TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAĞLAMSAL DOĞRULAMA İÇERİSİNDE EK ÖZELLİK OLARAK KLAVYE DİNAMİĞİ ANALİZİ VE DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Oguzhan SALMAN

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Ali Aydın SELÇUK

ARALIK 2020

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Oguzhan SALMAN

İMZA

ÖZET

Yüksek Lisans Tezi

BAĞLAMSAL DOĞRULAMA İÇERİSİNDE EK ÖZELLİK OLARAK KLAVYE DİNAMİĞİ ANALİZİ VE DEĞERLENDİRİLMESİ

Oguzhan SALMAN

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof.Dr. Ali Aydın SELÇUK

Tarih: ARALIK 2020

Tuş Vuruş Dinamikleri, kullanıcının kimliğinin doğruluğuna karar vermek için bireylerin tuş vuruş davranışlarını incelememize yardımcı olan bir davranışsal-biyometri çözümüdür; ancak, bu yaklaşımın dezavantajı, nispeten yüksek yanlış negatif ve yüksek yanlış pozitif oranlara sahip olmasıdır. Bu çalışmada, farklı anomali tespit yaklaşımlarını karşılaştırıyor ve bu çözümleri birleştirdiğimizde performans gelişmelerini inceliyoruz. Önce tuş vuruşu dinamikleri ve oturum bağlamı anomali bileşenlerini ayrı ayrı oluşturduk. Ardından, bu makine öğrenimi bileşenlerinin sonuçlarının nasıl birleştirileceğini inceledik. Deneylerimiz, bu bileşenlerden ağırlıklı ortalama topluluk modelini oluşturmak performansı artırırken, yeni bir özellik olarak oturum bağlam anomali bileşenine tuş vuruşu dinamikleri puanlarını dahil etmek sadece tuş vuruşu dinamiği puanlarını değil, aynı zamanda bu puanlar arasında değişimleri de gözlemleyebildiği için daha iyi performans sağladığını gözlemledik.

Anahtar Kelimeler: Davranışsal biyometri, Yapay zeka, Anomali deteksiyonu

ABSTRACT

Master of Science

ANALYSIS AND EVALUATION OF KEYSTROKE DYNAMICS AS A FEATURE OF CONTEXTUAL AUTHENTICATION

Oguzhan SALMAN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Prof.Dr. Ali Aydın SELÇUK

Date: DECEMBER 2020

Keystroke Dynamics is a behavioural-biometrics solution that helps us to examine individuals' keystroke behaviour to decide legitimacy of the user; however, the drawback of this approach is that it has relatively high false negative and high false positive rates. There are some other anomaly detection approaches which examine more static properties like user's contextual details such as IP address, screensize, browser type etc. to detect legitimacy of the user but these approaches also suffer from false alerts. In this study, we compare different anomaly detection approaches and observe performance improvements when we combine these solutions. We first built keystroke dynamics and session context anomaly components, separately. Then, we examined how to combine the results of these machine learning components. Our experiments showed that while using weighted average ensemble model from these components improved performance, another approach which was to include keystroke dynamics scores in session context anomaly component as a new feature gives the opportunity to capture not only the keystroke dynamics scores but also the deviations of these scores and thus yields better performance

Keywords: Behavioural biometrics, Machine learning, Anomaly detection

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Prof.Dr. Ali Aydın SELÇUK, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine ve destekleriyle her zaman yanımda olan aileme ve arkadaşlarıma çok teşekkür ederim.

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT	v
TEŞEKKÜR	vi
İÇİNDEKİLER	vii
ŞEKİL LİSTESİ	viii
ÇİZELGE LİSTESİ	ix
RESİM LİSTESİ	x
1. GİRİŞ	1
1.1 Tezin Katkıları	3
1.2 Literatür Araştırması	4
2. GÜVENLİK ALGISI VE ŞİFRELER	8
2.1 Şifre Tabanlı Kimlik Doğrulama Tarihçesi	10
2.2 Şifre Seçimi ve Şifrelerin Geleceği	12
2.3 Risk Tabanlı Kimlik Doğrulama	14
3. DENEY HAZIRLIK AŞAMASI	17
3.1 Dataların Toplanması	17
3.2 Data Özellikleri	18
3.3 Saldırı Simülasyonu	18
4. KİMLİK DOĞRULAMA ANOMALİ TESPİT SİSTEMLERİ	19
4.1 Klavye Dinamiği Bileşeni	19
4.2 Bağlamsal Anomali Bileşeni	22
4.3 Topluluk Modeli	24
4.4 Özellik Olarak Klavye Dinamiği	26
5. DEĞERLENDİRME	29
5.1 Karşılaşılan zorluklar	33
6. SONUÇ VE ÖNERİLER	34
KAYNAKLAR	36
ÖZGEÇMİŞ	39

ŞEKİL LİSTESİ

Şekil 2.1: Gmail hesaplarından gelen spam mesajlarının 2010-2012 yılları arası miktarı 15
Şekil 2.2: Şüpheli girişlerde kullanılan risk tabanlı doğrulama ekranı 16
Şekil 4.1: Klavye Dinamik bileşeninin gerçek kullanıcı ve saldırgan başarı skorları 21
Şekil 4.2: Klavye dinamik bileşeni ROC eğrisi. 21
Şekil 4.3: Bağlamsal Anomali bileşeninin gerçek kullanıcı ve saldırgan başarı skorları 23
Şekil 4.4: Bağlamsal Anomali bileşeni ROC eğrisi 23
Şekil 4.5: En iyi performans gösteren katsayılarla oluşturulan Topluluk Modelinin gerçek kullanıcı ve salgırgan başarı skorları 25
Şekil 4.6: Farklı katsayılara göre Topluluk Modeli ROC eğrisi 26
Şekil 4.7: Klavye dinamik skorunun bağlamsal anomali bileşeni gerçek kullanıcı ve saldırgan başarı skorları 27
Şekil 4.8: Klavye dinamik skorunun bağlamsal anomali bileşeni içerisinde kullanımı ROC eğrisi 28
Şekil 5.1: Standard deviasyon (std) değerlerine göre klavye dinamik skorlarının önemi: std (User-1): 15.04%, std(User-2): 10.49%, std(User-3): 5.16%. 31

