak Bir Sınıf Üyelığının Bulunması

Saf Bayes sınıflandırma kullanılarak tahmin etmek istiyoruz. Eğitim verisi Tablo 8.4 'deki veridir. Veri örnekleri *yas*, *gelir*, *öğrenci* ve *kredi_kullanımı* özellikleri tarafından tanımlanır.

Sınıf üyelik özellikleri, *bilgisayar_alma*, ([evet, hayır] olarak adlandırılan) iki ayrı değere sahiptir. C_1 , *bilgisayar_alma* = "evet" değerine ve C_2 , *bilgisayar_alma* = "hayır" değerine eşit olsun. $X = (\text{yas} = "<=30"$, $\text{gelir} = \text{"ortalama"}$, $\text{öğrenci} = \text{"evet"}$, $\text{kredi_kullanımı} = \text{"yüksek"}$) sınıflandırmak istediğimiz bilinmeyen örnektir.

$P(X/C_i)P(C_i)$ değerini maksimize etmeye ihtiyacımız var, $i = 1,2$. $P(C_i)$ için, her sınıf için önsel olasılık eğitim örneklerinden hesaplanabilir:

$$P(\text{bilgisayar_satılama} = \text{"evet"}) = 9/14 = 0.643$$

$$P(\text{bilgisayar_satılama} = \text{"hayır"}) = 5/14 = 0.357$$

$P(X/C_i)$ değerinin hesap etmek için, $i = 1,2$ için, aşağıdaki koşullu olasılıkları hesaplayacağız:

$$P(\text{yas} = "<30" | \text{bilgisayar_alma} = \text{"evet"}) = 7/9 = 0.777$$

$$P(\text{yas} = "<30" | \text{bilgisayar_alma} = \text{"hayır"}) = 2/5 = 0.400$$

$$P(\text{gelir} = \text{"ortalama"} | \text{bilgisayar_alma} = \text{"evet"}) = 4/9 = 0.444$$

$$P(\text{gelir} = \text{"ortalama"} | \text{bilgisayar_alma} = \text{"hayır"}) = 2/5 = 0.400$$

$$P(\text{öğrenci} = \text{"evet"} | \text{bilgisayar_alma} = \text{"evet"}) = 6/9 = 0.667$$

$$P(\text{öğrenci} = \text{"evet"} | \text{bilgisayar_alma} = \text{"hayır"}) = 1/5 = 0.200$$

$$P(\text{kredi_kullanımı} = \text{"yüksek"} | \text{bilgisayar_alma} = \text{"evet"}) = 6/9 = 0.667$$

$$P(\text{kredi_kullanımı} = \text{"yüksek"} | \text{bilgisayar_alma} = \text{"hayır"}) = 2/5 = 0.400$$

Yukarıdaki olasılıklar kullanılarak;

$$P(\text{bilgisayar_satılama} = \text{"evet"}) = 0.777 * 0.444 * 0.667 * 0.667 = 0,153$$

$$P(\text{bilgisayar_satılama} = \text{"hayır"}) = 0.400 * 0.400 * 0.200 * 0.400 = 0,0128$$

$$P(\text{bilgisayar_satılama} = \text{"evet"}) P(\text{bilgisayar_satılama} = \text{"evet"}) = 0.153 * 0.643 = 0.0983$$

$$P(\text{bilgisayar_satılama} = \text{"hayır"}) P(\text{bilgisayar_satılama} = \text{"hayır"}) = 0.0128 * 0.357 = 0.004$$

Bu sebeple, Saf Bayes sınıflandırıcı *bilgisayar_alma* = "evet" kuralını örnek X'e göre tahmin eder.

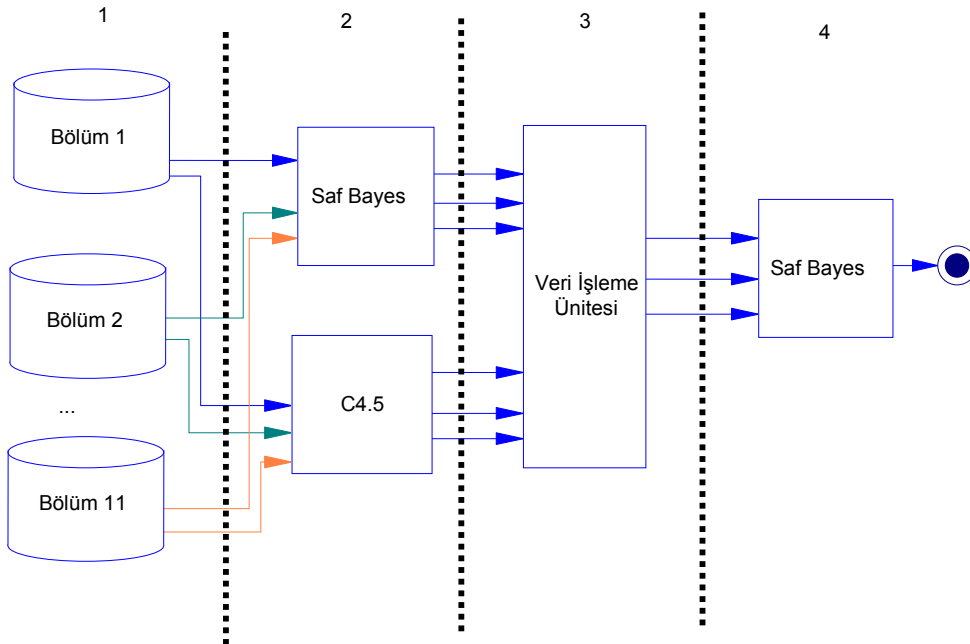
Uygulamamızda Saf Bayes algoritmasının tercih edilme nedenleri olarak;

- Bu sınıflandırıcı karar ağaçları ve yapay sinir ağları sınıflandırıcılar ile kıyaslanabilecek güçlü performans göstermesi.
- Büyük veri tabanları üzerinde işlem yapan Bayes sınıflandırıcılar yüksek hız ve doğruluk dereesine sahip olduklarından.

- Saf Bayes, verilen bir sınıf üzerindeki bir özelliğe ait değerin etkisinin diğer özelliğe ait değerlerden bağımsız olduğunu farz eder. Bu kabul sınıf koşullu bağımsızlık olarak adlandırılır. Bu ise gerekli hesaplamaları basitleştirir, anlaşılabilirliği kolaylaştırır ve doğal olarak “saf” kelimesi ile ifade edilir.

9 TEZ KAPSAMINDA KULLANILAN İNTERNET BANKACILIĞINDA DOLANDIRICILIK TESPİTİ

İnternet Bankacılığında amaç müşterinin şubelere gitmeden, şubeden yapabileceği işlemleri gerçekleştirebilmesidir. Bu işlemleri gerçekleştirirken müşteri numarası, parola, şifre ve eğer varsa şifre üretici gerekmektedir. Herhangi bir kişi bu bilgileri bulabilirse o zaman İnternet Bankacılığı bu kişinin müşteri olduğunu varsayıp her işlemine onay verebilir. İşte Dolandırıcılık Tespit Sistemi burada devreye girer. Müşterinin eski bilgilerine dayanarak , sisteme giren bu müşterinin dolandırıcı olup olmadığına karar vermektedir. Bunu veri madenciliği yöntem ve metotlarını kullanarak gerçekleştirmektedir.



Şekil 9.1 Tez kapsamında kullanılan Dolandırıcılık Tespit Sistemi

9.1 Tez Kapsamında Oluşturulan Dolandırıcılık Tespit Sistemi

Dolandırıcılık Tespit Sisteminde yapılan işlemler aşağıdaki şekilde özetlenebilir;

- 1.) Otomatik olarak oluşturulan İnternet Bankacılığına ait veriler belli formda çekilmiştir.
- 2.) Müşterilerin yaptığı tüm işlemler (para gönderme miktarı,zaman vs.) toplamı , yapılan işleme bölünerek müşteriye ait genel bilgiler oluşturulmuştur.
- 3.) Müşteriye ait genel bilgiler kullanılarak müşterinin grubu belirlenmiştir.
- 4.) Yapılan işlemler müşteri bilgisi yerine müşteri grubu olarak ele alınmıştır. Müşteri gruplarına ait işlemler çok fazla olduğu için 11 parçaya ayrılmıştır.
- 5.) Her bir parça için C4.5 ve Saf Bayes Sınıflandırıcılar teker teker uygulanmıştır.
- 6.) C4.5 ve Saf Bayes Sınıflandırıcıların sonuçları işlenmiştir.
- 7.) İşlenen sonuçlar tekrar Saf Bayes Sınıflandırıcıya giriş değeri olarak verilip sonuç bilgileri alınmıştır.

9.1.1 Verilerin Müşteri Veritabanından Çekilmesi

İnternet Bankacılığına ait olan veriler veri tabanı sorgulama dili ile sorgulanıp müşteriye ait olan veriler çekilmiştir. Bu veriler müşterinin parasal işlemleri, zamanı, gönderdiği kişi , gönderilen banka adı ile şube adı ve IP bilgisidir.

Zaman veritabanında tarih olarak girilmiştir. Zaman bilgisi ay, ayın günü, haftanın günü, gün içinde ki saat dilimleri(zaman1,zaman2,zaman3) olarak ayrıştırılmıştır. İşlemler direk tarih olarak değerlendirilmemiştir.

IP , gönderilen kişi, banka adı ve şube bilgisi yalnızca bir kez rastlanmışsa “evet”, birden fazla rastlanmışsa “hayır” değeri verilmiştir.

9.1.2 Müşterinin Genel Özelliklerinin Belirlenmesi

Müşterinin yaptığı işlemler(zamana göre yapılan parasal işlem miktarı, yeni bir kişiye gönderme sayısı, yeni bir IP numarasından gönderme sayısı) toplanıp, yapılan işlem sayısına bölünerek müşteriye ait özellikler grubu oluşturulmuştur.

9.1.3 Müşteri Grup Bilgilerinin Oluşturulması

VT’de bulunan verileri belirlenen niteliklere göre kümeler. Bu kümeleme işlemleri yapılırken belirlenen niteliklerdeki uzaklıkların en az, yani benzerliklerin en fazla olduğu veriler ortak kümelere konur. Bu kümeleme işlemi sonucunda ortaya çıkan kurullarla, hangi kaydın hangi kümeye girdiği belirlenebilir. Kümeleme algoritması denetimsiz öğrenme kategorisine giren bir algoritmadır. Kümeleme algoritmasındaki amaç verileri alt kümelere ayırmaktır (Michalski and Stepp, 1983). Sınıflama algoritmasında olduğu gibi ortak özellikleri olan veriler bir kümeye girer. Alt kümelere ayrılmak için keşfedilen kurullar yardımıyla bir kaydın hangi alt kümeye girdiği kümeleme algoritması sayesinde bulunur. Kümeleme algoritmasında aşağıdaki veriler girdi olarak kullanılmıştır.

