

Ege Eğitim Teknolojileri Dergisi

Journal of Ege Education Technologies

Sayı 2, Cilt 2, Aralık 2018, Sayfa 44- 54



Bilişim Suçları ve Psikolojik Etkileri Açısından Türkiye’de Telefon Dolandırıcılığının Etkin Analizi¹

Egemen Tekkanat

*Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu,
egementekkanat@trakya.edu.tr*

Murat Topaloğlu

*Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu,
murattopaloglu@trakya.edu.tr*

Okan Yılmaz

*Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu,
okanyilmaz@trakya.edu.tr*

Geliş Tarihi: 07.10.2018

Kabul tarihi: 23.12.2018

Yayınlanma Tarihi: 31.12.2018

Özet

Bilgisayar ve mobil teknolojilerin hızlı gelişimi ile birlikte kişilere ait özel verilerin elektronik ortamlarda depolanması dolandırıcılık faaliyetinin en büyük sebeplerinden biri olarak gösterilebilir. Dolandırıcılar aradıkları mağdurlara kendilerini çeşitli kamu ve özel meslek gruplarından biri gibi tanıtmaktadır. Bu kişiler çeşitli manipülasyon teknikleri kullanarak mağdurlara maddi ve manevi zararlar vermektedir. Teknolojik yenilikler ile birlikte hukuksal altyapının aynı paralellikle ilerlememesinden dolayı dolandırıcılar hukuksal boşlukları değerlendirerek dolandırma faaliyetlerine başlamaktadırlar. Günümüzde sayılarının hızla arttığı dolandırıcı ve dolandırılma faaliyetlerinin birçok örneği vardır. Bu çalışmada dolandırılma işlemine maruz kalmış kişilerden veri seti oluşturulmuştur. Kişisel olabilecek her türden bilgi veri setinden çıkarılmıştır. Çalışmamız bu olaya bilişim suçları ve bireylerin psikolojik yönleri açısından da yaklaşmaktadır. Yapılan uygulamada veri madenciliği yöntem ve algoritmaları kullanılmış ve analiz sonuçları aktarılmıştır.

Anahtar Kelimeler: bilişim suçları, mobil teknolojiler, telefon dolandırıcılığı, veri madenciliği

¹ Bu bildiri 12. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumunda bildiri olarak sunulmuştur.

Ege Eğitim Teknolojileri Dergisi

Journal of Ege Education Technologies

Volume 2, Issue 2, December 2018, Pages 44- 54



Effective Analysis of Telephone Fraud in Turkey in Terms of Cyber Crimes and Its Psychological Effects

Abstract

The electronic storage of personal and private data as a result of the swift advance of computer and mobile technologies can be counted among the primary reasons of fraud activity. Fraudsters introduce themselves as someone from different public or private professional groups. Those people cause material or moral damage to the victims by employing several manipulation techniques. Fraudsters have begun the fraud activities by benefiting from legal gaps since the legal infrastructure does not improve as fast as the technological innovations. There are a lot of examples of fraudsters and fraud activities expanding in size today. In this study, the data set is compiled through the interviews with people who suffered before from fraud activities. Any personal information is removed from the data set. The present study addresses this activity also with respect to cyber crimes and the psychological aspects of individuals. In the research, the data mining method and algorithms are employed and the analysis results are reported.

Keywords: cyber crimes, mobile technologies, telephone fraud, data mining

Giriş

Teknolojinin son yıllarda tüm dünyada hızla gelişmesi, insanların bu hızı etkili bir şekilde kullanarak tüm ihtiyaçlarını sanal platformda gerçekleştirme potansiyelini arttırmaktadır (Akbal ve Diğ., 2017).

Özellikle mobil telefonlar taşıma kolaylığı sağlamak ve böylece bilgisayar, tablet gibi cihazları taşıma gereği duymadan teknolojiyi rahatlıkla takip etmemizi sağlamaktadır. İletişim ihtiyacının dışında bankacılık, haber takip etme, oyun oynama, sosyal platformları kullanma gibi amaçlarda da kullanılabilir. Bu sebeple günümüzde yaygın bir şekilde kullanılan akıllı telefonlar dolandırıcılık faaliyetlerinde özellikle seçilen cihazların başında gelmektedir (Thomas ve Diğ., 2004).

Dünya üzerinde bilgi miktarının her geçen gün katlanarak arttığı günümüzde, veri tabanlarının sayısı da benzer, hatta daha yüksek bir oranda verilerin dijital ortamda saklanma ihtiyaca bağlı olarak sürekli olarak artmaktadır.