ÇİZELGE LİSTESİ

Çizelge 3.1: Toplanan data özeti 18
Çizelge 5.1: Performans özeti - Gerçek Giriş (752 test datası), Saldırı Simülasyon Girişi (120 test datası) (KaaF keystroke as a feature kısaltmasıdır). 32

RESİM LİSTESİ

Resim 3.1: Her girişte gerçekleşen örnek data akışı 18
Resim 4.1: Klavye dinamik skorlarının bağlamsal anomali datalarına eklenme örneği. 27

1. GİRİŞ

Fırsatlar yakalandıkça katlanır ***- Sun Tzu***

Eskiden kullanıcı doğrulama problemi genellikle binary yani doğru veya yanlış problemi olarak değerlendirilirdi. Kullanıcı adı ve şifresi doğruysa kullanıcı doğrulama başarılı ve yanlışsa doğrulama başarısız sonuçlanırdı. Probleme bu açıdan yaklaşmak, password kırma, oltalama gibi bilinen en yaygın güvenlik sorunlarının ana sebebi olarak karşımıza çıkmaktadır[22] ve günümüzde birçok websitesi bu yaklaşımdan uzaklaşıp probleme daha kapsayıcı bir yaklaşım geliştirmektedir[13]. Bu yaklaşımlar kullanıcı adı ve şifresinin doğru olmasını kimlik doğrulamak için tek şart olmaktan çıkarmakta ve kullanıcıyı diğer kullanıcılardan ayıran tüm bilgilerin toplanmasıyla o anki girişin çalıntı bir hesaba mı yoksa gerçek kullanıcıya mı ait olduğuna karar vermemize yardımcı olmaktadır. Yapay zeka algoritmalarının kullanıldığı bu çözümlerde artık kimlik doğrulama doğru veya yanlış gibi binary problemi olmaktan çıkarak her girişe 0 ile 1 arası bir skor verilerek kullanıcının doğruluğuna karar verilmektedir. Bir diğer deyişle, o anki kullanıcının bilgileri bir önceki girişlerine yakınsa 1'e yakın olmakta ve kullanıcı doğrulanmakta ama 0'a yakınsa kullanıcının doğru kullanıcı olmadığı veya çalıntı bir hesaba ait olduğu sonucuna varılmaktadır.

Risk tabanlı uygulamalarda doğrulama skoru, o anki kullanıcının kimliği hakkında bize kendi implementasyonumuza karar verme, değişken güvenlik politikaları tanımlama ve risk ölçeklendirme imkanı sağlamaktadır. Örneğin, kullanıcının o anki doğrulama skoru gerekli değerden düşük olması durumunda iki faktörlü kimlik doğrulamayla skor artırılarak giriş sağlanabilir veya sadece belirli ve kısıt-

landırılmış yetkilerle kullanıcının hesabına girişine izin verilebilir.

Risk tabanlı uygulamalarda en önemli faktörlerden birisi, hangi politika seçilirse seçilsin kimlik doğrulama skorunun yüksek doğruluk oranlarıyla gerçek kullanıcıyı saldırgandan ayırt edebilmesi gerekmektedir. Sınıflandırma doğruluk oranları hesaplanırken iki tür hata türüyle hesaplanır:

- Tip-1 hatası, bir diğer adıyla yanlış pozitif, gerçek kullanıcının saldırgan olarak değerlendirilmesi hatası

- Tip-2 hatası, bir diğer adıyla yanlış negatif, saldırganın gerçek kullanıcı olarak değerlendirilmesi hatası

Bu hataları düşürmek ve doğruluk oranını artırmak için kullanıcılardan olabildiğince fazla data toplanması gerekmektedir. Aynı şekilde anomali tespitlerini daha doğru yapmak için değişik senaryolara uygun anomali dataları eklenerek bu senaryolara göre Tip-1 ve Tip-2 başarı oranları hesaplanmalıdır.

Riske dayalı doğrulamanın olmadığı durumlarda güvenlik mail veya telefon gibi ikinci faktör doğrulamayla sağlanmaktadır. Ancak, kullanılabilirliğe büyük etkisi olan ikinci faktör doğrulamanın yerini yavaş yavaş riske dayalı doğrulamaya devrettiği görülmektedir. Riske dayalı kimlik doğrulama sistemlerinin rakiplerine göre en büyük avantajı, bu mekanizmadan hem son kullanıcının haberdar bile olmaması hem de kullanılabilirliğe etki etmemesine rağmen güvenlik sağlamasıdır ve bu tarz uygulamaların daha verimli çalışması siber güvenlik araştırmaları için büyük önem taşımaktadır.