Müşteri Grup		
No	Grup Adı	Grup Değeri
1	Zaman1 de Yapılan Para Transferi Miktarı	0..999.99,1000..2499.99,2500..
2	Zaman2 de Yapılan Para Transferi Miktarı	0..999.99,1000..2499.99,2500..
3	Zaman3 de Yapılan Para Transferi Miktarı	0..999.99,1000..2499.99,2500..
4	İlk Defa Para Transferi Yapılan Kişi Oranı	0<<0.4,0.4<
5	Yeni IP Kullanım Oranı	0<<0.4,0.4<

Tablo 8.1 müşteri grup özellikleri ve değer aralıkları

Kümeleme sorgusuyla müşteri bilgileri kullanılarak müşteri grup sayısı ve bu gruba girecek müşteri özellikleri keşfedilmiştir. Kümeleme Algoritmasının tercih edilmesinin sebebi:

- Küme sayılarını otomatik olarak bulabilmesi,
- Kümelere giren müşterilerin aynı özellikleri taşıması , diğer küme ile özellik olarak ayrılmasıdır.

Kümeleme algoritmasının kullanılmasında tavsiye edilen; olabildiğince az sayıda niteliğin girdi olarak verilmesidir (Zhong, 1994, Michalski, 1983). Kümeleme sorgusuyla müşteri grup sayısı ve bu gruplara girmek için gereken kuralların bulunması amaçlandığına göre, kullanılacak müşteri nitelikleri tablo 8.1 gösterilmiştir

Kümeleme algoritmasında değişen bir özellik bir kümeye denk gelmektedir. Zaman1,2,3 ;3'er özelliğe sahip; Yeni Kişi Oranı 2 özellik ,Yeni IP Oranı 2 özellik olmak üzere “Maksimum Toplam Küme Sayısı” = $3*3*3*2*2=108$ adet.

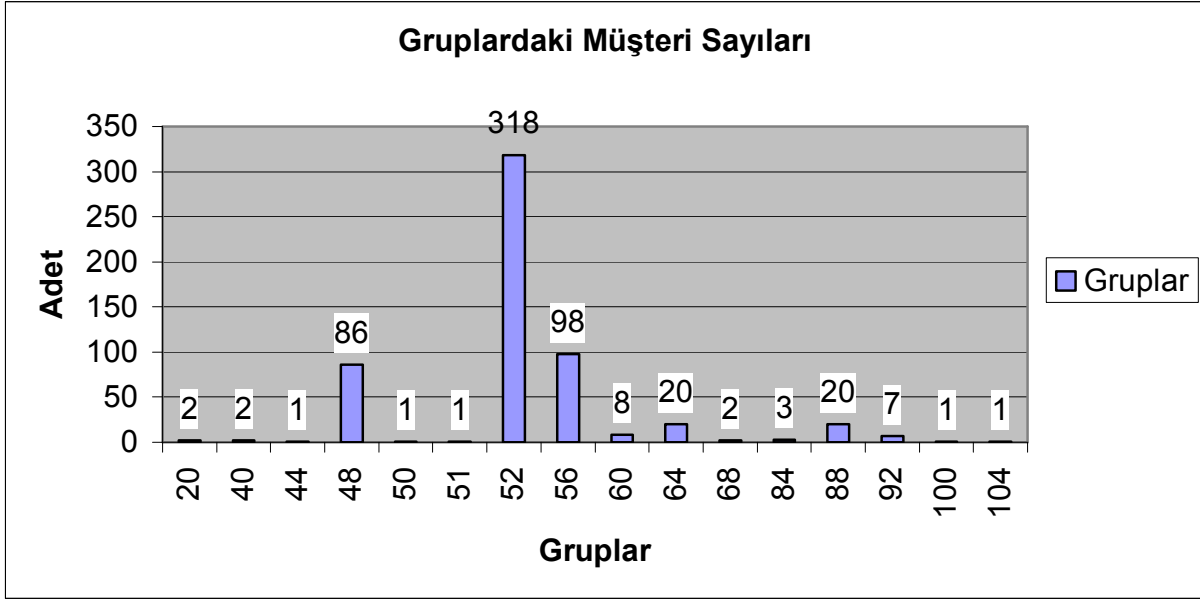
Tablo 8.1 de her gruba ait müşteri grup özellikleri, Tablo 8.2 de ise müşterilerin grup bilgileri yer almaktadır.

Grup Özellikleri						
No	Grup No	Zaman1	Zaman2	Zaman3	Yeni Kişi	Yeni IP
1	20	0..999.99	1000..2499.99	2500..	0<0.4	0<0.4
2	40	1000..2499.99	0..999.99	1000..2499.99	0<0.4	0<0.4
3	44	1000..2499.99	0..999.99	2500..	0<0.4	0<0.4
4	48	1000..2499.99	1000..2499.99	0..999.99	0<0.4	0<0.4
5	50	1000..2499.99	1000..2499.99	1000..2499.99	0.4<	0<0.4
6	51	1000..2499.99	1000..2499.99	1000..2499.99	0<0.4	0.4<
7	52	1000..2499.99	1000..2499.99	1000..2499.99	0<0.4	0<0.4
8	56	1000..2499.99	1000..2499.99	2500..	0<0.4	0<0.4
9	60	1000..2499.99	2500..	0..999.99	0<0.4	0<0.4
10	64	1000..2499.99	2500..	1000..2499.99	0<0.4	0<0.4
11	68	1000..2499.99	2500..	2500..	0<0.4	0<0.4
12	84	2500..	1000..2499.99	0..999.99	0<0.4	0<0.4
13	88	2500..	1000..2499.99	1000..2499.99	0<0.4	0<0.4
14	92	2500..	1000..2499.99	2500..	0<0.4	0<0.4
15	100	2500..	2500..	1000..2499.99	0<0.4	0<0.4
16	104	2500..	2500..	2500..	0<0.4	0<0.4

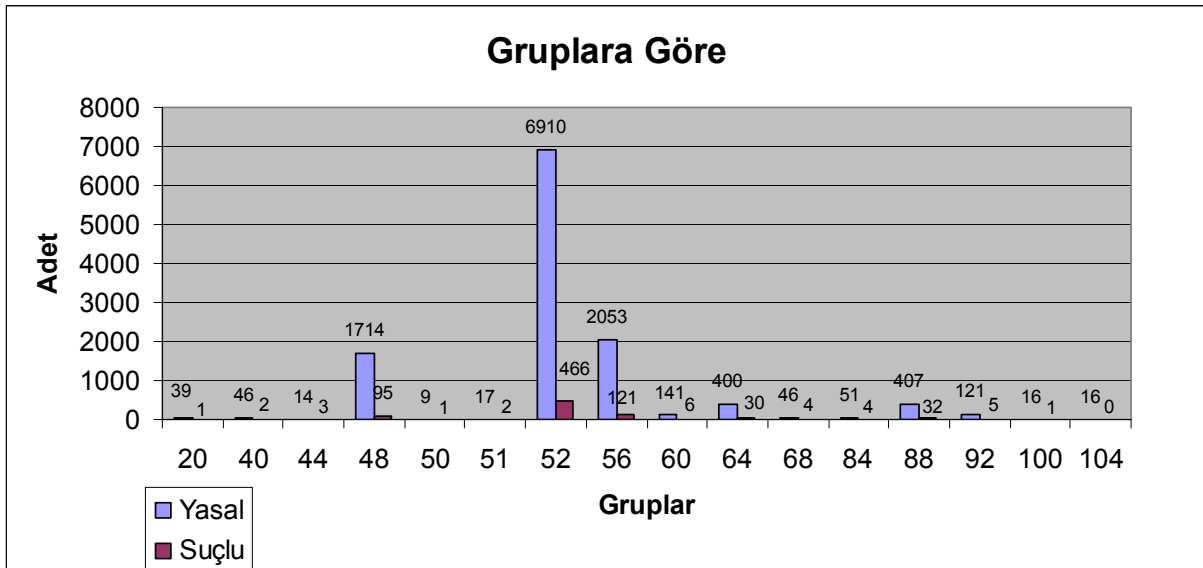
Tablo 8.2 Grup özellikleri

Müşteri Grup Bilgileri		
No	Grup No	Müşteri No
1	20	115,457
2	40	348,397
3	44	406
4	48	5,17,22,40,53,28,24,54,65,124,122,113,112,106,98,97,85,63,177,167,159,158,154,150,146,140,135,342,337,333,331,313,309,307,304,301,492,478,472,469,448,441,431,430,426,292,289,281,276,266,262,256,251,238,235,227,220,214,208,198,180,521,508,507,506,504,499,498,495,420,561,554,552,547,541,536,528,526,525,409,396,375,366,346,345,343,
5	50	121
6	51	267
7	52	3,4,7,9,11,13,12,27,26,25,23,20,19,18,16,46,45,44,43,42,41,39,38,37,68,67,64,58,57,56,55,51,50,49,48,47,100,99,95,93,92,91,90,89,88,87,86,84,136,134,132,131,129,128,126,125,118,248,245,244,240,239,237,234,233,232,231,229,226,225,224,223,213,212,210,209,207,206,205,204,202,201,200,199,197,195,194,193,192,191,190,188,187,185,184,183,182,181,179,178,176,174,173,170,169,166,165,164,162,160,157,156,153,151,149,148,145,143,142,141,139,138,117,114,111,110,109,108,107,105,446,445,444,443,442,439,438,437,436,435,434,433,432,429,428,427,422,421,418,417,416,414,413,412,411,410,408,405,404,402,401,400,395,394,392,390,389,386,385,384,383,380,379,378,377,376,374,373,372,370,368,365,364,363,362,360,359,357,355,354,351,350,340,339,335,330,326,324,322,318,317,316,315,1,571,570,569,568,567,565,564,558,551,550,549,548,546,545,544,543,540,538,537,535,533,532,530,529,527,522,520,519,518,513,511,509,505,503,501,500,497,496,493,491,490,489,487,486,484,483,480,477,476,474,473,468,467,463,462,461,458,455,454,453,452,451,450,449,447,314,311,308,306,305,303,299,298,297,296,294,293,291,287,282,280,279,278,274,273,272,271,270,269,268,265,261,257,255,252,250,249,83,82,80,79,76,74,73,72,36,4,33,32,31,30,10,8,6,
8	56	2,29,21,35,60,66,70,328,323,320,312,302,300,203,104,103,566,563,562,560,559,556,553,542,539,534,531,524,523,517,514,512,502,494,488,485,482,479,475,471,470,466,460,456,440,425,415,403,398,391,381,367,361,358,356,353,352,349,347,336,334,329,101,94,81,78,77,75,71,69,295,290,288,286,277,264,263,260,259,247,243,241,236,217,216,215,196,172,171,168,163,152,222,218,127,123,120,119,
9	60	15,555,464,102,327,393,399,319
10	64	52,61,424,407,388,382,369,338,325,283,275,254,219,189,144,137,62,516,515,481,
11	68	285,465,
12	84	211,230,246,
13	88	14,116,147,175,510,459,423,419,387,371,321,310,284,258,242,221,186,161,557,130,
14	92	59,133,96,341,344,332,253,
15	100	155
16	104	228

Tablo 8.3 Müşteri grup özellikleri



Gruplara göre yasal ve suçlu işlem sayıları;



9.1.4 Müşterinin Müşteri Grubu Olarak Adlandırılması ve Verinin Bölümlenmesi

Müşterilerin, grup bilgileri bilindiği için artık müşteri numaraları yerine müşteri grup numarası kullanılmıştır.