Buna bağlı olarak ülkemizde sıkça rastlanan olgulardan veri kaybı ve veri hırsızlığı hızla gelişen teknoloji dünyasında verilerin elektronik olarak kayıt altına alınmasından ve alınan bu kayıtların yeterli ve geçerli bir koruma ile korunamıyor olmasından kaynaklanmaktadır. Dolandırıcılık faaliyetlerinde dolandırıcıların ellerinde ki verilerin neredeyse tamamı insanların kendi bilgi ve iradesi ile alınan veriler olduğundan dolayı dolandırıcılar rahatlıkla bu verileri çeşitli alanlarda kullanabilmektedirler. Maddi ve manevi olarak insanları büyük zarara uğratan örgüt ve gayri resmi kuruluşlar ülkemiz toplumunda büyük huzursuzluğa yol açmaktadır.

Telefon dolandırıcıları gerçekleştirdikleri faaliyetlerinde sosyal mühendislik ve resmi belge ele geçirme gibi yöntemler kullanmaktadırlar. Bu yöntemleri ile veri toplama işlemi sonrasında elde ettikleri veriler ile tespit ettikleri insanları amaçları doğrultusunda yönlendirmeye çalışır (Thomas ve Diğ., 2004).

Bu çalışmadaki amaç, veri madenciliği kavram ve algoritmaları kullanılarak ülkemizde gerçekleştirilen telefon dolandırıcılığı faaliyetlerini incelemek ve bu dolandırıcılık işlemleri arasında çeşitli sebep sonuç ilişkileriyle birlikte farklı bağıntıların ortaya çıkarılması olarak belirlenmiştir.

Veri Madenciliği

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

Veri madenciliği birçok teknoloji arasında bağlantı görevi gören çok disiplinli bir alandır. Bu teknolojiler arasında veri tabanı teknolojisi, istatistik, yapay zekâ makine öğrenimi yer almaktadır (Ertuğrul, Organ ve Şavlı, 2013).

Veri madenciliği günümüzde birçok farklı alanda ve farklı amaçla kullanılmaktadır. Bunlar pazarlama, bankacılık, finans, biyoloji, tıp, meteoroloji, atmosfer bilimleri, reklamcılık ve sosyal bilimler olarak sıralanabilir (Ertuğrul, Organ ve Şavlı, 2013).

Veri madenciliğinin kökeni ENIAC (Electrical Numerical Integrator And Calculator)’a kadar dayanmaktadır. 1946 yılında geliştirilen ve bugün kullandığımız kişisel bilgisayarların atası olan ENIAC, ABD’li bilim adamları John Mauchly ve J. Presper Eckert tarafından, II. Dünya Savaşı sırasında ABD ordusu için geliştirilmiştir (Karacan ve Yeşilbudak, 2010).

Literatür Çalışması

Kılıçarslan (2013) tarafından yapılan çalışmada; Türkiye’deki GSM sektörü genel hatlarıyla ele alınmıştır. Sektörün hacmi, yatırımlar ve istihdam, operatörler ve özellikleri açıklanmıştır. Sektörün bu yönü açıklandıktan sonra, bu sektörden yasadışı yollarla kazanç elde etmek isteyen şahısların, uyguladıkları yöntemler belirtilmiştir. Bunun yanında GSM sektörünü de dolandırıcılık konularını içine alan mevcut kanunlar ve düzenlemeler belirtilmiştir. Operatörlerin satış kanallarından biri olan alternatif satış kanallarında meydana gelen sahtekârlık girişimlerinin nasıl engelleneceği üzerinde durulmuştur. Bununla beraber, müşteri bilgi ve belge güvenliği konularına değinmiştir (Kılıçarslan,2013).

Özcan (2014) tarafından yapılan çalışmada; veri madenciliği teknolojisi güvenlik uygulamaları açısından incelenmiş, bu konu ile ilgili hile, dolandırıcılık ve sahtekârlık kavramları üzerinde durulmuş, konu hukuki boyutları ile ele alınmıştır. Sahtekârlık konusunda ise çalışanların rolüne değinilmiş, bu konudaki standartlar incelenmiş ve sağlık sigortası sektöründe gerçek verilerden hareketle sahtekârlık tespitlerinin bulunarak öğrenici model uygulamasının kullanıldığı bir çalışmanın incelemesi yapılmıştır (Özcan, 2014).