1.1 Tezin Katkıları

Kullanıcı ağ, makine ve biyometrik bilgilerinin beraber kullanılmasının bu dataların tek başına kullanıldığı modelden daha iyi sonuç vereceği öngörülmekle beraber halen tartışmalı bir konudur ve literatürde gerçek bir senaryoda birden fazla yapay zeka algoritmasının başarısını analiz eden bir çalışma bulunmamaktadır. Bu tezin amacı literatürde ki bu boşluğu doldurmak ve birden fazla yapay zeka algoritmasının performansını riske dayalı doğrulama senaryolarında ortaya koymaktır. Literatüre yaptığımız başlıca katkılar aşağıdaki gibidir:

- Kurduğumuz bir websitesi ile tüm kullanıcıların bağlamsal özellikleri ve klavye dinamikleri gerçek senaryoya uygun bir şekilde toplandı. (Önceki bir çalışma, birden fazla yapay zeka algoritmasının başarısını değerlendirmesine rağmen kullanılan datalar yapay bir şekilde birleştirilmiştir ve tek bir birleştirme yönteminin başarısı değerlendirilmiştir [16])

- Klavye dinamikleri ve bağlamsal anomali yapay zeka algoritmaları kullanıldı ve bu algoritmaların birleştirme yöntemleri karşılaştırıldı.

- En iyi performans veren modelin bağlamsal anomali yapay zeka algoritmasında kullanılan dataya klavye dinamik algoritmasından çıkan datanın eklenmesi olduğu gözlemlendi. Bunun nedeninin klavye dinamiklerinde ki varyasyondan kaynaklandığı ve varyasyonu yüksek olan kullanıcıların klavye dinamik skorunun öneminin azaldığı belirlendi.

1.2 Literatür Araştırması

Literatürde şifre tabanlı kimlik doğrulama mekanizmasına yapılan katkılar birçok farklı disiplinden gelmektedir ve kullanılabilirlik ve uygulanabilirlik açısından şifre tabanlı doğrulama mekanizmasından daha iyi performans gösteren doğrulama mekanizması henüz mevcut değildir ve bu kadar sık kullanılan bir mekanizmanın yerini başka bir mekanizmanın alacağı yakın zamanda ön görülmemektedir [1].

Kullanıcıların kolay hatırlanabilir/tahmin edilebilir şifreler seçtiği uzun zamandır bilinen bir gerçektir[19]. Bu sorunu aşmak için literatürde o anki girişin doğruluğunu tespit etmek için lokasyon-tabanlı [2, 12], cihaz parmakizi[3] ve davranışsal biyometri [4, 8, 15, 17, 18, 20] gibi birçok öneri sunulmuştur. Bu doğrulama tekniklerinin motivasyonu kullanıcı dostu olması ve şifrelerini zayıf seçen kullanıcıların bile hesaplarını koruma altına almak ve şifreleri çalınsa/tahmin edilebilse bile gerçek kullanıcıyı saldırgandan ayırmaktır. Bir diğer avantajı da, saldırganlar tarafından biyometri datalarını toplanmasının ve kopyalanmasının şifre kadar kolay olmamasıdır [21].

Bu gibi örtülü kimlik doğrulama tekniklerinin en büyük eksisi yüksek oranda yanlış kabul ve yanlış ret oranlarıdır. Ayrıca, genel kanının aksine davranışsal biyometri mekanizmalarına saldırı gerçekleştirilebildiği ve taklit edilebildiği gösterilmiştir[7]. Dolayısıyla, davranışsal biyometri kabul edilebilir bir seviyede hata oranına sahip olduğu senaryoda bile halen yardımcı bir doğrulama mekanizmasına ihtiyaç vardır.

Son yıllarda hızla popülerlik kazanan riske dayalı kimlik doğrulama mekanizmaları, birçok şirket tarafından uygulanmaya başlanmakta ve son kullanıcı bunu farketmese bile günlük hayatta sıklıkla bu mekanizmalardan faydalanmaktadır. Şirketlerin riske dayalı kimlik doğrulama sistemlerinin nasıl uygulandığını araştıran Wiefling ve diğ. [13] riske dayalı doğrulama implementasyonunda genel bir konsensüs olmadığı sonucuna varmasına rağmen tüm implementasyonlarda kullanıcıyı doğrularken en önemli indikatörün IP adresleri olduğu sonucuna varmış ve kullanıcı girişindeki IP adresinin değişmesi durumunda araştırmaya dahil olan tüm şirketlerde çok faktörlü doğrulamanın tetiklendiğini gözlemlemişlerdir.

Anomali tespit mekanizmalarında da benzer uygulamalar görmekteyiz. Örneğin, şirket içi ağlarda Siadati ve diğ. [14] ağ trafiğinin birçok noktadaki düğümlerin korelasyonu çıkarılarak anlık trafiğin önceki trafikle uyuşup uyuşmadığı tespit edilebileceği ve kötü niyetli trafik tespitinin bu yolla yapılabileceği gösterilmiştir.

Network anomali sistemleri tasarlanırken en çok karşılaşılan engeller, bu sistemlerdeki anomali datalarının çok az olması ve bu dataların ölçeklemesinin zor olmasıdır. Bu sorunu çözmek adına Freeman ve diğ. [5] data içerisindeki her feature'ın yani özelliğin olasılıksal tahminini(probability estimation) çıkararak istatistiksel bir yol izlemişler ve daha önceden görülmemiş özelliklerin önemini artırarak olasıkların arasındaki farkın çok fazla olmasının önüne geçmişlerdir.