Müşteri gruplarının yasal olan verileri kendi içinde rasgele olarak 11 parçaya bölünüp , suçlu kayıtları bu 11 parça olan her bir gruba teker teker eklenmiştir. Suçlu kayıtları yasal kayıtlardan oldukça az olduğu için verinin fakirleşmemesi böylece sağlanmış olur. Böyle yapılmadığı zaman 11 parçanın bazısında suçlu sayısı az, bazısında fazla olacağı için kimi kısımlarda kötü sonuçlar elde edilecekti. (Chan ve Stolfo,1995) ve (Prodromidis,1999) veri parçalarının(bölümlerinin) öğrenme algoritmasında zaman kaybı oluşmaması için ne çok büyük , zayıf sınıflandırmalar üretmemesi için ne de çok küçük olmaması gerektiğini söylemiştir.

9.1.5 C4.5 ve Saf Bayes Sınıflandırıcıların Bölümlere Uygulanması

Bu bölümden itibaren grup52'ye ait veriler kullanılmıştır.

9.1.5.1 C4.5 Sınıflandırıcısının Bölümlere Uygulanması

Her bir bölüm için C4.5 sınıflandırıcı uygulanmıştır. Daha sonra oluşan karar ağaçlarına sırası ile elde olan veriler uygulanarak sonuçlar elde edilmiştir. Yani her bir verinin C4.5 sınıflandırıcı için 11 adet çıkış bilgisi oluşmuştur. Aşağıdaki tablo, 11 bölümden ilki için çıkarılmış sonuçları içermektedir.

C4.5 Sınıflandırıcısı Sonucunda Oluşan Ağaç Yapısı	
Ağaç 1. Kısım	Ağaç2.kısım
yeniKisi = evet	gun = 13: hayır (0.0)
yeniIP = evet	gun = 14: hayır (4.0)
gun = 1: evet (4.0)	gun = 15: hayır (9.0)
gun = 2	gun = 16: hayır (5.0)
ay = 1: evet (1.0)	gun = 17: hayır (2.0)
ay = 2: evet (2.0)	gun = 18: hayır (1.0)
ay = 3: evet (0.0)	gun = 19: hayır (0.0)
ay = 4: evet (1.0)	gun = 20: hayır (0.0)
ay = 5: evet (2.0)	gun = 21: hayır (0.0)
ay = 6: evet (0.0)	gun = 22: hayır (0.0)
ay = 7: evet (0.0)	gun = 23: evet (2.0/1.0)
ay = 8: evet (1.0)	gun = 24: evet (2.0)
ay = 9: evet (0.0)	gun = 25: hayır (0.0)
ay = 10: evet (0.0)	gun = 26: hayır (0.0)
ay = 11: hayır	gun = 27: hayır (4.0/1.0)
ay = 12: evet (2.0)	gun = 28: hayır (2.0)
gun = 3: evet (15.0/1.0)	gun = 29: hayır (0.0)
gun = 4: evet (16.0)	gun = 30: evet (2.0/1.0)
gun = 5: evet (29.0)	gun = 31: hayır (7.0)
gun = 6: evet (31.0)	yeniKisi = hayır

gun = 7: evet (29.0)	yeniIP = evet
gun = 8: evet (34.0)	gun = 1: hayır (6.0)
gun = 9: evet (45.0)	gun = 2: hayır (3.0)
gun = 10: evet (3.0)	gun = 3: hayır (4.0)
gun = 11: evet (3.0)	gun = 15: hayır (3.0)
gun = 12: hayır (1.0)	gun = 16: hayır (4.0)
gun = 13: evet (5.0)	gun = 17: hayır (6.0)
gun = 14: evet (5.0)	gun = 18: hayır (0.0)
gun = 15: evet (2.0)	gun = 19: evet (2.0)
gun = 16: evet (4.0)	gun = 20: hayır (2.0)
gun = 17	gun = 21: hayır (1.0)
ay = 1: evet (0.0)	gun = 22: hayır (0.0)
ay = 2: evet (0.0)	gun = 23: hayır (0.0)
ay = 3: evet (0.0)	gun = 24: evet (1.0)
ay = 4: evet (0.0)	gun = 25: evet (4.0/2.0)
ay = 5: evet (0.0)	gun = 26: hayır (3.0)
ay = 6: hayır (1.0)	gun = 27: evet (1.0)
ay = 7: evet (0.0)	gun = 28: hayır (2.0)
ay = 8: evet (2.0)	gun = 29: hayır (2.0)
ay = 9: evet (0.0)	gun = 30: hayır (1.0)
ay = 10: evet (0.0)	gun = 31: hayır (5.0/1.0)
ay = 11: evet (0.0)	yeni IP = hayır
ay = 12: evet (2.0)	gun = 1: hayır (37.0)
gun = 18: evet (9.0)	gun = 2: hayır (50.0)
gun = 19: evet (7.0)	gun = 3: hayır (51.0)
gun = 20: evet (12.0)	gun = 4: hayır (11.0/1.0)
gun = 21: evet (8.0)	gun = 5: hayır (4.0/1.0)
gun = 22: evet (8.0)	gun = 6: hayır (9.0/1.0)
gun = 23: evet (9.0)	gun = 7: hayır (11.0/1.0)
gun = 24: evet (16.0)	gun = 8: hayır (8.0)
gun = 25: evet (6.0)	gun = 9
gun = 26: evet (22.0)	hafta = 1: evet (1.0)
gun = 27: evet (13.0)	hafta = 2: hayır (1.0)
gun = 28: evet (23.0)	hafta = 3: hayır (2.0)
gun = 29: evet (15.0)	hafta = 4: evet (2.0/1.0)
gun = 30: evet (29.0)	hafta = 5: hayır (2.0)
gun = 31: evet (21.0)	hafta = 6: hayır (4.0)
yeniIP = hayır	hafta = 7: hayır (1.0)
gun = 1: hayır (4.0)	gun = 10: hayır (6.0)
gun = 2: hayır (4.0)	gun = 11: hayır (3.0)
gun = 3: hayır (2.0)	gun = 12: hayır (7.0)
gun = 4: evet (1.0)	gun = 13: hayır (7.0)
gun = 5: evet (1.0)	gun = 14: hayır (53.0)
gun = 6: evet (1.0)	gun = 15: hayır (45.0)
gun = 7: evet (1.0)	gun = 16: hayır (52.0)
gun = 8: evet (1.0)	gun = 17: hayır (36.0)
gun = 9: evet (2.0/1.0)	gun = 18: hayır (2.0)

gun = 10: hayır (0.0)	gun = 19: hayır (4.0)
gun = 11: hayır (1.0)	gun = 20: hayır (9.0)
gun = 12: hayır (0.0)	gun = 21: hayır (7.0)
gun = 4: evet (2.0/1.0)	gun = 22: hayır (9.0)
gun = 5: evet (1.0)	gun = 23: hayır (5.0)
gun = 6: evet (2.0/1.0)	gun = 24: hayır (6.0)
gun = 7: hayır (0.0)	gun = 25: hayır (5.0)
gun = 8: evet (3.0)	gun = 26: hayır (4.0)
gun = 9: evet (1.0)	gun = 27: hayır (4.0)
gun = 10: hayır (1.0)	gun = 28: hayır (16.0)
gun = 11: hayır (1.0)	gun = 29: hayır (8.0)
gun = 12: hayır (0.0)	gun = 30: hayır (21.0)
gun = 13: hayır (2.0)	gun = 31: hayır (22.0)
gun = 14: hayır (9.0)	

Yaprak Sayısı : 152

Ağacın Boyu: 162

Model oluşturmak için geçen zaman: 0.03 saniye

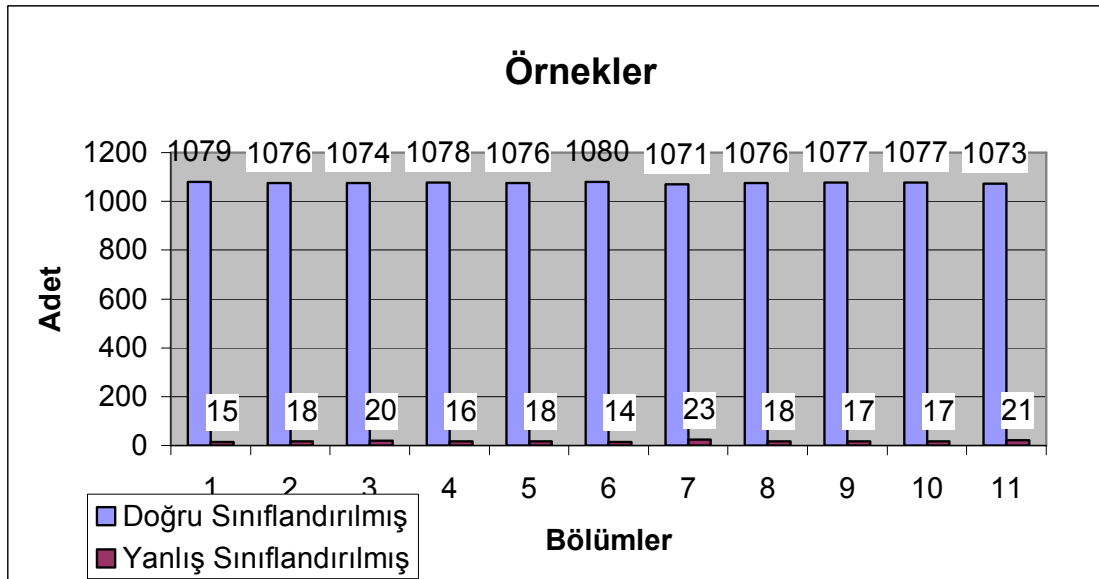
Eğitim verisinde ki doğru ve hatalı sınıflandırmalar;

Doğru olarak sınıflandırılmış örnekler 1079 98.6289 %

Hatalı olarak sınıflandırılmış örnekler 15 1.3711 %

Diğer bölümler için veriler aynı şekilde belirtilmektedir. Tüm bölümlerin sınıflandırma sonuçları aşağıdaki grafikte verilmiştir.