Tavacı (2011); GSM sektörlerindeki sahtekârlık yönetimi için, müşteri verilerinin sınıflandırılması problemi üzerinde durulmuş ve sahtekârlık çeşitlerinden olan abone sahtekârlığı (invoice) incelenmiştir. Müşteri bilgileri olarak; yaş, cinsiyet, abonelik yaşı, ortalama aylık fatura tutarı, ortalama aylık kullanılan sms sayısı, geç ödenen fatura sayısı, son borç durumu, sondan 3. fatura ödemesi, sondan 2. fatura ödemesi, son fatura ödemesi ve fraud mu abone bilgilerine sınıflandırma yöntemleri uygulanmıştır. Sahtekârlığın kesin tanısının konulmasında ise, abonelerin ödeme ve ödememe durumları göz önünde bulundurulmuştur. Çalışmada uygulanan sınıflandırma yöntemleri; Weka 3.7.1 (Witten & Frank, 2005) veri madenciliği ara yüzü ile; Karar Ağaçları, Çok Katmanlı Algılayıcı, Bayes Kuralı, Bayesian Ağları, Part, Zeror, Oner, Rbf Ağları' dir. MATLAB 7.8.0 (R2009a) (Moler, 2008) Bulanık Mantık aracı kullanılmıştır. Uygulanan sınıflandırma yöntemleri neticesinde; Bulanık Mantık ile diğer sınıflandırma yöntemlerinin performansları kıyaslanmıştır. Yapılan çalışmalar sonucunda, Bulanık Mantık çalışmasının performansının diğer sınıflandırma yöntemleri olan, Karar Ağaçları, Çok Katmanlı Algılayıcı, Bayes Kuralı, Bayesian Ağları, Part, Zeror, Oner, Rbf Ağları' na göre daha tutarlı ve güvenilir olduğu gözlemlenmiştir (Tavacı, 2011).

Ekinci T (2009); Son yıllarda oldukça yaygınlaşan ve önemi artan Veri Madenciliği, büyük veri kümeleri içindeki gizli kalmış, anlamlı bilgiyi ortaya çıkarma sürecidir. Veri madenciliğinin yaygın olarak kullanıldığı önemli alanlardan biri Müşteri İlişkileri Yönetimidir. Müşteri İlişkileri Yönetimi, müşterilerin elde tutulmasına, onlarla olan ilişkilerin geliştirilmesine ve müşteri memnuniyetinin arttırılmasına odaklanan bir yaklaşımdır. Veri Madenciliği ve Müşteri İlişkileri Yönetimi kavramlarını tanıtmak ve bunun yanı sıra telekomünikasyon sektöründe bir veri madenciliği modeli uygulamasını gerçekleştirmektir. Çalışma, telekomünikasyon sektöründe bir firmanın ayrılma eğilimi gösteren

müşterilerinin profilini belirleyerek; bu müşterilere özel pazarlama stratejileri geliştirilmesini hedeflemektedir. Ayrılacak müşteri profilini belirlemek için sınıflama teknikleri kullanılmış ve uygulamanın sonuçları sunulmuştur.

Özbay E (2007) tarafından yapılan çalışmada; İnternet bankacılığında yapılan dolandırıcılık işlemlerinin, veri madenciliği teknik ve metotları kullanılarak belli ölçülerde önlenmesinin sağlanması üzerinde durulmuş ve internet bankacılığındaki müşteri işlemleri incelenmiştir. Bu işlemler için elde edilmiş olan eğitim verileri parçalara ayrılarak sınıflandırılmış ve elde edilmiş olan parçalar için C4.5 ve Saf Bayes Sınıflandırıcı uygulanmıştır.

Yöntem

Bu çalışmadaki veriler karar ağacı yöntemi kullanılarak analiz edilmiştir. Karar ağacı yönteminde veriler sınıflandırılırken veri yığını, eğitim ve test verisi olmak üzere ikiye ayrılır ve eğitim verisi ile öğrenme işlemi sağlanır (Akbal, Doğan ve Varol, 2017).

Karar ağaçları sınıflandırma problemlerinin çözümlenmesinde en çok tercih edilen algoritmalarından birisidir. Var olan diğer uygulamalar ile kıyaslandığı zaman karar ağaçlarının yapılandırılması kolay ve basit bir uygulamadır denilebilir. Bu teknikte sınıflandırma için bir ağaç oluşturulur. Daha sonra, veri tabanındaki her bir kayıt bu ağaca uygulanır ve çıkan sonuca göre bu kayıt sınıflandırılır. Temel olarak iki adımdan oluştuğu söylenebilir; Birincisi ağacın kurulması, ikincisi de verilerin teker teker ağaca uygulanarak sınıflandırmanın gerçekleşmesi şeklindedir (Silahtaroğlu, 2008). Bu çalışmada WEKA programından yararlanılmıştır.