Yakın zamana kadar anomali tespit yapay zeka uygulamaları üzerine yapılan araştırmalar genellikle tek bir yapay zeka bileşeni üzerine yoğunlaşır ve bu çalışmalarda bu bileşenin ne kadar geliştirilebileceği üzerine çalışılmıştır. Ancak, 2019 senesinde Solano ve diğ. [16] birden fazla makine öğrenimi bileşenlerini birleş-

tirmenin anomali tespitindeki performans iyileştirmelerini üzerine araştırmasıyla, birden fazla yapay zeka bileşeninden oluşan uygulamaların tek bileşene sahip yapay zeka uygulamalarına göre daha iyi performans verdiğini göstermiştir. Çalışmalarında fare ve klavye dinamiklerini The Wolf Of SUTD[29] adındaki halka açık bir datasetten almış ve bunları davranışsal biyometri dataları olarak yapay zeka algoritmasını eğitmişlerdir. Session datalarını da kendi uygulamalarından toplamışlardır ve bu dataları da ayrı bir yapay zeka algoritmasıyla eğitmişlerdir ve sonuç olarak bu iki yapay zeka uygulamasının ağırlıklı ortalamasını aldıklarında iki uygulamanın ayrı ayrı başarısından daha yüksek çıktığını göstermişlerdir.

2. GÜVENLİK ALGISI VE ŞİFRELER

Digital dünyada kullanıcıların bilgisayar kullanırken yaptığı güvenlikle alakalı çoğu hata aynı zamanda güvenlik açığı olarak değerlendirilir ve güvenlik politikalarının bu hatada büyük paya sahip olduğu kabul edilir. Kullanılan kriptoloji algoritmalarının veya güvenlik protokollerinin, yazılımda bir hata olmadığı takdirde güvenli oldukları düşünüldüğünde, güvenliğin sadece bu araçların doğru kullanıldığında bir anlamı olduğu unutulmamalıdır. Dolayısıyla, siber güvenlik problemi aslında bir kullanılabilirlik problemi olarak karşımıza çıkmaktadır.

Siber güvenliğin kuvveti sadece en zayıf halkası kadar kuvvetli olduğu ve en zayıf halkanın da insan olduğu herkes tarafından kabul edilir[35]. Saldırgan en zayıf halkayı kullanarak sisteme sızması halinde sistemde ne kadar güvenlik tabakası olursa olsun çok bir anlam ifade etmeyecektir. Bu yüzden saldırganlar güvenlik tabakalarını aşmakla uğraşmak yerine sosyal mühendislik veya insan hatalarından faydalanmaktadır. Siber güvenliğin en büyük problemlerinden birisi, günümüzde neredeyse herkesin farkında olmadan kullandığı siber güvenlik terimlerinin halk arasında bir anlam ifade etmemesidir. Çünkü, kullanıcıların bilgisayarın başına geçmesinin amacı aslında yapacakları işleri (mail atmak, internette gezinmek vb.) olabildiğince basit ve çabuk bir şekilde yapmaktır ve güvenlik yazılımlarının veya araçlarının asıl görevi siber güvenlik uygulamalarını olabildiğince sade tutarak kullanıcıyı hem rahatsız etmemeli hemde kullanıcının güvenlik zaafiyeti yaratmasının önüne geçmesidir. Çünkü, sistemi "güvenli" bir şekilde kullanmak kullanıcıların önceliklerinden birisi değildir ve güvenlik politikaları anlaşılması çok zor veya uğraştırıcı olursa kullanıcılar güvenlik önlemlerini kullanmaktan tama-

men vazgeçebilir ve güvensiz bir şekilde sistemi kullanmaya devam edebilir[34]. Dolayısıyla, güvenlik tasarımları sadece saldırganları engellemeyi amaçlamamalı aynı zamanda da bu güvenlik politikalarını uygulamak konusunda motivasyonu ve siber güvenlik konularında bilgisi olmayan insanlara göre tasarlanması gerekmektedir.

Güvenlik politikaları için en uygun çözüm yukarıda belirtilen sebeplerden ötürü, kritik güvenlik kararları verilirken insan faktörünü olabildiğince dışarda bırakmaktır ve olabildiğince güvenlik politikalarının otomatize edilmesi gerekmektedir. Ancak, bazı senaryolar için insanı dışarıda bırakmak ve kararları otomatize etmek gerek operasyonel zorluklar gerekse teknolojinin yeterli seviyede olmaması yüzünden mümkün değildir. İnsanın dışarıda kalamayacağı durumlarda güvenlik sisteminin makul seviyede bilgilendirici olmalıdır. Literatürde bazı araştırmalar bu bilgilendirici mesajları pasif ve aktif olarak ikiye ayırarak kullanıcıya sadece güvenlik için kritik kararları verdirme önerisinde bulunmuşlardır ve kullanıcının önemli ve tehlikeli olabilecek kararlara daha fazla dikkat etmelerini sağlamaya çalışmışlardır[36]. Aktif bilgilendirici mesajlar kullanıcıya bir karar vermeye zorlayarak kararlarının önemli olduğu izlenimi yaratmaya çalışır. Pasif kararlar ise daha az önemli ve tehlikeli bilgilendirici mesajlar olarak değerlendirildiği için kullanıcı bu mesajları tamamen yok sayarak yapmak istedikleri birincil işi yapmalarına izin verilebilir. Örneğin, Firefox oltalama önleyici aracı aktif bilgilendirici olarak değerlendirilebilir ve kullanıcının devam etmesi engellenerek bir kere daha düşünmesi istenir. Pasif bilgilendiriciye örnek olarak bir yazılımın güncellenmesi gösterilebilir. Ancak, bilgilendirici mesajlar, verilecek kararın ne kadar tehlikeli ve korkutucu sonuçları olabileceği izlenimini verecek şekilde tasarlansa