9.1.5.1.1 C4.5 Algoritmasına Göre Sınıflandırma Sonuçları



9.1.5.2 Saf Bayes Sınıflandırıcının Bölümlere Uygulanması

Her bir bölüm için Saf Bayes Sınıflandırıcı uygulanmıştır. Yani her bir verinin Saf Bayes Sınıflandırıcı için 11 adet çıkış bilgisi oluşmuştur.

Aşağıdaki tablolar, 11 bölümden 1. si için çıkarılmış sonuçları içermektedir. Burada $P(x_k / C_i)$ ifadesinin sonucu 'Değeri' kısmında yer almıştır.

Sınıf evet: $P(C) = 0.42609489$ evet için;

Özellik	Grup						
	Grup No	Değeri	Grup No	Değeri	Grup No	Değeri	Grup No
0	0.00174216	27	0.00174216	54	0.00174216	81	0.00174216
1	0.00174216	28	0.00174216	55	0.00174216	82	0.00174216
2	0.00174216	29	0.00174216	56	0.00174216	83	0.00174216
3	0.00174216	30	0.00174216	57	0.00174216	84	0.00174216
4	0.00174216	31	0.00174216	58	0.00174216	85	0.00174216
5	0.00174216	32	0.00174216	59	0.00174216	86	0.00174216
6	0.00174216	33	0.00174216	60	0.00174216	87	0.00174216
7	0.00174216	34	0.00174216	61	0.00174216	88	0.00174216
8	0.00174216	35	0.00174216	62	0.00174216	89	0.00174216
9	0.00174216	36	0.00174216	63	0.00174216	90	0.00174216
10	0.00174216	37	0.00174216	64	0.00174216	91	0.00174216
11	0.00174216	38	0.00174216	65	0.00174216	92	0.00174216
12	0.00174216	39	0.00174216	66	0.00174216	93	0.00174216
13	0.00174216	40	0.00174216	67	0.00174216	94	0.00174216
14	0.00174216	41	0.00174216	68	0.00174216	95	0.00174216
15	0.00174216	42	0.00174216	69	0.00174216	96	0.00174216
16	0.00174216	43	0.00174216	70	0.00174216	97	0.00174216
17	0.00174216	44	0.00174216	71	0.00174216	98	0.00174216
18	0.00174216	45	0.00174216	72	0.00174216	99	0.00174216
19	0.00174216	46	0.00174216	73	0.00174216	100	0.00174216
20	0.00174216	47	0.00174216	74	0.00174216	101	0.00174216
21	0.00174216	48	0.00174216	75	0.00174216	102	0.00174216
22	0.00174216	49	0.00174216	76	0.00174216	103	0.00174216
23	0.00174216	50	0.00174216	77	0.00174216	104	0.00174216
24	0.00174216	51	0.00174216	78	0.00174216	105	0.00174216
25	0.00174216	52	0.81358885	79	0.00174216	106	0.00174216
26	0.00174216	53	0.00174216	80	0.00174216	107	0.00174216

Özellik		Ay					
Ay No	Değeri	Ay No	Değeri	Ay No	Değeri	Ay No	Değeri
1	0.0690376	4	0.07949791	7	0.06485356	10	0.12761506
2	0.11297071	5	0.07949791	8	0.06903766	11	0.07531381
3	0.10878661	6	0.06485356	9	0.07531381	12	0.07322176

Özellik		Hafta					
Hafta No	Değeri	Hafta No	Değeri	Hafta No	Değeri	Hafta No	Değeri
1	0.14376321	3	0.1205074	5	0.11839323	7	0.14164905
2	0.16701903	4	0.17336152	6	0.13530655		

Özellik		Gün					
Gün No	Değeri	Gün No	Değeri	Gün No	Değeri	Gün No	Değeri
1	0.01006036	9	0.10060362	17	0.01006036	25	0.01810865
2	0.02012072	0	0.00804829	18	0.02012072	26	0.04627767
3	0.03018109	11	0.00804829	19	0.02012072	27	0.03219316
4	0.04024145	12	0.00201207	20	0.02615694	28	0.04828974
5	0.06639839	13	0.01207243	21	0.01810865	29	0.03219316
6	0.07042254	14	0.01207243	22	0.01810865	30	0.06237425
7	0.06438632	15	0.00603622	23	0.0221328	31	0.04627767
8	0.07847082	16	0.01006036	24	0.04024145		

Özellik		Zaman			
Zaman No	Değeri	Zaman No	Değeri	Zaman No	Değeri
1	0.31556503	2	0.34115139	3	0.34328358

Özellik		Para Transferi Miktarı			
Para Transfer Miktarı Aralığı	Değeri	Para Transfer Miktarı Aralığı	Değeri	Para Transfer Miktarı Aralığı	Değeri
0..999.99	0.15565032	1000..2499.99	0.50533049	2500..	0.33901919

Özellik		Yeni Kişi	
Yeni Kişi	Değeri	Yeni Kişi	Değeri
Evet	0.95512821	Hayır	0.04487179

Özellik		Yeni IP	
Yeni IP	Değeri	Yeni IP	Değeri
Evet	0.96153846	Hayır	0.03846154

Özellik		Yeni Banka	
Yeni Banka	Değeri	Yeni Banka	Değeri
Evet	0.26923077	Hayır	0.73076923

Özellik	Yeni Şube		
Yeni Şube	Değeri	Yeni Şube	Değeri
Evete	0.4465812	Hayır	0.5534188

Sınıf hayır: $P(C) = 0.57390511$ için ;

Özellik	Grup						
Grup No	Değeri	Grup No	Değeri	Grup No	Değeri	Grup No	Değeri
0	0.0013587	27	0.0013587	54	0.0013587	81	0.0013587
1	0.0013587	28	0.0013587	55	0.0013587	82	0.0013587
2	0.0013587	29	0.0013587	56	0.0013587	83	0.0013587
3	0.0013587	30	0.0013587	57	0.0013587	84	0.0013587
4	0.0013587	31	0.0013587	58	0.0013587	85	0.0013587
5	0.0013587	32	0.0013587	59	0.0013587	86	0.0013587
6	0.0013587	33	0.0013587	60	0.0013587	87	0.0013587
7	0.0013587	34	0.0013587	61	0.0013587	88	0.0013587
8	0.0013587	35	0.0013587	62	0.0013587	89	0.0013587
9	0.0013587	36	0.0013587	63	0.0013587	90	0.0013587
10	0.0013587	37	0.0013587	64	0.0013587	91	0.0013587
11	0.0013587	38	0.0013587	65	0.0013587	92	0.0013587
12	0.0013587	39	0.0013587	66	0.0013587	93	0.0013587
13	0.0013587	40	0.0013587	67	0.0013587	94	0.0013587
14	0.0013587	41	0.0013587	68	0.0013587	95	0.0013587
15	0.0013587	42	0.0013587	69	0.0013587	96	0.0013587
16	0.0013587	43	0.0013587	70	0.0013587	97	0.0013587
17	0.0013587	44	0.0013587	71	0.0013587	98	0.0013587
18	0.0013587	45	0.0013587	72	0.0013587	99	0.0013587
19	0.0013587	46	0.0013587	73	0.0013587	100	0.0013587
20	0.0013587	47	0.0013587	74	0.0013587	101	0.0013587
21	0.0013587	48	0.0013587	75	0.0013587	102	0.0013587
22	0.0013587	49	0.0013587	76	0.0013587	103	0.0013587
23	0.0013587	50	0.0013587	77	0.0013587	104	0.0013587
24	0.0013587	51	0.0013587	78	0.0013587	105	0.0013587
25	0.0013587	52	0.85461957	79	0.0013587	106	0.0013587
26	0.0013587	53	0.0013587	80	0.0013587	107	0.0013587

Özellik	Ay						
Ay No	Değeri	Ay No	Değeri	Ay No	Değeri	Ay No	Değeri
1	0.0796875	4	0.0671875	7	0.0640625	10	0.0671875
2	0.0875	5	0.078125	8	0.096875	11	0.08125
3	0.0875	6	0.09375	9	0.109375	12	0.0875

Özellik		Hafta					
Hafta No	Değeri	Hafta No	Değeri	Hafta No	Değeri	Hafta No	Değeri
1	0.12283465	3	0.14645669	5	0.13858268	7	0.15905512
2	0.15433071	4	0.14645669	6	0.13228346		

Özellik		Gün					
Gün No	Değeri	Gün No	Değeri	Gün No	Değeri	Gün No	Değeri
1	0.07283763	9	0.01972686	17	0.06980273	25	0.01213961
2	0.08952959	10	0.01213961	18	0.0060698	26	0.01213961
3	0.08952959	11	0.0091047	19	0.00758725	27	0.01213961
4	0.01820941	12	0.01365706	20	0.01820941	28	0.03186646
5	0.0060698	13	0.01517451	21	0.01365706	29	0.01669196
6	0.01517451	14	0.1016692	22	0.01517451	30	0.03641882
7	0.01669196	15	0.08801214	23	0.01062215	31	0.05159332
8	0.01365706	16	0.09408194	24	0.01062215		

Özellik		Zaman			
Zaman No	Değeri	Zaman No	Değeri	Zaman No	Değeri
1	0.44057052	2	0.42155309	3	0.13787639

Özellik		Para Transferi Miktarı			
Para Transfer Miktarı Aralığı	Değeri	Para Transfer Miktarı Aralığı	Değeri	Para Transfer Miktarı Aralığı	Değeri
0..999.99	0.33597464	1000..2499.99	0.34548336	2500..	0.318542

Özellik		Yeni Kişi	
Yeni Kişi	Değeri	Yeni Kişi	Değeri
Evet	0.08253968	Hayır	0.91746032

Özellik		Yeni İP	
Yeni İP	Değeri	Yeni İP	Değeri
Evet	0.1	Hayır	0.9

Özellik		Yeni Banka	
Yeni Banka	Değeri	Yeni Banka	Değeri
Evet	0.11269841	Hayır	0.88730159

Özellik		Yeni Şube	
Yeni Şube	Değeri	Yeni Şube	Değeri
Evet	0.22698413	Hayır	0.77301587