WEKA bir proje olarak başlayıp bugün dünya üzerinde birçok insan tarafından kullanılmaya başlanan bir Veri Madenciliği uygulaması geliştirme programıdır. WEKA java platformu üzerinde geliştirilmiş açık kodlu bir programdır (Dener, Dörterler ve Orman, 2009).

Dünyada ve ülkemizde teknoloji ve mobil iletişim ağı ve hizmetleri çok hızlı bir şekilde gelişme göstermektedir. Özellikle ülkemizde son 5 yıldır etkin bir şekilde faaliyetlerini sürdüren telefon dolandırıcılarını dolandırma başarıları her geçen gün katlanarak artmaktadır.

Gelişen teknolojiler ile birlikte bilgilerin elektronik ortamlarda taşınması getirdiği kolaylık ve kullanılabilirliğin yanında hayati derecede önemli sorunları beraberinde getirmektedir. Kişiyi özel bilgi ve belgelerin 3.cü şahıslar tarafından zoraki veya kişinin bilgisizliğinden ötürü ele geçirilmesinden sonra bu bilgileri kişinin maddi ve manevi zararına kullanan dolandırıcılar her yıl ülkemizde binlerce kişiyi mağdur etmekte ve kişisel özlük haklarını taciz etmektedirler.

Her geçen gün telefon dolandırıcılığı üzerine sayısız dava açılmakla beraber artan teknoloji ve iletişim sektöründeki değişimler aynı hızla hukuksal olarak bir paralellik göstermemekle beraber sahtekârlara yeterli caydırıcılığı sağlamamaktadır.

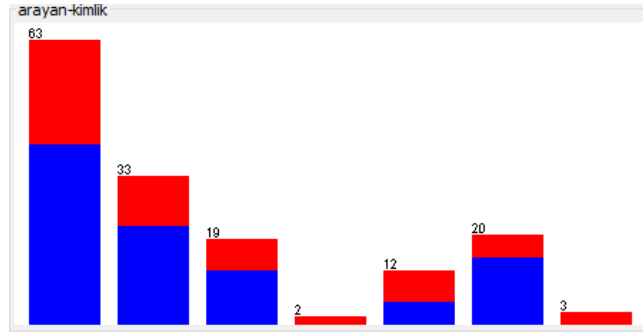
Telefon dolandırıcılığı ve mobil iletişimde sahtekârlık konuları halk arasında fazla önemsenmediği gibi gerekli bilgilendirme ve eğitimler sadece teorik çalışmaların ötesine geçemediği için bu dolandırıcılar gün geçtikçe yaptığı etik olmayan davranışlarını sürdürmekte ve vatandaşlarımızı taciz etmektedirler.

Bu çalışmada telefon dolandırıcılığı suçlarına maruz kalmış maddi manevi zarara uğramış veya uğramamış kişilerce karşılıklı olarak yapılan görüşmeler sonrasında Türkiye’ de yapılan telefon dolandırıcılığı faaliyetleri veri olarak kullanılarak günümüzde sayıları hızla artan telefon dolandırıcılığı suçları incelenmiştir.

Veri toplama, insanların belli bir süre sanal ortamda takip edilmesi ile elde edilen verilerin depolanması sürecidir (Thomas ve Diğ. ,2004). Veri toplamak için çeşitli internet sitelerindeki verilerinden yararlanılmıştır. Elde edilen verileri işlemek için karar ağacı teknolojisinden yararlanılmıştır.

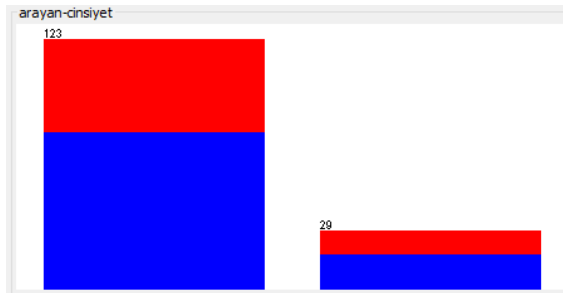
Bulgular

Kullanılan verilerde arayan kimlik niteliğinde 63 polis,33 savcı,19 pazarlamacı,2 asker 12 mit,20 banka ve 3 sigortacı telefon dolandırıcısı bulunmaktadır.