bile halen insan faktörünün "tehlikeli" kelimesini tam anlamadığını gösteren çalışmalar bulunmaktadır. Örneğin, Sunshine ve diğ.[37] tarayıcılardaki geçersiz ssl sertifika uyarısının kullanıcılar üzerinde ne kadar etkili olduğunu sınamak için 5 farklı geçersiz ssl sertifika uyarısını denekler arasında test etmişler ve deneklerin bu uyarılara nasıl reaksiyon verdiklerini gözlemlemişlerdir. Çalışmaları deneklerin en tehlikeli uyarı mesajını bile dikkate almadıklarını ve güvenlik uyarısına rağmen deneklerin %45'inin bankalarına bile giriş yaptıklarını göstermişlerdir. Girmeyen insanların bile bir kısmının aslında güvenlik endişeleri nedeniyle değil de sitede bir sorun olduğunu düşündükleri için girmemeleri aslında insanların güvenlik hakkında ne kadar bilgi sahibi olduklarını ve insan faktörünün güvenlikte ne kadar zayıf bir halka olduğunu net bir şekilde göstermektedir.

2.1 Şifre Tabanlı Kimlik Doğrulama Tarihçesi

Güvenliği tamamen insan faktörüne bağlı olan şifre tabanlı doğrulama sistemleri bilgisayarların ilk kullanılmaya başlanmasından beri en yaygın kullanılan kimlik doğrulama sistemidir. Türkçemize fransızcadan[9] chiffrer kelimesiyle giren şifreleri (ingilizce karşılığı encode veya encrypt [10, 11]) ilk olarak MIT tarafından 1961 [25] yılında geliştirilen zaman paylaşımlı işletim sisteminde (Compatible Time Sharing System - CTSS) görmekteyiz. Ancak, doğrulamanın insanlar tarafından seçilen bir şifre ile yapılmasının dezavantajları daha yayımlandıktan hemen sonra kullanıcıların birbirlerinin şifrelerini tahmin edebilmeleriyle ve admin yetkili 2 kullanıcının hatası yüzünden kullanıcıların şifrelerinin tutulduğu dosyanın tüm terminallerde günün mesajı olarak gösterilmesiyle daha o günlerden tanımlanmaya başlanmıştır. Bu dönemlerde yapılan çalışmalar ile de şifre

seçiminin önemi daha tam anlaşılmadığı için basit bir sözlük saldırısıyla bile şifrelerin %80'inin kırılabildiği gösterilmiştir [28]. Şifre seçimlerinin önemi zaman içerisinde anlaşıldıkça sözlük saldırılarının başarısı %80'lerden %25'lere kadar düşmesine rağmen[33] şifre güvenliğinin öneminin anlaşılmasına en çok yardımcı olan daha 23 yaşındaki Cornell Universitesi öğrencisi ve 2020 yılı itibariyle MIT'de profesör olan Robert Tappan Morris[1]'ın ilk bilinen solucanı yazması ile olmuştur. 1988 yılında yayımlanan Morris Solucanı, yaklaşık 400 kelimelik bir sözlük saldırısıyla bile ülke çapında tüm ağları çalışamaz hale getirmeyi başarmıştır.

> **Morris Solucanı**
>
> *Morris Solucanı özünde durum makinelerinden oluşan (State Machine) ve ağ içerisinde birden fazla metod kullanarak kendini çoğaltmaya çalışan bir solucandır. Eğer bir metod ile sistemi kıramaz ise diğer metodlarına başvuran Morris Solucanı, unix sistemlerinde kullanımı kolaylaştırmak için güven ilişkisini veya yüklü olan fingerd ile sendmail programlarının açıklarını sömürerek makineleri enfekte etmiş ve sözlük saldırısı ile kullanıcıların hesaplarına giriş yapmıştır.[31].*

Kullanıcılar Morris Solucanı gibi talihsiz olayları gördükçe zaman içerisinde şifreler konusunda daha bilgili davranmaktadır. Ancak, saldırı tekniklerinde de gelişmeler görmemiz, şifrelerin çok daha dikkatli seçilmesini gerektirmektedir ve günümüzde yapılan saldırılar önceki saldırılardan çok daha etkili olmaktadır. Ör-

[1]Robert T. Morris ve Robert Morris siber güvenlik araştırmacıları tarafından çok iyi tanınan ancak birbirlerine çok karıştırılan iki farklı bilim adamıdır. Robert T. Morris, Robert Morris'in oğludur. Robert Morris ilk sözlük saldırıları üzerine çalışmış ve Robert T. Morris ilk solucanı yazmıştır.

neğin, dünya çapında en sık kullanılan ücretsiz John the Ripper [30] milyonlarca kelimelik bir sözlüğe sahip bir şifre kırıcı aracı olarak karşımıza çıkmaktadır ve öncesinden çok daha verimli rainbow table'ları ile saldırganların kabiliyetleri de katlanarak artış göstermektedir[32].