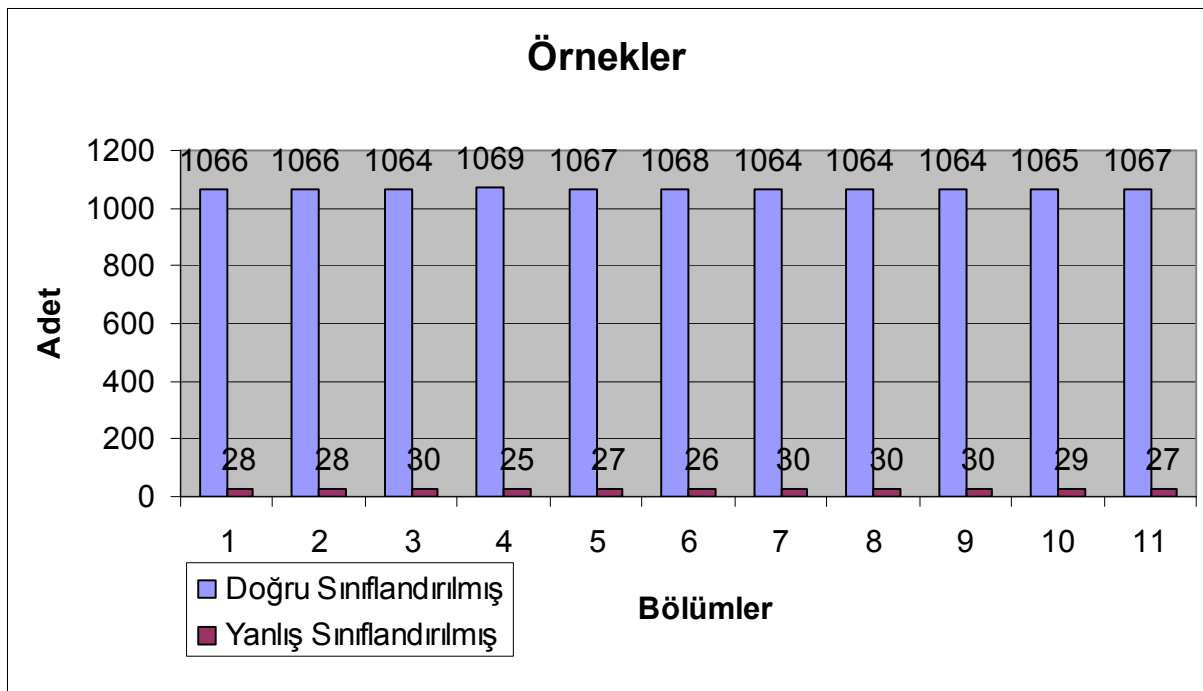
Model oluşturmak için geçen zaman: 0.03 saniye

Eğitim verisinde ki doğru ve hatalı sınıflandırmalar;

Doğru olarak sınıflandırılmış örnekler	1066	97.4406 %
Hatalı olarak sınıflandırılmış örnekler	28	2.5594 %

Diğer bölümler için veriler aynı şekilde belirtilmektedir. Tüm bölümlerin sınıflandırma sonuçları aşağıdaki grafikte verilmiştir.

9.1.5.2.1 Bölümlerin Saf Bayes Sınıflandırmasına Göre Sonuçları

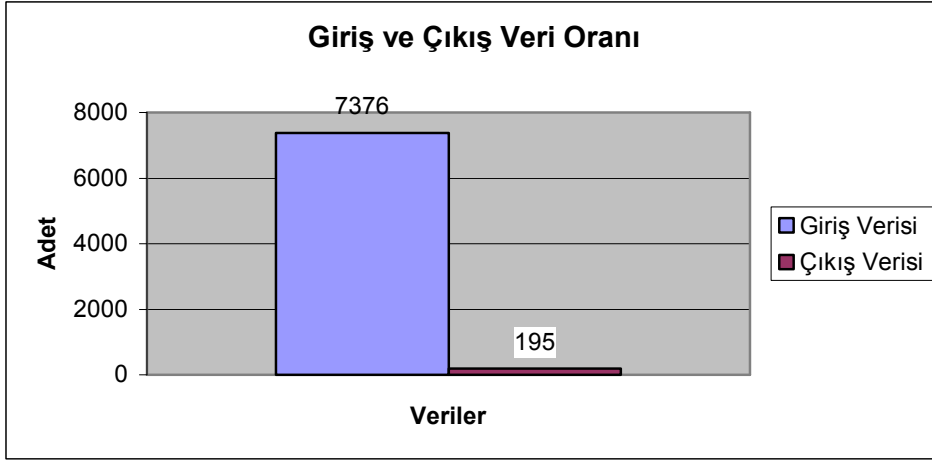


9.1.6 Sınıflandırma Sonuçlarının İşlenmesi

C4.5 ve Saf Bayes Sınıflandırıcılardan çıkan sonuçlar belli işlemlere tabi tutulmuştur. Her bir eğitim verisi var olan 11 adet bölüme C4.5 ve Saf Bayes Sınıflandırıcı için uygulanmıştır. Her bir örnek için çıkış sayısı C4.5 sınıflandırıcı için 11, Saf Bayes Sınıflandırıcı için 11 olmak üzere toplam 22 tane olmaktadır.

Çıkan sonuç listelerinden değerleri aynı olanlar sonuç değerlerine (evet sayısı ve hayır sayısı) göre tekrar sayıları ile birlikte kayıt edilmiştir. Grup 52 için sınıflandırıcılardan çıkan sonuç sayısı 7376 bu sonuçların işlenmesi sonucunda 195 adet veri sonucu ortaya çıkmıştır.

9.1.6.1 Giriş ve Çıkış Veri Sonuçları



Çıkış değerlerinin evet ve hayır sayıları toplanıp evet sayısına bölünerek evet oranı elde edilmiştir. Çıkan sayıda bulunduğu aralığa yuvarlanır mesela 0.34 çıkarsa bu 0.3 olarak kabul edilmiştir. Sonuç kümesi $\{0.0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0\}$ aralığındadır.

9.1.7 Sonuçların Saf Bayes Sınıflandırıcıya Uygulanması

Elde edilen sonuç verileri Saf Bayes Sınıflandırıcıya uygulanmıştır.

9.1.7.1.1 Girdi Veri Tipleri

Verilerin girdileri ve alabileceği değerler aşağıdaki gibidir.

$a1\{0,1\}; a2\{0,1\}; a3\{0,1\}; a4\{0,1\}; a5\{0,1\}; a6\{0,1\}; a7\{0,1\}; a8\{0,1\}; a9\{0,1\}; a10\{0,1\}; a11\{0,1\};$
 $a12\{0,1\}; a13\{0,1\}; a14\{0,1\}; a15\{0,1\}; a16\{0,1\}; a17\{0,1\}; a18\{0,1\}; a19\{0,1\}; a20\{0,1\}; a21\{0,1\};$
 $a22\{0,1\}; sonuc\{0.0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0\}$

9.1.7.1.2 Saf Bayes Sınıflandırıcı İçin Çıkan Değerler

Özellik a1

0	1
0.40229885	0.59770115

Yukarıdaki ifade de a1 özelliği için 0 gelme ve 1 gelme oranları sırasıyla 0.40229885, 0.59770115 dir. Aşağıdaki tablo tüm özellik ve sınıflar için olasılıkları belirtmektedir.

Sınıf 0.0: P(C)=0.83980583		Sınıf 0.1: P(C)=0.02912621		Sınıf 0.2: P(C)= 0.01456311	
Özellik a1		Özellik a1		Özellik a1	
0	1	0	1	0	1
0.40229885	0.59770115	0.42857143	0.57142857	0.25	0.75
Özellik a2		Özellik a2		Özellik a2	
0	1	0	1	0	1
0.52873563	0.47126437	0.71428571	0.28571429	0.5	0.5
Özellik a3		Özellik a3		Özellik a3	
0	1	0	1	0	1
0.49425287	0.50574713	0.42857143	0.57142857	0.5	0.5
Özellik a4		Özellik a4		Özellik a4	
0	1	0	1	0	1
0.6091954	0.3908046	0.42857143	0.57142857	0.25	0.75
Özellik a5		Özellik a5		Özellik a5	
0	1	0	1	0	1
0.49425287	0.50574713	0.42857143	0.57142857	0.25	0.75
Özellik a6		Özellik a6		Özellik a6	
0	1	0	1	0	1
0.50574713	0.49425287	0.42857143	0.57142857	0.25	0.75
Özellik a7		Özellik a7		Özellik a7	
0	1	0	1	0	1
0.57471264	0.42528736	0.42857143	0.57142857	0.5	0.5
Özellik a8		Özellik a8		Özellik a8	
0	1	0	1	0	1
0.5	0.5	0.28571429	0.71428571	0.25	0.75
Özellik a9		Özellik a9		Özellik a9	
0	1	0	1	0	1
0.49425287	0.50574713	0.42857143	0.57142857	0.25	0.75
Özellik a10		Özellik a10		Özellik a10	
0	1	0	1	0	1
0.46551724	0.53448276	0.57142857	0.42857143	0.25	0.75
Özellik a11		Özellik a11		Özellik a11	
0	1	0	1	0	1
0.68965517	0.31034483	0.42857143	0.57142857	0.25	0.75

Özellik a12 0 0.58045977	1 0.41954023	Özellik a12 0 0.71428571	1 0.28571429	Özellik a12 0 0.25	1 0.75
Özellik a13 0 0.55172414	1 0.44827586	Özellik a13 0 0.71428571	1 0.28571429	Özellik a13 0 0.25	1 0.75
Özellik a14 0 0.54597701	1 0.45402299	Özellik a14 0 0.71428571	1 0.28571429	Özellik a14 0 0.25	1 0.75
Özellik a15 0 0.63218391	1 0.36781609	Özellik a15 0 0.71428571	1 0.28571429	Özellik a15 0 0.25	1 0.75
Özellik a16 0 0.57471264	1 0.42528736	Özellik a16 0 0.71428571	1 0.28571429	Özellik a16 0 0.25	1 0.75
Özellik a17 0 0.66091954	1 0.33908046	Özellik a17 0 0.71428571	1 0.28571429	Özellik a17 0 0.25	1 0.75
Özellik a18 0 0.6091954	1 0.3908046	Özellik a18 0 0.71428571	1 0.28571429	Özellik a18 0 0.25	1 0.75
Özellik a19 0 0.5862069	1 0.4137931	Özellik a19 0 0.71428571	1 0.28571429	Özellik a19 0 0.25	1 0.75
Özellik a20 0 0.63793103	1 0.36206897	Özellik a20 0 0.71428571	1 0.28571429	Özellik a20 0 0.25	1 0.75
Özellik a21 0 0.62643678	1 0.37356322	Özellik a21 0 0.71428571	1 0.28571429	Özellik a21 0 0.25	1 0.75
Özellik a22 0 0.66091954	1 0.33908046	Özellik a22 0 0.71428571	1 0.28571429	Özellik a22 0 0.25	1 0.75