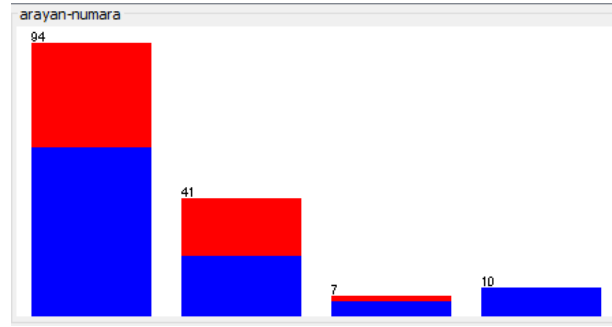
Şekil 1:Arayan Kimlik Dağılımları

Arayan kişinin cinsiyeti 123 bay ve 29 bayan olarak incelenmiştir.



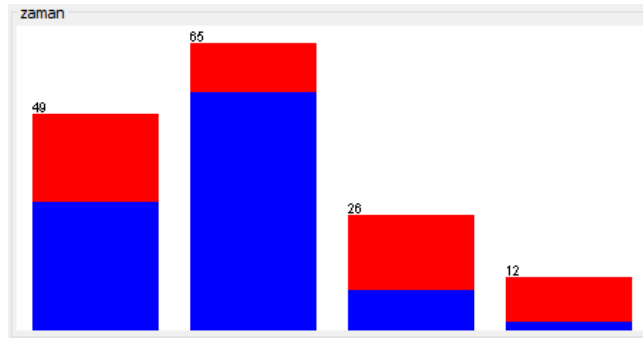
Şekil 2:Arayan Kişinin Cinsiyet Dağılımları

Arayan Numara bilgileri 94 GSM, 41 sabit, 7 444'lü Numara ve 10 tanesi 0850 hat üzerinden yapılmıştır.



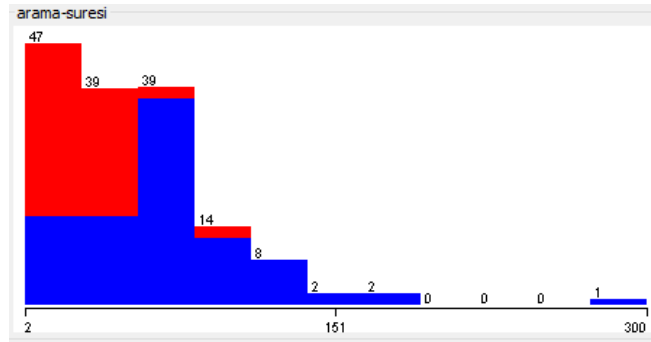
Şekil 3: Arayan numaranın hatlara göre dağılımı

Aranılan zamana göre 49 kişi sabah, 65 kişi öğlen 26 kişi akşam ve 12 kişi ise gece aranmıştır.



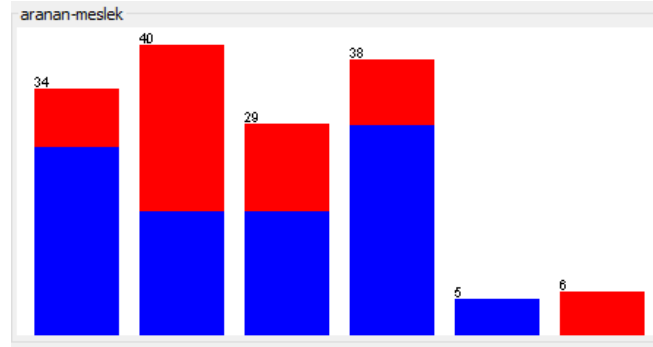
Şekil 4 : Aranılan Zamana göre veri dağılımları

Arama süresine göre veri dağılımları 2 dakika ile 151 dakika arası 149 kişi 152 dakika ile 300 dakika arası ise 3 kişinin arandığı gözlenmektedir.



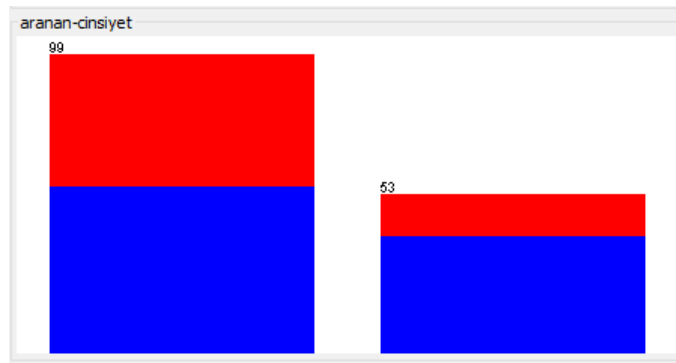
Şekil 5: Arama süresine göre kişi dağılımları

Dolandırıcılar tarafından aranan mesleklere göre kişilerin dağılımları 40 özel sektör, 34 kamu çalışanı 29 işsiz 38 emekli 5 çocuk ve 6 öğrenci olarak dağılmaktadır.