2.2 Şifre Seçimi ve Şifrelerin Geleceği

Kullanıcıların siber güvenlik konusunda iyi bir bilgiye sahip veya güvenlik konularının uygulanmasında motivasyonu olmadığı için şifre seçimi konularında yanlış seçimler yapabilmektedir. Teorik olarak şifrelerin anahtar boyutu (keyspace) güvenli sayılabilecek bir güvenlik sağlar ve anahtar boyutunun maksimum entropisi aşağıdaki formül ile hesaplanabilir[38].

$$H_{max} = log_2 c^n$$

Burada n karakter boyutu ve c ise olası tüm karakterleri ifade etmektedir. İstatistiksel entropi olarak adlandırılan bu formül bize kullanıcıların olası anahtar boyutu içerisinden seçtikleri şifrenin ne kadar belirsiz olduğunun bit tabanında bir ölçütüdür. En somut örnek olarak, 4 haneden oluşan PIN'in anahtar boyutu her hane 10 farklı değer alabildiği için 10^4 yani 10000'dir ve entropisi de $log_2 10000 = 13.3$ bittir. Ancak, insanlar PIN seçerken rasgele seçmediği ve hatırlanabilirliği daha kolay şifreler seçtikleri bilinmektedir ve gerçek entropi bu değerden son derece düşüktür. Örneğin, şifresini doğum yılı yapan ve 2000'den önce ve 1940'dan sonra doğan birisinin şifresi, ilk hanesi için 1, ikinci hanesi için 9, üçüncü hanesi için 4-9

ve dördüncü hanesi için 0-9 değerlerini alabildiği için 1x1x6x10 = 60 farklı değere sahip olabilir ve entropisinin $log_2 60 = 5.9$ bit olduğu düşünüldüğünde yaklaşık 7 bit daha az anahtar boyutuna sahiptir.

İnsanlar şifre seçerken rasgele seçmediği ve daha hatırlanabilir bir havuzdan şifrelerini seçmesi şifre tabanlı doğrulama sistemlerini sözlük saldırısı gibi saldırılara açık hale getirmektedir. Ancak, tüm sorunlarına rağmen günümüzde halen şifre tabanlı doğrulama mekanizmasını en çok kullanılan doğrulama mekanizması olarak görmekteyiz. Bunun nedenleri arasında şifre tabanlı doğrulama mekanizmasının yerine geçebilmek için gerek kullanışlılık gerekse ulaşılabilirlik açısından bazı şartların sağlanması gerektiğidir ve alternatif olarak sunulan seçeneklerin bu şartları sağlamadığını görmekteyiz [27]. Bunlardan bazılarına değinecek olursak:

- ***Kolaylık:*** Çoğu kullanıcı şifre tabanlı doğrulamayı kolay bir doğrulama mekanizması olarak görmekte ve kullanıcıların kullanması daha zor bir alternatif için isteksiz davranmaları
- ***Erişilebilirlik:*** Günümüzde neredeyse tüm servisler şifre tabanlı doğrulamayı kullanmakta ve yeni bir teknoloji için gerekli adaptasyonun olmaması
- ***Ekonomik Nedenler:*** Kullanıcılara daha güvenli bir hizmet vererek kullanıcıları daha çok uğraştırmak ve daha az güvenli ama daha kullanışlı bir şirkete müşterilerini kaptırma ihtimalinden korkmaları

Bu gibi nedenlerden ötürü şifre tabanlı doğrulama mekanizmasını günümüzde halen en çok kullanılan kimlik doğrulama seçeneği olarak görüyoruz.

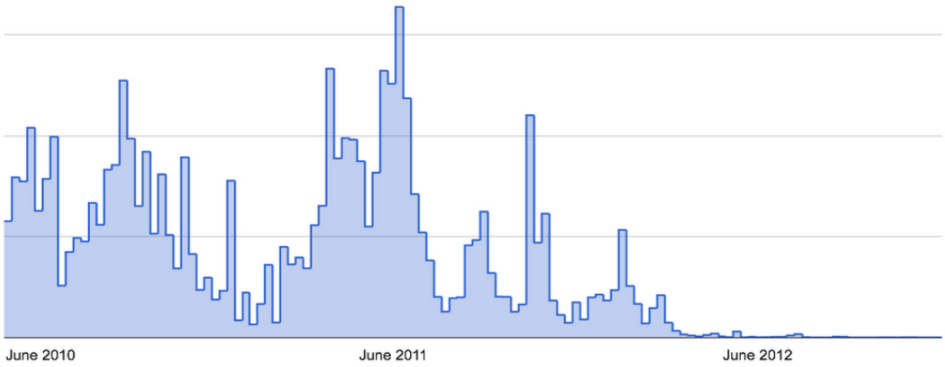
2.3 Risk Tabanlı Kimlik Doğrulama

Şifre tabanlı kimlik doğrulama mekanizmalarının zaafiyetleri ve kullanışsızlığı bilindiği ve yerine başka bir doğrulama mekanizmasının geçmesi gerektiği tüm siber güvenlik araştırmacıları tarafından kabul edilir. Ancak, 2004 yılında RSA konferansında Bill Gates'in "Şifreler artık öldü" [26] sözünden neredeyse 20 yıl geçmesine rağmen şifre tabanlı doğrulamanın yerine geçebilecek rakip bir kimlik doğrulama mekanizması çıkmadığı gibi şifre tabanlı doğrulamanın popülerliği internetin yaygınlaşmasıyla katlanarak artmıştır.

Riske dayalı doğrulama şifrelerin yaygınlaşmasının devam edeceği öngörüsüyle hazırlanmıştır ve şifre tabanlı doğrulamayı daha güvenli hale getiren bir doğrulama mekanizmasıdır. Riske dayalı doğrulama mekanizması, kullanıcının sadece şifresinin doğru olmasını değil aynı zamanda kullanıcının IP adresi, işletim sistemi ve klavye dinamiği gibi kullanıcıdan gelen çok farklı özellikleri kullanarak kullanıcının doğrulandığı doğrulama mekanizmasıdır.