Sınıf 0.3: P(C)=0.01941748			Sınıf 0.4: P(C)=0.00485437			Sınıf 0.5: P(C)=0.02427184		
Özellik a1			Özellik a1			Özellik a1		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.33333333	0.66666667	
Özellik a2			Özellik a2			Özellik a2		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.33333333	0.66666667	
Özellik a3			Özellik a3			Özellik a3		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.16666667	0.83333333	
Özellik a4			Özellik a4			Özellik a4		
0	1		0	1		0	1	
0.4	0.6		0.5	0.5		0.33333333	0.66666667	
Özellik a5			Özellik a5			Özellik a5		
0	1		0	1		0	1	
0.4	0.6		0.5	0.5		0.33333333	0.66666667	
Özellik a6			Özellik a6			Özellik a6		
0	1		0	1		0	1	
0.4	0.6		0.5	0.5		0.16666667	0.83333333	
Özellik a7			Özellik a7			Özellik a7		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.5	0.5	
Özellik a8			Özellik a8			Özellik a8		
0	1		0	1		0	1	
0.4	0.6		0.5	0.5		0.16666667	0.83333333	
Özellik a9			Özellik a9			Özellik a9		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.5	0.5	
Özellik a10			Özellik a10			Özellik a10		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.33333333	0.66666667	
Özellik a11			Özellik a11			Özellik a11		
0	1		0	1		0	1	
0.2	0.8		0.5	0.5		0.66666667	0.33333333	

Özellik a12 0 1 0.4 0.6	Özellik a12 0 1 0.5 0.5	Özellik a12 0 1 0.33333333 0.66666667
Özellik a13 0 1 0.4 0.6	Özellik a13 0 1 0.5 0.5	Özellik a13 0 1 0.33333333 0.66666667
Özellik a14 0 1 0.4 0.6	Özellik a14 0 1 0.5 0.5	Özellik a14 0 1 0.33333333 0.66666667
Özellik a15 0 1 0.4 0.6	Özellik a15 0 1 0.5 0.5	Özellik a15 0 1 0.33333333 0.66666667
Özellik a16 0 1 0.4 0.6	Özellik a16 0 1 0.5 0.5	Özellik a16 0 1 0.33333333 0.66666667
Özellik a17 0 1 0.4 0.6	Özellik a17 0 1 0.5 0.5	Özellik a17 0 1 0.33333333 0.66666667
Özellik a18 0 1 0.4 0.6	Özellik a18 0 1 0.5 0.5	Özellik a18 0 1 0.33333333 0.66666667
Özellik a19 0 1 0.2 0.8	Özellik a19 0 1 0.5 0.5	Özellik a19 0 1 0.33333333 0.66666667
Özellik a20 0 1 0.4 0.6	Özellik a20 0 1 0.5 0.5	Özellik a20 0 1 0.33333333 0.66666667
Özellik a21 0 1 0.4 0.6	Özellik a21 0 1 0.5 0.5	Özellik a21 0 1 0.33333333 0.66666667
Özellik a22 0 1 0.4 0.6	Özellik a22 0 1 0.5 0.5	Özellik a22 0 1 0.33333333 0.66666667

Sınıf 0.6: P(C)=0.00485437	Sınıf 0.7: P(C)=0.00485437	Sınıf 0.8: P(C)=0.00485437
Özellik a1 0 1 0.5 0.5	Özellik a1 0 1 0.5 0.5	Özellik a1 0 1 0.5 0.5
Özellik a2 0 1 0.5 0.5	Özellik a2 0 1 0.5 0.5	Özellik a2 0 1 0.5 0.5
Özellik a3 0 1 0.5 0.5	Özellik a3 0 1 0.5 0.5	Özellik a3 0 1 0.5 0.5
Özellik a4 0 1 0.5 0.5	Özellik a4 0 1 0.5 0.5	Özellik a4 0 1 0.5 0.5
Özellik a5 0 1 0.5 0.5	Özellik a5 0 1 0.5 0.5	Özellik a5 0 1 0.5 0.5
Özellik a6 0 1 0.5 0.5	Özellik a6 0 1 0.5 0.5	Özellik a6 0 1 0.5 0.5
Özellik a7 0 1 0.5 0.5	Özellik a7 0 1 0.5 0.5	Özellik a7 0 1 0.5 0.5
Özellik a8 0 1 0.5 0.5	Özellik a8 0 1 0.5 0.5	Özellik a8 0 1 0.5 0.5
Özellik a9 0 1 0.5 0.5	Özellik a9 0 1 0.5 0.5	Özellik a9 0 1 0.5 0.5
Özellik a10 0 1 0.5 0.5	Özellik a10 0 1 0.5 0.5	Özellik a10 0 1 0.5 0.5
Özellik a11 0 1 0.5 0.5	Özellik a11 0 1 0.5 0.5	Özellik a11 0 1 0.5 0.5

Özellik a12		Özellik a12		Özellik a12	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a13		Özellik a13		Özellik a13	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a14		Özellik a14		Özellik a14	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a15		Özellik a15		Özellik a15	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a16		Özellik a16		Özellik a16	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a17		Özellik a17		Özellik a17	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a18		Özellik a18		Özellik a18	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a19		Özellik a19		Özellik a19	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a20		Özellik a20		Özellik a20	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a21		Özellik a21		Özellik a21	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5
Özellik a22		Özellik a22		Özellik a22	
0	1	0	1	0	1
0.5	0.5	0.5	0.5	0.5	0.5

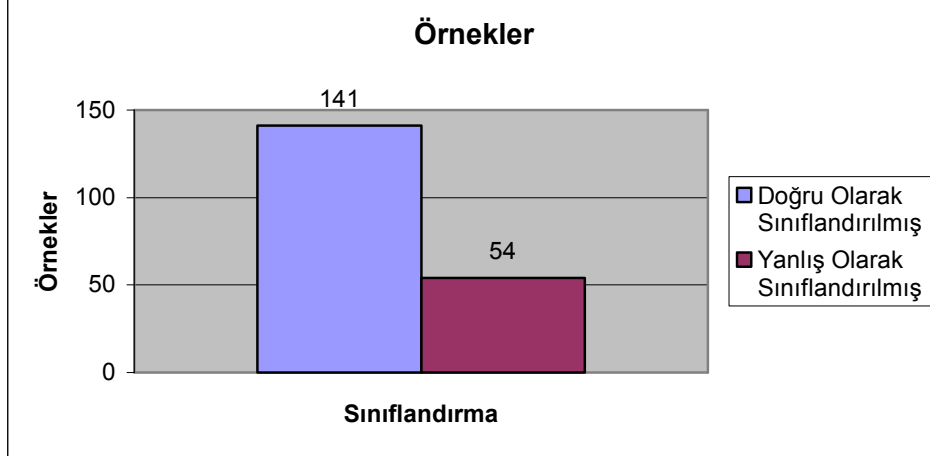
Sınıf 0.9: P(C)=0.00970874		Sınıf 1.0: P(C)=0.04368932	
Özellik a1		Özellik a1	
0	1	0	1
0.33333333	0.66666667	0.3	0.7
Özellik a2		Özellik a2	
0	1	0	1
0.33333333	0.66666667	0.3	0.7
Özellik a3		Özellik a3	
0	1	0	1
0.33333333	0.66666667	0.4	0.6
Özellik a4		Özellik a4	
0	1	0	1
0.33333333	0.66666667	0.5	0.5
Özellik a5		Özellik a5	
0	1	0	1
0.33333333	0.66666667	0.3	0.7
Özellik a6		Özellik a6	
0	1	0	1
0.33333333	0.66666667	0.2	0.8
Özellik a7		Özellik a7	
0	1	0	1
0.33333333	0.66666667	0.6	0.4
Özellik a8		Özellik a8	
0	1	0	1
0.33333333	0.66666667	0.4	0.6
Özellik a9		Özellik a9	
0	1	0	1
0.33333333	0.66666667	0.3	0.7
Özellik a10		Özellik a10	
0	1	0	1
0.33333333	0.66666667	0.2	0.8
Özellik a11		Özellik a11	
0	1	0	1
0.33333333	0.66666667	0.5	0.5

Özellik a12		Özellik a12	
0	1	0	1
0.33333333	0.66666667	0.4	0.6
Özellik a13		Özellik a13	
0	1	0	1
0.33333333	0.66666667	0.5	0.5
Özellik a14		Özellik a14	
0	1	0	1
0.33333333	0.66666667	0.6	0.4
Özellik a15		Özellik a15	
0	1	0	1
0.33333333	0.66666667	0.7	0.3
Özellik a16		Özellik a16	
0	1	0	1
0.33333333	0.66666667	0.5	0.5
Özellik a17		Özellik a17	
0	1	0	1
0.33333333	0.66666667	0.7	0.3
Özellik a18		Özellik a18	
0	1	0	1
0.33333333	0.66666667	0.6	0.4
Özellik a19		Özellik a19	
0	1	0	1
0.33333333	0.66666667	0.5	0.5
Özellik a20		Özellik a20	
0	1	0	1
0.33333333	0.66666667	0.8	0.2
Özellik a21		Özellik a21	
0	1	0	1
0.33333333	0.66666667	0.5	0.5
Özellik a22		Özellik a22	
0	1	0	1
0.33333333	0.66666667	0.7	0.3

Eđitim verisinde ki dođru ve hatalı sınıflandırmalar;

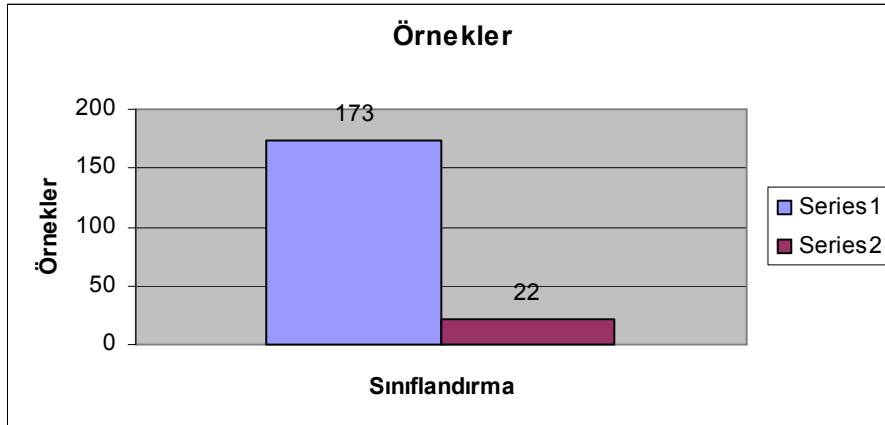
Doğru olarak sınıflandırılmış örnekler	141	72.3077 %
Hatalı olarak sınıflandırılmış örnekler	54	27.6923

Sınıflandırma yapılırken ilk kısımdaki veriyi bölümlere yapmadım çünkü bu aşamadaki veri miktarı bölümlere yapmayı gerektirecek kadar fazla değildir.



