Kullanıcı Giriş Sistemlerinde Yapay Sinir Ağları Kullanılarak Şifre Güvenlik Sisteminin Geliştirilmesi

Developing Password Security System By Using Artificial Neural Networks In User Log In Systems

Yusuf Korkmaz[1]

[1]Bilgisayar Mühendisliği,
Fatih Sultan Mehmet Vakıf Üniversitesi
yusuf.korkmaz@stu.fsm.edu.tr

Özetçe

Gelişen teknolojiyle birlikte sanal dünya bizlere gerekli olan tüm hizmeti sunabilmek adına her geçen gün bir adım daha ileri gitmektedir. Bize sunulan hizmetlerle doğru orantılı olarak sosyal medyadaki varlığımız da artmaktadır. Kişisel sosyal medya hesaplarımızdan günlük hayatlarımızı rahatlıkla paylaşabilmekteyiz. Internet bankacılığı sayesinde evlerimizden çıkmadan banka işlemlerimizi gerçekleştirebilmekteyiz. Tüm bu işlemleri, kişisel ve özel olduğunu düşündüğümüz birtakım tuş kombinasyonları ardında koruduğumuza inanmaktayız. Fakat şu an kullanılan sistemler sadece şifremizi karşılaştırarak güvenlik sistemini oluşturmakta, şifreyi giren kullanıcıyı ayırt etmek ile ilgilenmemektedir. Bu da kötü niyetli kişilerin şifremizi öğrenerek sistemimize sızmasının önüne geçememiz anlamına gelmektedir. Geliştirilen sistemde, şifrenin şahsa münhasır olmasını sağlayan bir yapı tasarlanmıştır. Bu sistem kişinin tuş kombinasyonunu girerken kullandığı klavye stilini öğrenmektedir. Böylece bir başkası şifremizi öğrense dahi kullanıcının klavye kullanım stili ile aynı tarzda giremeyeceğinden, girilen şifre yanlış kabul edilmekte ve giriş izni verilmemektedir. Bu şekilde kullanıcı dışındaki kişilerin sisteme girişi engellenmektedir. Bu çalışmada makine öğrenmesi tabanlı kullanıcı giriş sistemi geliştirilmiştir. Bu sistemin geliştirilmesinde yapay sinir ağları kullanılmıştır. Kullanıcının şifreyi giriş stili öğrenilerek, giriş işlemi sırasında şifrelerin eşleşmesine ek olarak şifreyi giriş stilleri de karşılaştırılmıştır. Kullanıcı giriş sisteminin giriş yapan kişiyi ayırt edebilmesi, bilgisayarlarla insanlar arasında duygusal bir bağ oluşmasını sağlamaktadır.

Anahtar Kelimeler: *Yapay zeka, Yapay sinir ağları, Makine öğrenmesi, Kullanıcı giriş sistemi güvenliği*

Abstract

By the developing technology, the virtual world is progressing every day to serve us and we are more being on the social media by this services. We can easily share about our daily lives from our social media accounts. Thanks to mobile banking, even in our houses we can go on banking. And we all believe its safety by using some key combinations that we think they are private. However today all the systems that we use, are providing security by comparing the passwords without differanciating the users. It means that this way is not blocking some malicious people that try to learn our passwords and get enter our systems. It was desinged a structure, is unique for each individual in the system that we developed. This system knows the users' keyboard style while typing key combination.Even if someone else tries to log in with your password,system recognizes your personal keyboard style and does not allow to access unless this person is you.In that way noone other than user him/herself can access the system.In this work,user entry system is developed by machine learning by based. Artificial neural networks used in developing this system.The way of user's password entry style is learned,and during login process these stiles are compared besides password matching. Since the user log in system recognizes us that also makes an emotional connection between people and computers.

Keywords: *Artificial intelligence, Artificial neural network, Machine learning, User log in system security*