Riske dayalı doğrulama mekanizması içerisinde kullanılan her bir özellik taklit edilebilir olmasına rağmen buradaki varsayım, riske dayalı doğrulamada kullanılan özelliklerin çok boyutluluğundan dolayı saldırganların tüm bu özellikleri taklit etmesinin pratikte pek mümkün olmamasıdır. Bu mekanizmanın en büyük başarısını Google'in verilerinde görebiliriz. Örneğin, Google'ın verilerine göre, Gmail'de kullanıcılarını korumak ve spama karşı etkili bir mücadele vermek için çok gelişmiş bir spam filtresi kullanılmaktadır. Genel olarak iyi performans gösteren bu filtre, Gmail kullanıcılarının daha önceden iletişime geçtiği insanların mesajlarına karşı iyi çalışmamakta ve Gmail kullanıcılarının gelen kutusuna dü-

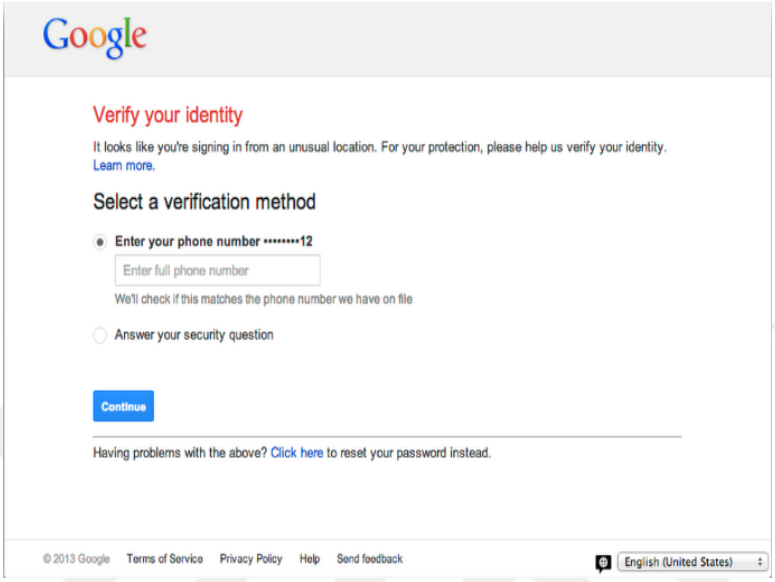
şen mesajların yüzde biri tanıdığımız insanlardan gelen spamlardan oluşmaktadır. Gelen kutusuna düşen bu spam mesajlarının çoğu, Gmail kullanıcılarının hesaplarında kullandıkları şifreleri başka hesaplarda da kullanmaları ve saldırganların bu kullanılan websitelerden Gmail şifrelerini çıkarmaları yüzünden gerçekleşmektedir. 2010 ve 2011 yılları arasında Gmail hesaplarına olan saldırı tavan yapmış ve saldırganlar her saniye 100 tane Gmail hesabına girme teşebüsünde bulunmuşlardır. Ancak 2011 yılından sonra Google, Gmail'e giriş için sadece şifrenin doğru olması kriterini kaldırarak riske dayalı doğrulama mekanizmasını kullanmaya başlamış ve saldırganların başarı oranlarında büyük bir düşüş gözlemlenmiştir [23].



Şekil 2.1: Gmail hesaplarından gelen spam mesajlarının 2010-2012 yılları arası miktarı

2011 yılında tavan yapan saldırılar ve ele geçirilen Gmail hesaplarından sonra 2012 yılında yüzde 99.7 kadar büyük bir başarı sağlamalarının en büyük nedeni, şifre dışında 120 farklı değişken kullanarak kullanıcının doğruluğuna karar verilmesidir. Bu mekanizma ile eğer bir giriş şüpheli bulunursa, örneğin okyanus ötesi veya önceden kullanılmayan bir bilgisayardan giriş, kullanıcıya aşağıda gösterilen hesabın kayıtlı olduğu telefon numarası veya güvenlik sorusu gibi kullanıcı için

basit ancak saldırgan için cevaplaması zor sorular sorularak yüzde 99.7 oranında şüpheli girişlerin hesabı kontrol etmesinin önüne geçilmiştir.



Şekil 2.2: Şüpheli girişlerde kullanılan risk tabanlı doğrulama ekranı

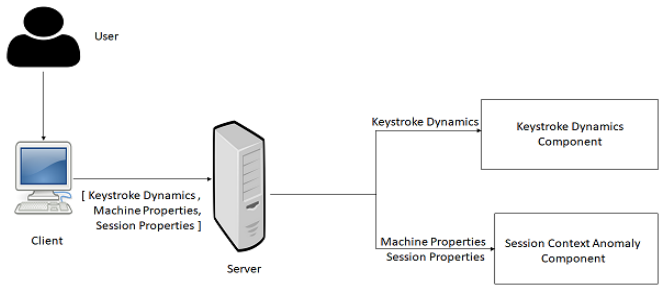
3. DENEY HAZIRLIK AŞAMASI

Deneyimizde riske dayalı doğrulama mekanizmasının gerçek bir senaryoda nasıl çalışabileceğini araştırdık. Bunun için klavye dinamiği ve bağlamsal anomali bileşenlerini oluşturduk. Ardından bu 2 bileşenin nasıl birleştirilebileceği üzerine denemeler gerçekleştirdik.

3.1 Dataların Toplanması

Deneyde kullandığımız datalar, kullanıcıların kullanıcı adı ve şifresini girmesi gerektiği yaklaşık 6 ay süren bilgiledirme ve duyuruların yapıldığı bir kurs websitesi üzerinden toplandı. Gizlilik gerekçesiyle, kullanıcı adlarının hashlenmiş versiyonları tutuldu ve kullanıcılara farklı bir websitesinde kullandıkları şifreyi bizim sitemizde de kullanmamaları için kendi şifrelerini seçmelerine izin verilmedi [6]. Tüm kullanıcılara "operatingsystem" ile başlayan ve 4 farklı rakamla biten birer şifre verildi.