Sonuç verileri yukarı şekildeki gibi sınıflandırılırsa elde edilen sonuçlar pek yeterli gözükmemektedir. Sonuçlar $\{0.0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0\}$ arasında olabilir. 0.3 anlamı gelen değerler içerisinde 10 taneden 3 tanesi suçlu 7 tanesi yasal demektir. Amacımız suçlu ve yasal olma olasılıklarını bulmak olacağı için aşağıdaki algoritma sonuç verilerine uygulanmıştır.

Sonuçlar 11 adet olduğu için bu değerlerin evet ve hayıra etkisi teker teker hesaplanıp toplanarak evet ve hayır için bir değer ikilisi oluşturulmuştur. Mesela 0.3 'ün etki edeceği değer evet için 0.3 ile hayır için 0.7 ile çarpılmıştır. Evet ve hayır oranlarını elde etmek için 0.0 ile 1.0 aralığı ayrı ayrı uygulanmıştır. Daha sonra evet ve hayır için elde edilen değerlerin % si hesaplanılarak beklenen değere uyup uymadığı belirlenmiştir. Bu işleme göre grafik aşağıdaki şekilde çıkmıştır.



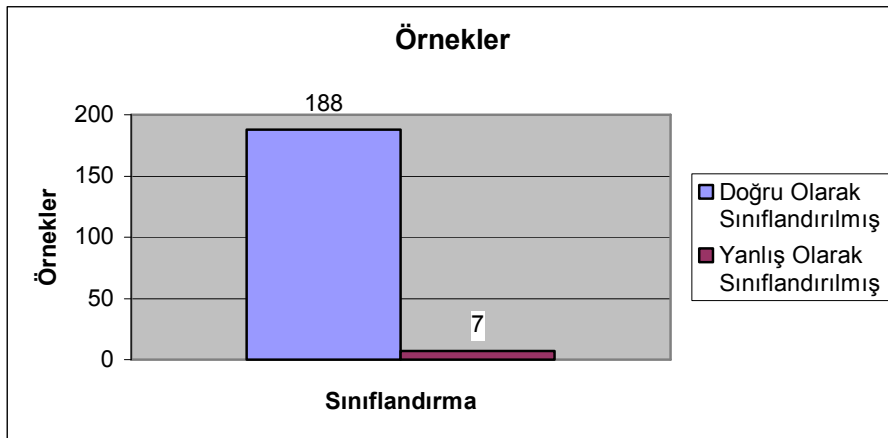
Yukarıdaki grafikte veri karşılaştırılması beklenen ile hesaplanan değerler $\{0.0,1.0\}$ olanların bilgisidir

Sonuçlar üretilirken C4.5 ve Saf Bayes Sınıflandırma sonuç değerlerinden hepsinin “0” veya “1” olması durumunda “0”lar için hayır oranı evet oranından fazla ve “1”ler içinde evet oranı , hayır oranından fazla olması gerektiğinden hatalı sonuçlarda sonuç değeri evet ve hayır sayı oranına göre hesaplanmıştır.(Bu özellik sonuçlar üzerinde kural çıkarma olarak değerlendirilir).

Hatalı sınıflandırılmış veriler aşağıdaki tabloda görülmektedir. Eğer olması gereken değeri {0.0,0.5} arasında ise {0.0} ve {0.6,0.9}arasını 1.0 olarak kabul edersek 15 tane daha değer doğru olarak sınıflandırıldı kabul edilmiştir.

No	C4.5 ve Saf Bayes Sınıflandırma Sonuç Değerleri	Beklenen Değer	Çıkan Sonuç	Evet Oranı	Hayır Oranı	Evet Sayısı	Hayır Sayısı
1	1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,1,0,1,0,1,0	1,0	0,0	49,87	50,13	1	0
2	1,1,1,1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1	0,2	0,0	27,13	72,87	1	4
3	1,1,1,1,0,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1	0,3	0,0	32,57	67,43	1	2
4	0,1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	0,5	0,0	36,07	63,93	1	1
5	0,0,0,1,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0	1,0	0,0	4,29	95,71	1	0
6	1,1,1,1,1,1,1,1,1,1,1,1,0,1,1,0,1,0,0,1,0,1,0	0,0	1,0	52,79	47,21	0	1
7	1,1,0,0,1,1,0,1,0,1,0,1,1,1,1,1,1,1,1,1,1,1	1,0	0,0	34,97	65,03	1	0
8	0,1,1,1,0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,1	1,0	0,0	7,47	92,53	1	0
9	1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,1,0	1,0	0,0	41,27	58,73	1	0
10	1,1,1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	0,3	0,0	30,8	69,2	1	2
11	1,1,1,0,1,1,1,1,1,0,0,0,1,1,1,1,1,1,1,1,1,1	0,5	0,0	44,59	55,41	1	1
12	1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0	0,1	0,0	28,51	71,49	3	14
13	1,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	0,2	0,0	21,43	78,57	2	5
14	1,0,1	0,1	0,0	25,43	74,57	1	5
15	1,0,1,1,1,1,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0	0,5	0,0	10,62	89,38	1	1
16	0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,1	0,0	1,13	98,87	1	6
17	0,0,1,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,1	0,0	1,68	98,32	1	5
18	1,1,1,1,1,1,0,1,0,1,0,1,1,1,1,1,1,1,1,1,1,1	0,5	0,0	41,42	58,58	1	1
19	1,0,0,0,0,0,1,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0	0,1	0,0	3,79	96,21	1	7
20	1,1,1,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,1,0,0,0	0,3	0,0	32,68	67,32	1	2
21	1,0,1,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0	1,0	0,0	5,37	94,63	1	0
22	1,1	0,9	1,0	93,62	6,38	440	30

Gri renkte olan satırlar yanlış , diğerleri ise doğru olarak sınıflandırılmış örnekleri göstermektedir. Buna göre 195 örnekten 7 tane yanlış 188 tane ise doğru olarak sınıflandırılmıştır.



10 SONUÇ ve ÖNERİLER

10.1 Tez Çalışmasının Özeti

İnternet Bankacılığı günümüz de yaygın olarak kullanılmaktadır. Tez kapsamında İnternet Bankacılığında oluşabilecek suçlu kayıtlarının tespit işlemleri gerçekleştirilmiştir. Bu işlemleri yaparken kümeleme,bölümleme , sınıflandırma algoritmaları kullanılmıştır.

Kümeleme algoritması ile kullanıcıların belli gruplara atanması sağlanmıştır. Böylece kullanıcılarda var olmayan dolandırıcılık işlemi , eğer atandığı grupta var ise onlarda da olmuş gibi işleme alınmıştır. Kişi bazlı sistem daha özel olduğu için herhangi bir dolandırıcılık işlemi diğer kişi için uygulamaya alınmaz. Bu sebepten dolayı gruplara atama yapılmaktadır. Gruplama ile gerçekleştirilen her bir işlemde gerçekleştiren müşteri numarası yerine müşteri grup bilgisi yer almıştır.

Bölümleme algoritması ile yapılan işlemler belli sayıda parçalara bölünmüştür. Her bir bölümdeki veriler rasgele olarak seçilip , varolan suçlu verileri parçalanmadan, bütün halinde bölümlere eklenmiştir. Böylece bölümlerdeki suçlu ve yasal veri sayı oranları dengelenmiştir.

Bölümlenen veriler Saf Bayes sınıflandırıcı ile C4.5 Sınıflandırma algoritmaları ile sınıflandırılır. Elde bulunan tüm veriler(bölümleme yapılmadan önceki yasal ve suçlu verileri) sırasıyla her bir bölüme uygulanarak sonuçlar oluşturulur.

Oluşan sonuçlar beklenen sonuç (yasal ve suçlu için) sayıları eklenerek tekrar Saf Bayes Sınıflandırıcıya sokularak bir sonuç elde edilir. Dolandırıcılık Tespit Sistemi; para transferi yapan müşterinin dolandırıcı mı olup olmadığına % olarak evet veya hayır cevabını vermektedir.

10.2 Çalışmanın Getirileri, Sağladığı Katkılar

Bu tez çalışmasının birincil katkısı kümeleme,bölümleme ve sınıflandırma algoritmaları ile İnternet Bankacılığında yapılan dolandırıcılık işlemlerini mümkün mertebe azaltmayı sağlamasıdır. Bu sistem önleyici bir yapıya sahiptir, yani müşteri işleminin onaylanmadan önce kontrolünü yapmaktadır. Oluşan sonuca göre eğer suçsuz ise onay verip, suçlu ise onay vermemektedir. Böylece müşteri memnuniyeti sağlanarak bankanın müşterisini kazanması, dolandırıcılıktan dolayı maddi yönden zararın azalması, suçlulara karşı caydırıcı bir etkinin oluşması sağlanmıştır.

10.3 Gelecekte Yapılabilecekler

Gelecekte, daha işlevsel olması açısından sisteme yeni fonksiyonlar ve yetenekler kazandırmak gerekebilir. Uzun dönemli planlamalarla, sınıflandırıcı kısmına yeni sınıflandırıcılar eklenebilir. Böylece sistem diğer sınıflandırıcıları da kullanarak daha etkili sonuçlar elde edilebilir. Sınıflandırıcılardan çıkan sonuçların sınıflandırılmasında Saf Bayes Sınıflandırıcı yerine , C4.5 veya Yapay Sinir Ağları kullanılabilir.

10.4 Sonuç

Bu tez çalışması ile İnternet Bankacılığında oluşan dolandırıcılık işlemlerini önleyen bir sistem tasarlanmıştır. İnternet Bankacılığında 01/01/2004 ile 01/01/2007 tarihleri arasındaki 571 adet müşteriye ait 12773 adet parasal işlem incelemeye alınmıştır.

571 adet müşteriye ait bilgilere göre gruplandırma yapıp 16 tane grup oluşturulmuştur. Bu gruplardan grup52'ye ait 6910 tane yasal, 466 tane suçlu kayıt Dolandırıcılık Tespit Sisteminde işleme alınmıştır.

7376 adet veri 11 bölüme ayrılıp, C4.5 ve Saf Bayes Sınıflandırıcılara sokulmuştur. Bu işlem sonucunda 195 adet veri oluşmuştur, sonuçlar {0.0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0} arasında olmaktadır. Bu veriler direk Saf Bayes Sınıflandırıcıya sokulduğunda 141 adet doğru , 54 adet yanlış sınıflandırılmıştır. Sonuçlar 11 adet olduğu için bu değerlerin evet ve hayıra etkisi teker teker hesaplanıp toplanarak evet ve hayır için bir değer ikilisi oluşturulmuştur. Bu işlem sonucunda 195 örnekten 7 tane yanlış 188 tane ise doğru olarak sınıflandırılmıştır. Bu da 7376 adet veriden sadece 54 tanesi yanlış sınıflandırılmıştır. Oran olarak %0,7 oranında yanlış sınıflandırma yapılmıştır.