1. Giriş

Teknolojinin günbegün ilerlemesiyle bilişim sistemlerinin (ATM, internet bankacılığı, sosyal medya hesapları, e-posta adresleri vb.) kullanım alanları da doğru orantılı olarak artmaktadır. Araştırma şirketi e-Marketer'ın yayımladığı rapora göre, dünya genelinde internet kullanıcı sayısının 2016 yılında yüzde 5.7 artarak 3 milyarı aşacağı öngörülmüştür [1]. Çoğu şahsi bilgilerimizi, dosyalarımızı, fotoğraflarımızı, bulut ortamlarında saklamaktayız. Kimlerle arkadaş olduğumuzu Facebook'ta, gittiğimiz yerleri adım adım Swarm'da, çektiğimiz fotoğrafları Instagram'da, hangi görüşte olduğumuzu ise Twitter'da gözler önüne sermekteyiz. Satın aldığımız ya da almak istediğimiz ürünleri e-ticaret sitelerinde incelemekteyiz. Maddi işlemlerimizi, teknolojinin bizlere sağladığı imkanlar dahilinde kolaylıkla ATM'lerden veya internet bankacılığı sistemleri sayesinde gerçekleştirebilmekteyiz [2]. Tüm bu verileri ise yalnızca 5-10 karakterlik şifrelerin ardında saklamaktayız. Şifre sadece iki tarafın bildiği gizli bir bilgidir. Bu gizli bilgi sayesinde taraflar birbirlerini güvenli olarak tanımlayabilmekteler [3]. Google

978-1-5090-0876-6/16/$31.00 ©2016 IEEE

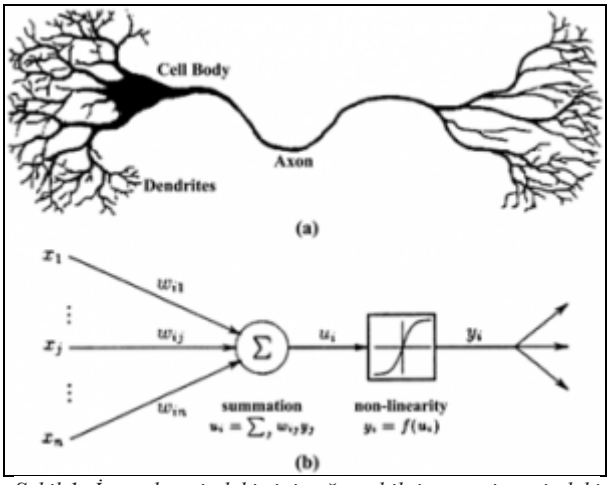
Apps tarafından yaklaşık 2000 kullanıcı üzerinde yapılan ankette; seçilen şifrelerin ağırlıklı olarak sabit ve hazır bilgilerden seçildiği anlaşılmıştır. Bu da şifre seçerken dikkat edilmediğini ve bu durumun da kötü niyetli hackerların işini kolaylaştırdığını göstermektedir [4]. Çünkü şifrelerin kırılabilmesi teknolojinin gelişmesiyle daha da kolaylaşmaktadır. Kullandığımız antivirüs programları ve güvenlik duvarları çoğu casus yazılımını önemsiz görerek tespit etmemektedir [5]. Sosyal ağlardaki güncel güvenlik tehditleri: Kimlik hırsızlığı, e-dolandırıcılık, iyi bilinen şirketlerin adını kullanma, piyango dolandırıcılıkları, sahte güvenlik yazılımı dolandırıcılıkları, profil klonlama, üçüncü kişi uygulama tehlikeleri, sahte ürün satışı, kötü bağlantı istekleri, istenmeyen e-postalar, düzenbaz site kodlamaları [6]. Sanal ortamda kimlik bilgilerimizi çalan kişiler, bizim adımıza istemeyeceğimiz işlemler gerçekleştirebilmekte, bankacılık şifremize ulaşabilmekte ve bizi zor durumda bırakacak işlemler gerçekleştirebilmektedirler [7]. Tüm bu saldırıların önüne geçebilmek için kullandığımız kullanıcı giriş sistemini daha güvenilir hale getirebilmek adına bir sistem gerçekleştirilmiştir. Kullanıcı giriş sisteminin güvenlik seviyesini birkaç adım daha öteye taşımak amacıyla geliştirilen bu sistem, kullanıcı şifresini girmeye başladığı an iki tuş basımı arasında geçen süreyle kişinin tuş takımı kullanım hızını öğrenmektedir. Şifreyi giriş esnasında kullandığı kendisine has tuşlar ile de tuş tercihleri öğrenilmektedir. Bu bilgiler ışığında kişinin klavye kullanım stili öğrenilmektedir. Bu sayede şifre karakteristik bir yöne sahip olmaktadır. Kullanıcı hesabına giriş yapmak istediğinde şifre giriş tarzını öğrenmiş olan sistem, hesabın gerçek sahibine giriş izni vermektedir. Diğer yandan başka bir kullanıcı şifreyi bilerek giriş yapmak istese dahi kişiye özgü klavye kullanım tarzı eşleşmeyeceğinden kullanıcının sisteme girişi engellenmektedir.