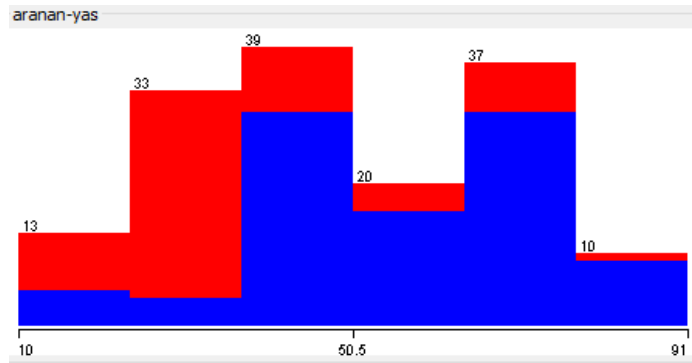
Şekil 6 :Telefon Dolandırıcıları tarafından aranan mesleğe göre kişi dağılımları

Dolandırıcılar tarafından ulaşılan kişilerin 99’u kadın 53’ü erkek olarak incelenmiştir.



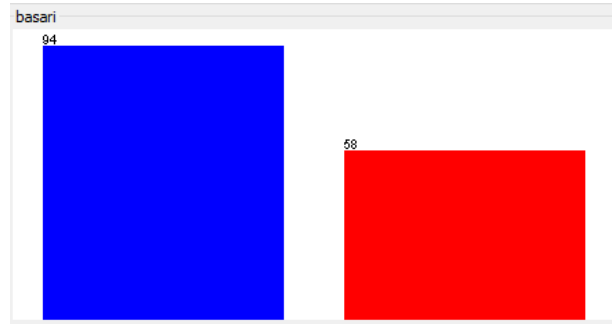
Şekil 7 :Aranan cinsiyet bilgilerine göre kişi dağılımları

Dolandırıcılar tarafından ulaşılan kişilerin yaş dağılımları 10 ile 50,5 arası 85 kişi 51 ve 91 yaşları aranan kişilerin sayısı ise 67 olarak incelenmiştir.



Şekil 8 : Aranan yaş bilgilerine göre kişi dağılımları

Son olarak bu dolandırıcılık faaliyetinde dolandırıcıların ulaştıkları başarı normları 94 başarılı ve 58 başarısız olarak incelenmiştir.



Şekil 9: Başarı Grafiği

Çalışma sırasında elde edilen veriler düzenlenerek WEKA programının arff uzantılı dosyalarına kayıt edilir. Arff formatına göre düzenlenen veriler program üzerinden tanıtılarak WEKA'nın görselleştirme paneli üzerinden görünerek açılmaktadır.

```
polis,bay,gsm,ogle,10,emekli,bay,61,hayir
pazarlamaci,bay,sabit,sabah,25,issiz,bayan,46,evet
savci,bay,gsm,aksam,6,ozel,bay,34,hayir
pazarlamaci,bayan,sabit,ogle,12,ozel,bay,39,hayir
polis,bay,sabit,sabah,20,emekli,bay,72,hayir
banka,bayan,444,ogle,56,ozel,bay,32,evet
banka,bayan,444,aksam,5,ozel,bay,34,hayir
polis,bay,gsm,ogle,22,emekli,bayan,72,evet
polis,bay,gsm,aksam,17,issiz,bayan,46,evet
polis,bay,gsm,ogle,39,kamu,bay,65,evet
polis,bay,sabit,ogle,13,cocuk,bay,10,evet
polis,bay,gsm,sabah,60,kamu,bay,74,evet
savci,bay,gsm,ogle,27,kamu,bay,50,evet
sigortaci,bayan,sabit,sabah,44,issiz,bay,24,hayir
polis,bay,sabit,ogle,21,emekli,bay,65,hayir
polis,bay,sabit,sabah,66,kamu,bay,45,evet
savci,bay,sabit,ogle,55,kamu,bay,66,evet
```

Şekil 10 : Arff dosyası görüntüsü

Programa tanıtılan ve herhangi bir problem çıkarmayan kullanılabilir halde olan veri tabanımız WEKA programı üzerinde çeşitli analizler yapmak için uygun hale gelmiştir. Program üzerinde bulunan Classify(Sınıflandırma) sekmesine gelerek bu sekme altında bulunan verimize uygun olarak kullanabileceğimiz tüm algoritmaları kullanabiliriz.