Oluşturulan veriler grafiksel olarak anlatıldıktan sonra bu verilerin sisteme girilip ara yerdeki sonuç bilgileri detaylı bir şekilde anlatılmıştır. Adım adım anlatılan bu sistemle sonuç bilgisi ile beklenen sonuç bilgileri karşılaştırılıp %0,7 oranda hata ile sonuçlandırılmıştır.

Bu sistem bir işlemin suçlu olup olmadığına önceki verileri inceleyerek karar verdiği için eğitim kümesi son derece önemlidir. Şuan için İnternet Bankacılığında kullanımına yönelik oluşturulmuş olmasına rağmen küçük değişikliklerde sigorta, kredi kartı vb. alanlarda da etkili olarak kullanılabilir.

11 KAYNAKLAR

- 1.) Von Altrock C (1995) Fuzzy Logic and NeuroFuzzy Applications in Business and Finance, Prentice Hall, NJ, USA, pp286-294.
- 2.) Cox E(1995)"A Fuzzy System for Detecting Anomalous Behaviours in Healthcare Provider Claims", in Goonatilake S and Treleaven P(eds), in Intelligent Systems for Finance and Business, John Wiley and Sons, Chichester, England, pp111-134
- 3.) Maes S, Tuyls K, Vanschoenwinkel B and Manderick B(2002)"Credit Card Fraud Detection Using Bayesian and Neural Networks", in Proceedings of NF2002, Havana Cuba.
- 4.) Chan P, Fan W, Prodromidis A and Stolfo S(1999)"Distributed data mining in credit card fraud detection", IEEE Intelligent Systems, 14, pp67-74.
- 5.) Brause R, Langsdorf and Hepp M(1999)"Neural Data Mining for Credit Card Fraud Detection", in Proceedings of 11th IEEE International Conference on Tools with Artificial Intelligence, Illinois, USA.
- 6.) Weatherford M(2002)"Mining for Fraud", IEEE Intelligent Systems, July/August Issue, pp4-6.
- 7.) Cahill M, Lambert D, Pingeiro J and Sun D(2002)"Detecting Fraud In The Real World", in The Handbook of Massive datasets, Kluwer Academic Publishers, pp911-930.
- 8.) Abagnale F(2001) The Art of the Steal: How to Protect Yourself and Your Business from Fraud, Transworld Publishers, NSW, Australia.
- 9.) Brachman R J and Anand T(1996)"The Process of Knowledge Discovery in Databases", in Fayyad et al(eds), in Advances in Knowledge Discovery and Data Mining, AAAI Press, USA.
- 10.) Chan, K. C. C. and Wong, A. K. C., 1991, A statistical technique for extracting significant knowledge from databases, In Knowledge Discovery In Databases (G. Piatetsky-Shapiro and W. J. Frawley, eds.), pp. 107-123, Cambridge, MA: AAAI/MIT.
- 11.) Fayyad, P. S. U. M., Piatetsky-Shapiro, G. and Uthurusamy, R., 1996a, Advances in knowledge discovery and data mining, Cambridge, MA: MIT Press. Fayyad, P.S.U. M., Piatetsky-Shapiro, G. , 1996b, The KDD process for extracting useful knowledge from volumes of data, Communications Of ACM 39, 11, 27-34.
- 12.) Witten I and Frank E(1999) Data Mining: Practical Machine Learning Tools and Techniques with Java, Morgan Kaufman Publishers, CA, USA.
- 13.) Quinlan J R(1993) C4.5 Programs for Machine Learning, Morgan Kaufman, CA, USA.
- 14.) Chan P and Stolfo S(1995)"A Comparative Evaluation of Voting and Meta-learning on Partitioned Data", in Proceedings of 12th International Conference on Machine Learning, pp90-98.
- 15.) Alpaydın, E., 1999, Zeki veri madenciliği: Ham veriden altın bilgiye ulaşma yöntemleri, www.cmpe.boun.edu.tr/~ethem/files/papers/veri-maden_2k-notlar.doc.
- 16.) Frawley, W. J., Piatetsky-Shapiro, G., Matheus, C. J., 1991, Knowledge discovery databases: An overview, In Knowledge Discovery In Databases (G. Piatetsky-Shapiro and W. J. Frawley, eds.), Cambridge, MA: AAAI/MIT pp. 1-27.
- 17.) Fayyad, P. S. U. M., Weir, N., Djorgovski, S.G., 2000, Mart 22, Automated analysis of a large-scale sky survey: The SKI CAT System, <http://techreports.ipi.nasa.gov/1993/93-0597.pdf>.
- 18.) Holsheimer, M. and Siebes, A.P J. M., 1994, Data mining: the search for knowledge in databases., Technical Report CS-R9406, CWI, P .0. Bo x 94079, 1090 BG Amsterdam, The Netherlands.

- 19.) Frawley, W. J., Piatetsky-Shapiro, G., Matheus, C. J., 1991, Knowledge discovery databases: An overview, In Knowledge Discovery In Databases (G. Piatetsky-Shapiro and W. J. Frawley, eds.), Cambridge, MA: AAAI/MIT pp. 1-27.
- 20.) Matheus, C. J., Chan, P. K., and Piatetsky-Shapiro, G., 1993, Systems for knowledge discovery in databases, IEEE Trans. On Knowledge And Data Engineering, vol. 5, no. 6, pp. 903-912.
- 21.) Corinna, C., Drucker, H., Hoover, D. and Vapnik, V., Capacity and complexity control in predicting the spread between harrowing and lending interest rates, In The First International Conference on Knowledge Discovery and Data Mining (U. Fayyad and R. Uthurusamy, eds.), (Montreal, Quebec, Canada), pp. 51-76, aug 1995.
- 22.) Zhong, N. and Ohsuga, S., 1994, Discovering concept clusters by decomposing databases, Data & Knowledge Engineering, vol. 12, pp. 223-244.
- 23.) Shapiro, G. P. and Matheus, C. J., 1992, Knowledge discovery workbench for exploring business databases, International Journal of Inteldigent Systems, vol. 7, pp. 675-686.
- 24.) Elder-IV, J. F. and Pregibon, D., 1995, August, A statistical perspective on KDD, In The First International Conference on Knowledge Discovery and Data Mining (U. Fayyad and R. Uthurusamy, eds.), (Montreal, Quebec, Canada), pp. 87-93.
- 25.) Fayyad, U. M. and Irani, K. B., 1993, Multi interval discretization of continuous Özelliks for Smifification learning, In Proceedings of I3th International Joint Conference on Artificial Intelligence (R. Bajcsy, ed.), pp. 1022-1027, Morgan Kauffmann.
- 26.) Quinlan, J. R., 1986, Induction of decision trees, Machine Learning, vol. 1, pp. 81- 106.
- 27.) Grzymala-Busse, J. W., 1991, On the unknown Özellik values in learning from examples, In Proceedings of Methodologies for Intelligent Systerrzs (Z. W. Ras and M. Zemanikowa, eds.), Lecture Notes in AI, New York: Springer-Verlag, 542, pp. 368-377.
- 28.) Thiesson, B., 1995, August, Accelerated quantification of bayesian networks with incomplete data, In The First International Conference on Knowdedge Discovery and Data Mining U. Fayyad and R. Uthurusamy, eds.), Montreal, Quebec, Canada, pp. 306-311.
- 29.) Kira, K. and Rendeli, L., 1992, The feature selection problem; Tradational methods and a new algorithm, In Proceedings of AAAI 92, AAAI Press pp. 129-134.
- 30.) Almuallim, H. and Dietterich, T., 1991, Learning with many irrelevant features, In Proceedings of AAI 91, (Menlo Park, CA), AAAI Press, pp. 547-552.
- 31.) Pawlak, Z., Slowinski, K., and Slowinski, R., 1986, Rough Smifification of patients after highly selective vagotomy for duodenal ulcer, International Journal Of Man-Machine Studies, vol. 24, pp. 413-433.
- 32.) Simoudis, E., October 1996, Reality check for data mining, In IEEE Expert: Intelligent Systems and Their Applications , pages ll(5):26-33.
- 33.) Weiss, S. M. and Kulikowski, C. A., 1991, Computer systems that learn: Smifification and prediction methods from statistics, Neural Nets, Machine Learning, and Expert Systems , Morgan Kaufman.
- 34.) Michalski, R. S. and Stepp, R. E., 1983, Learning from observation: Conceptual clustering, In R. S. Michalski, J. G. Oneli C., and Mite T. M., hell editors, Machine Learning: An Artificial Intelligence Approach , Vol 1, Morgan Kaufmann, pp 331-363.
- 35.) Agrawal, R., Imielinski, T. and Swami, A., May 1993, Mining association rules between sets of items in farge databases, In ACM SIGMOD Conf. Management of Data.
- 36.) Seidman, C., 2000, Data Mining with Microsoft SQL Server 2000, Microsoft Press.
- 37.) Agrawal, R. and Srikant, R., 1995, Mining sequential patterns, In l Ith Intl. Conf. on Data Engg.
- 38.) Piatetsky-Shapiro, G., 1994, An overview of knowledge discovery databases: Recent progress and challenges. In W. P . Ziarko, editör, Rough Sets, Fuzzy Sets and Knowledge. Discovery.

Proceedings of the International Workshop on Rough Sets and Knowledge Discovery (RSKD'93), Berlin, Germany, Springer-Verlag, pages 1-10.

- 39.) Agent-Based Distributed Learning Applied to Fraud Detection Andreas L. Prodromidis and Salvatore Stolfo Department of Computer Science Columbia University
- 40.) A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL IN AN INTEGRATED SUPPLY CHAIN Vasiliu, Lucian, Deakin University,
- 41.) Neural Data Mining for Credit Card Fraud Detection
- 42.) Data Mining: Concept and Techniques Jiawei HAN kitabı, Nevcihan DURU ders notları
- 43.) R. Brause, T. Langsdorf, M. Hepp J.W.Goethe-University, Frankfurt a. M., Gesellschaft f. Zahlungssysteme GZS, Frankfurt a. M., Germany, Credit Card Fraud Detection by Adaptive Neural Data Mining.
- 44.) Fraud Detection for Online Retail using Random Forests Eric Altendorf, Peter Brende, Josh Daniel, Laurent Lessard, 2005.
- 45.) Distributed Data Mining in Credit Card Fraud Detection Philip K. Chan, Florida Institute of Technology Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo, Columbia University, 1997.
- 46.) Maximum likelihood continuity mapping for fraud detection John Hogden, 1997.
- 47.) Veri Tabanlarında Bilgi Keşfine Formel Bir Yaklaşım; Hayri SEVER, Buket OĞUZ.
- 48.) <http://www.ankara.pol.tr/?id=606>
- 49.) <http://www.bilgisayarpolisi.com/>
- 50.) www.sekerbank.com.tr