2. Yöntem

Klavye kullanım stili, davranışın analiz edilerek kimlik tespitini sağlayan karakterlerden biridir. Bu sistemler, tuşa basım işleminin kişiye özgü bir ritme sahip olduğu varsayımı üzerine ortaya çıkmıştır. Klavye kullanım stiline dayalı sistemlerde tuşa basım ve tuşu bırakma anına dayalı olarak tanıma işlemi gerçekleştirilmeye çalışılmaktadır [8]. Kullanıcıların klavye kullanım stilini öğrenip, sisteme giriş isteği yapıldığında şifrelerin karşılaştırılmasının yanında, kullanıcının klavye kullanım stilleri de karşılaştırılarak sisteme giriş izni verilmektedir. Bu sistem ile birlikte sosyal medyanın ötesinde ATM'lerin ve internet bankacılığının da şifre güvenlik sistemleri daha güvenilir bir hal almaktadır.
Klavye kullanım stilini öğrenerek kullanıcıları ayırt etme işlemlerini gerçekleştiren bir sistem tasarlanmıştır. Kişilerin girdikleri şifrelerinin yazış stillerini, hızlarını, yanlışlarını ve tuş kombinasyonlarını öğrenerek ayırt etmektedir. Bu sistem, makine öğrenmesi tabanlı yapay sinir ağları kullanmaktadır. Etkinlik fonksiyonu olarak basamak (step) fonksiyonu kullanılmaktadır.

2.1 Yapay Sinir Ağları

Yapay sinir ağı, insan beyninin sinir hüclerinden oluşmuş katmanlı ve paralel olan yapısının tüm fonksiyonlarıyla beraber bilgisayar ortamında modellenmesidir. Yapay sinir ağları, yapay bilgi gösterim ve işletme sistemidir. İnsan beynindeki bir sinir hücresi (nöron) ve bağlantıları örnek alınarak tasarlanmştır. (Şekil 1)

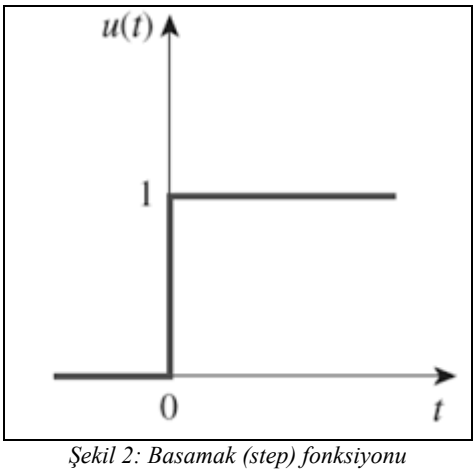


Şekil 1: İnsan beynindeki sinir ağı ve bilgisayar sistemindeki tasarlanmış sinir ağı

Yapay sinir ağları en temel olarak bir girdi kümesini ağırlıklarıyla işleyerek kullanılan etkinlik fonksiyonunun sonucuna göre tek bir çıktı üretmektedir [9]. (Şekil 1)

2.2 Etkinlik Fonksiyonu

Yapay sinir ağlarında girdilerin ağırlıklarıyla işlenerek toplanması sonucunda elde edilen değer, eşik olarak belirlenen değeri aşıyorsa fonksiyon çıktı olarak 1 veya True üretmektedir. Eğer toplama işlemi sonucunda elde edilen değer eşik olarak belirlenen değerin altında kalıyorsa fonksiyon çıktı olarak 0 veya False üretmektedir. Bu etkinlik fonksiyonuna basamak (step) fonksiyonu adı verilmiştir [10]. (Şekil 2)



Şekil 2: Basamak (step) fonksiyonu

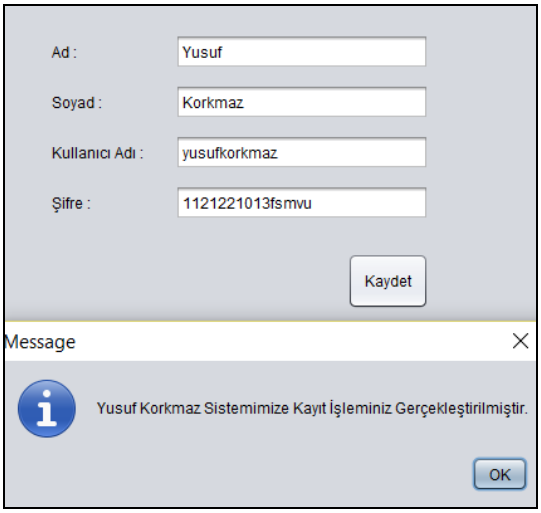
3.Uygulama

Hedeflenen amaçlara uygun şekilde kullanıcıların klavye kullanım stillerini öğrenen, giriş esnasında klavye kullanım stillerini karşılaştıran, uygunluğa yönelik kullanıcı girişine izin veren veya reddeden bir sistem gerçekleştirilmiştir.