Kullanılan Veri tabanının bulundurduğu nitelikler bakımından hem nominal hem de numerik karakterler bulunduğu için WEKA programı üzerinde sınıflandırma algoritmalarından tümünü gerçekleştirmemiz mümkün değildir. Belirli kriterlere göre yapılan araştırmalar sonucu bizim problemimize hizmet eden en uygun yol karar ağaçları olarak belirlenmiştir.

J48 Algoritması

```

Correctly Classified Instances      27      90 %
Incorrectly Classified Instances    3       10 %
Kappa statistic                    0.8
Mean absolute error                0.1123
Root mean squared error            0.3125
Relative absolute error            22.4615 %
Root relative squared error        60.0145 %
Total Number of Instances          30

=== Detailed Accuracy By Class ===

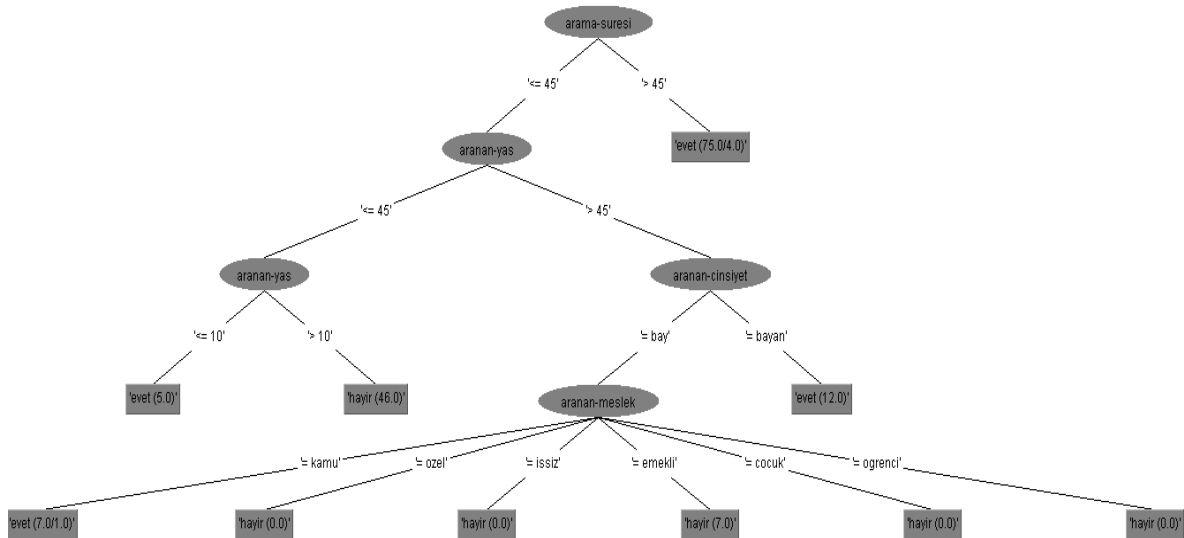
      TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
      -----  -----  -
      1         0.2     0.833     1       0.909     0.873     evet
      0.8       0       1         0.8     0.889     0.873     hayir
Weighted Avg.  0.9     0.1     0.917     0.9     0.899     0.873

=== Confusion Matrix ===

  a  b  <-- classified as
15  0  | a = evet
 3 12 | b = hayir

```

WEKA programı üzerinden sınıflandırma algoritmalarından verimiz üzerinde uygulayabileceğimizi algoritmalarından biriside J48 algoritmasıdır. Verimiz üzerinde yapılan testler sonucunda makine öğrenimimiz %90 doğru sınıflandırma %10 ise birbirleri ile örtüşmeyen sınıflandırma yaptığının göstergesidir. Verinin çeşitliliği ve heterojenliği üst düzeyde olduğundan dolayı %10'luk bir hata payını kabul edebiliriz.



Şekil 11: Karar Ağacı

Tartışma ve Öneriler

Bu çalışmanın sonuçlarından hızla gelişen teknoloji ve mobil iletişim ağları ile paralellik gösteren dolandırıcılık faaliyetleri ve dolandırılan kişilerin dolandırma işlemi tamamlanmadan önce ve tamamlandıktan sonra dolandırıcılara önemli ve kişisel bilgilerini kendileri tarafından verildiği için hukuksal boşluğa düştüğü gözlemlenmiştir. Gelişen teknolojiler erişim ve uygulama kolaylığı sağlamakla beraber kişiye özel bilgilerin internet ortamlarında saklanması ve bu saklanan verilerin

yeteri kadar güvenliğinin sağlanamaması büyük bir zafiyet doğurduğunu gözleme şansını sunmuştur. Kişilerin kendi taraflarınca yöneltilen anket sorularına cevaplar vermesi ve bazı anketlerde bulunan kişisel bilgileri de bu gibi eylemlerle 3.cü kişiler ile paylaşımları kendilerine maddi ve manevi sıkıntı olarak geri döndüğü gözlemlenmiştir.

Uygulama çıktılarına baktığımız zaman 60 yaş ve üstü kişilerin yapılan bu dolandırıcılık işlemlerinde diğer yaş gruplarına göre dolandırılma olasılığı oldukça yüksektir. Toplum huzur ve asayişini bozan dolandırıcılar çeşitli sosyal mühendislik uygulamaları yaparak eğitim düzeyi düşük ve ev hanımlığı yapan bayanlar üzerinde yoğunlaşarak çeşitli etkileme yöntemleri kullanarak başarı sağlamaktadırlar. Diğer bir yandan çalışma açık bir şekilde gösteriyor ki veri olarak kullanılan 2 çocuk dolandırıcılar tarafından %100 oranında dolandırılmıştır. Bunun nedeni ise evde ve okulda bu tarz dolandırıcılık yöntemleri için gerekli bilgi ve dokümantasyon ile çocuklara bilgilendirme yapılmaması olarak gösterilebilir. Özellikle arayan kişilerin kendilerini kamu personeli olarak tanıtmaları (savcı, mit, polis, hâkim,) dolandırılma faaliyetinde başarıyı etkileyen en önemli unsurlardan biridir. Dikkat çekilmesi gereken bir başka öge ise arama süresidir, Çalışma çıktılarında bakılacak olursa konuşma süresi ne kadar uzarsa dolandırıcılık işlemi o kadar başarıya yakınlaşmaktadır. Gelişen teknolojiler ile birlikte dolandırıcılık faaliyetlerinin aynı hızda paralellik gösterdiği kanısına varılmakla birlikte bu teknolojilere ve bu teknolojilerin beraberinde getirdiği risklerin farkında olmayan kişilerin dolandırıcılar tarafından kolayca dolandırılabilmesi görülmektedir.

Kaynakça

- Karacan, H., & Yeşilbudak, M. (2010). *Kullanıcı Merkezli İnteraktif Veri Madenciliği: Bir Literatür Taraması. INTERNATIONAL JOURNAL OF INFORMATICS TECHNOLOGIES, 3(1).*
- Kılıçarslan H.. (2013). "Türkiye GSM Sektöründe Veri Madenciliği Yöntemi ile Sahtekârlık Tespiti Ve Bir Uygulama." Yüksek Lisans Tezi. Beykent Üniversitesi İstanbul.
- Özcan C (2014) "Veri madenciliği güvenlik uygulama alanları ve veri madenciliği ile sahtekârlık analizi" Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü
- Tavacı H (2011) "GSM şebekelerinde sahtekârlık yönetimi için veri madenciliği yöntemlerinin uygulanması" Yüksek Lisans Tezi. Bahçeşehir Üniversitesi Fen Bilimler Enstitüsü
- Ekinci T (2009) "Veri madenciliği ve telekomünikasyon sektöründe uygulanması" Yüksek Lisans Tezi. Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü
- Özbay C (2007) "finans sektöründe veri madenciliği ile dolandırıcılık tespiti" Yüksek Lisans Tezi. Selçuk Üniversitesi Fen Bilimleri Enstitüsü
- Silahtaroglu, G., "Kavram ve Algoritmalarıyla Temel Veri Madenciliği", s. 46, Papatya Yayıncılık, İstanbul, 2008
- Akbal, E., Doğan, Ş., & Varol, N. (2017). *Karar Ağaçları ile Telefon Dolandırıcılığı Verilerinin Analizi.*
- Thomas, B., Clergue, J., Schaad, A., & Dacier, M. (2004). *A comparison of conventional and online fraud. In CRIS (Vol. 4, pp. 25-27).*
- Dener, M., Dörterler, M., & Orman, A. (2009). *Açık Kaynak Kodlu Veri Madenciliği Programları: Weka'da Örnek Uygulama. Akademik Bilişim, 9, 11-13.*
- Ertuğrul, İ., Organ, A., & Şavlı, A. (2013). *Veri madenciliği uygulamasına ilişkin PAÜ hastanesinde hasta profilinin belirlenmesi. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 19(2), 97-103.*