Sistemimizin test edilebilir olması ve istenen düzeyde başarılı olup olmadığını görmek için java dilinde örnek bir giriş arayüzü tasarlanmıştır. Kullanıcı adı ve şifrenin farklı birçok kullanıcıya verilerek sisteme giriş yapmaları istenmiştir. Kullanıcı adı ve şifrenin doğru verilmiş olmasına rağmen sistemimiz gerçek kullanıcısını ayırt edebilmekte ve diğer kullanıcılara giriş izni vermeyerek başarılı olmaktadır.

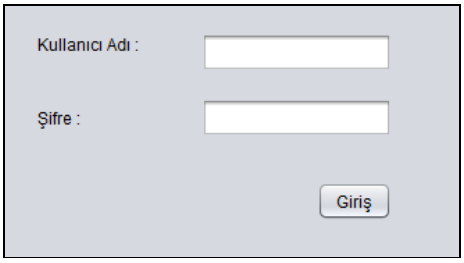
Şekil 3 : Program giriş ekranı

Programımıza giriş ekranı Şekil 3'te gösterildiği gibidir. Bu ekranda kullanıcı girişi veya kullanıcı kayıt işlemleri gerçekleştirilmektedir.



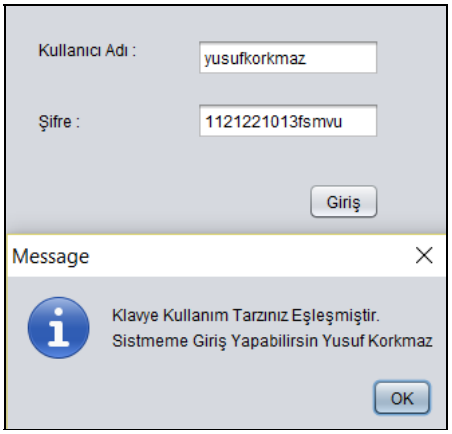
Şekil 4 : Kullanıcı kayıt ekranı

Programımızın kullanıcı kayıt ekranı Şekil 4'te gösterilmektedir. Bu ekranda kullanıcı adını, soyadını, kullanıcı adını ve şifresini tanımlamaktadır. Tanımlanan şifre için sistem yapay sinir ağını oluşturarak öğrenme işlemine başlamaktadır.

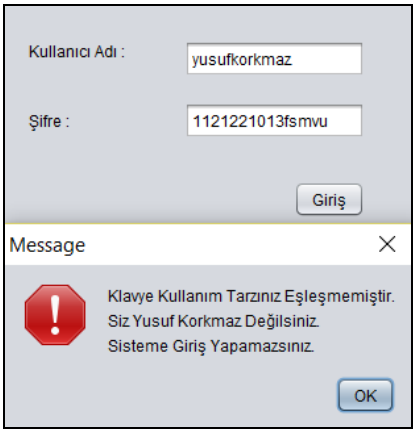


Şekil 5 : Kullanıcı giriş ekranı

Programımızın kullanıcı giriş ekranı Şekil 5'te gösterilmektedir. Bu ekranda kullanıcı, giriş arayüzünü geçmeye çalışmaktadır. Kullanıcı adı ile eşleşen yapay sinir ağına şifre gönderilmekte ve kullanıcının ayırt edilmesi istenmektedir. Eğer yapay sinir ağı girilen şifrenin kullanıcıya ait olduğu yönünde bir çıktı üretirse kullanıcı giriş arayüzünü geçebilmektedir. Sistem aksi yönde bir çıktı üretirse programımız kullanıcı adı veya şifrenin yanlış olduğuyla ilgili uyarı verir ve giriş izni vermez.
Sistemimiz olumlu yönde bir çıktı ürettiği taktirde test edilen veriyi de öğrenmek için işler. Bunun nedeni ise daha ayırt edici ve doğru sonuçlar üretmektir.



Şekil 6 : Olumlu sonuç



Şekil 7 : Olumsuz sonuç

Sistemimizin klavye kullanım stili için oluşturmuş olduğu yapay sinir ağındaki veri oranı ile kullanıcıyı ayırt etme oranının doğrusal olarak arttığı gözlemlenmiştir.

Tablo 1: Sistemimizin başarı oranı

Öğrenilen Veri Adedi	Başarı Oranı
10	30,00%
100	70,00%
250	81,00%
500	83,20%
1000	85,50%
1500	85,50%

Öğrenilen veri adedi ile kullanıcıyı ayırt etme başarı oranlarının görsel hali Tablo 1'de gösterilmektedir.

Tablo 2: Farklı kullanıcılarla sistemin test edilmesi

Kullanıcı / Deneme	1. Deneme	2. Deneme	3. Deneme	4. Deneme	5. Deneme
Yusuf Korkmaz	Olumlu	Olumlu	Olumsuz	Olumlu	Olumlu
Ahmet Ak	Olumsuz	Olumsuz	Olumsuz	Olumsuz	Olumsuz
Cem Dırman	Olumsuz	Olumsuz	Olumsuz	Olumlu	Olumsuz
Burhan Gül	Olumlu	Olumsuz	Olumsuz	Olumsuz	Olumlu
Ömer Özcan	Olumsuz	Olumsuz	Olumsuz	Olumsuz	Olumlu
Ömer Koçbil	Olumsuz	Olumsuz	Olumsuz	Olumsuz	Olumsuz

Farklı kullanıcılara kullanıcı adı ve şifrenin verilerek sistemin test edilmesi Tablo 2'de gösterilmiştir.

4. Sonuçlar

Kullanıcıların klavye kullanım stillerinin şahsa özgü olması ve şifrelerin tuş takımları (klavye , ATM tuş takımı vb.) üzerinden girilmesi sistemimizi kolay adapte edilebilir hale getirmektedir. Bu durumu şifre güvenliğini arttırıcı bir özellik olarak sunmaktadır. Kullanıcının sürekli şifreyi girerken yapmış olduğu yanlışları veya kendine has karakterler kullanımını fark edebiliyor olması (büyük karakter için caps lock tuşu yerine shift kullanılması gibi) kullanıcıyı tanıma açısından önemli noktalardan birkaçı olduğu da gözlemlenmiştir.
Sistemimizin test aşamasında gözlemlediğimiz diğer hususlar ise eklemelerin ve algoritmasının daha özelleştirilebilir olmasıdır. Makine öğrenmesini kullanıyor olmamız, algoritmamızın sürekli iyileştirilebilir olduğunu göstermektedir.
Yapmış olduğumuz bu çalışma sonucunda makine öğrenmesi ve yapay sinir ağları kullanıcı giriş sisteminde kullanımının güvenliği arttırabileceği tespit edilmiştir.

Teşekkür

Yapay zeka dersini aldığım ve geliştirmiş olduğum bu sistemi dönem projesi olarak kabul eden sayın hocam Yrd. Doç. Dr. Ebubekir Koç'a teşekkür ederim.

Kaynakça

[1]http://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602 (01.04.2016)

[2] Vural, Z. B. A., & Batb, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim fakültesine Yönelik Bir Araştırma Socıal Medıa As a New Communıcatıon Envıronment: a Research on Ege Unıversıty Faculty of Communıcatıon. Journal of Yasar University, 20(5), 3348-3382.

[3]http://www.chip.com.tr/haber/sifre-guvenligi-ve-hack_17955.html (01.04.2016)

[4] Savvas, A. (2013), Pets Lead The Way As Google Reveals Top 10 Most Popular Passwords, < http://www.itproportal.com/2013/08/01/google-reveals-top-10-popular-passwords-pets-lead-the-pack/ >, erişim: 01.04.2016

[5] Sönmez, Y., Katabatak, M., & Avcı, E. (2013). Uygulamalarda Şifre Güvenliği İçin Yeni Bir Yaklaşım. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, 315-318.

[6] Ceyhan, E. B., Demiryürek, E., & Kandemir, B. (2015). Sosyal Ağlarda Güncel Güvenlik Riskleri Ve Korunma Yöntemleri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 1(1).

[7] Yıldırım, E. Y. Sosyal Ağlarda Güvenlik Farkındalığının Arttırılması.

[8] Turhan, C. G., Ceyhan, E. B., & Sağıroğlu, Ş. Biyometrik Sistemlerde Güvenlik Üzerine Bir İnceleme.

[9] Uğur, A., Ve Kınacı, A. C. (2006). Yapay Zeka Teknikleri ve Yapay Sinir Ağları Kullanılarak Web Sayfalarının Sınıflandırılması. *XI. Türkiye'de İnternet Konferansı (inet-tr'06), Ankara*, 1-4.

[10] Hassoun, M. H. (1995). *Fundamentals of artificial neural networks*. MIT press.