Kullanıcıların websitesiye her girişlerinde makine bilgileri(Machine Properties), oturum bilgileri(Session Properties) ve klavye vuruş bilgileri(Keystroke Dynamics) toplandı ve toplanan makine bilgileri ve oturum bilgileri bağlamsal anomali (Session Context Anomaly Component) ve klavye vuruş bilgileri klavye dinamik(Keystroke Dynamics Component) yapay zeka algoritmalarını eğitmek için kullanıldı. Klavye dinamikleri bilgileri toplamak için kullanıcı adı ve şifresini dinleyen bizim yazdığımız bir javascript ile toplandı. Yaklaşık 6 ay süren kurs boyunca toplamda 102 farklı kullanıcıdan 4748 giriş bilgisi elde edildi.



Resim 3.1: Her girişte gerçekleşen örnek data akışı

3.2 Data Özellikleri

Yukarıda ki bölümde belirtildiği gibi kullanıcıların her girişlerinde klavye dinamikleri, makine ve oturum bilgileri toplandı. Toplanan bu dataları detaylandırmak gerekirse; makine özellikleri için topladığımız özellikler işletim sistemi(operating system), monitör boyutu(screen-size) ve girişte kullanılan tarayıcı türü(browser-type), oturum bilgileri için topladığımız özellikler şehir(city), internet sağlayıcısı(ISP) ve giriş yapılan tarih(time of login) ve son olarak klavye dinamikleri için tuş basma ve tuş çekme arasındaki zaman aralıkları toplandı.

Çizelge 3.1: Toplanan data özeti

Data Field	**Description**
Keystroke Dynamics	*Timestamps of Key-up and Key-down Events*
Machine Properties	*Operating System, Screen-size, Browser Type*
Session Properties	*City, ISP, Time of Login*

3.3 Saldırı Simülasyonu

Saldırı simülasyonunu gerçekleştirmek için websitemize en az 20 defa giren 29 öğrenci seçildi ve yetkisiz girişi simüle etmek için farklı konumlardan veya farklı

internet sağlayıcısı ile en az 10 defa giriş yaptık. Saldırı simülasyonunun yarısını aynı şehirden ama farklı internet sağlayıcısıyla diğer yarısını ise vpn kullanarak ülke dışından giriş yaptık. Tüm saldırılarda ise farklı işletim sistemleri, internet tarayıcısı ve giriş zamanı kullandık.

4. KİMLİK DOĞRULAMA ANOMALİ TESPİT SİSTEMLERİ

Deneyimiz sırasında toplamda bağlamsal anomali ve klavye dinamiği bileşeni olmak üzere 2 farklı anomali yapay zeka bileşenleri oluşturduk ve bunları kendi aralarında karşılaştırdık. Bunları birleştirerek üçüncü bir model olarak yapay zeka algoritmalarında çokça kullanılan ve ağırlıklı ortalama tekniğini kullanan topluluk modeli(ensemble model) oluşturduk. Son olarak, klavye dinamiğinden çıkan skoru bağlamsal anomali yapay zeka bileşenimize yeni bir özellik(feature) olarak eğittik.

Yapay zeka algoritması olarak deneylerimiz, en iyi performans veren algoritmanın klavye dinamiği bileşeni için isolation forest ve bağlamsal anomali bileşeni için random forest olduğunu gözlemledik. Seçtiğimiz 29 öğrenciden toplamda 2870 giriş datasını kullandık ve bu dataların aynı eğitme(train) ve test dataları olmak şartıyla %70 eğitme ve %30 test olacak şekilde deneylerimizi tamamladık.

4.1 Klavye Dinamiği Bileşeni

Klavye dinamiği bileşenimizde kullanılan datalar, giriş anında kullanıcıların kullanıcı adı ve şifrelerini girdikleri alanlarda toplandı. Her form alanı için vuruş

basma(key-down) ve vuruş çekme(key-up) olaylarının(event) zaman aralıkları (timestamp) çıkartıldı ve bu basılan tuşlar için aşağıdaki gibi 2 özellik(feature) oluşturuldu:

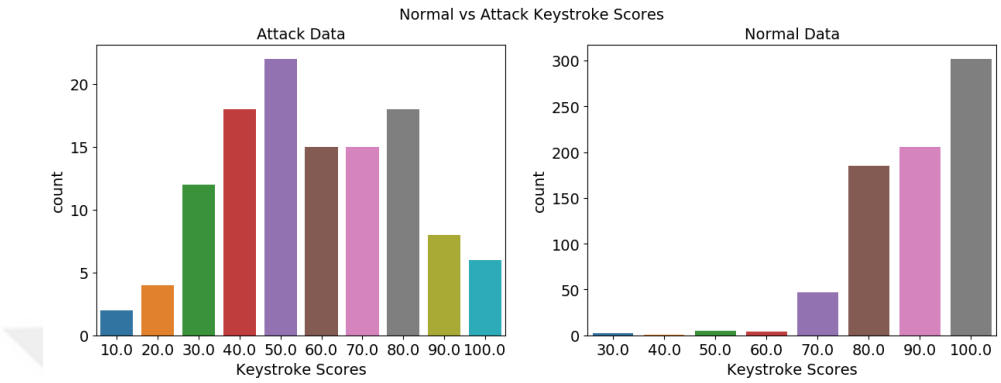
$$F_1 = T_{KeyUp}(n) - T_{KeyDown}(n)$$

$$F_2 = T_{KeyUp}(n) - T_{KeyUp}(n+1)$$

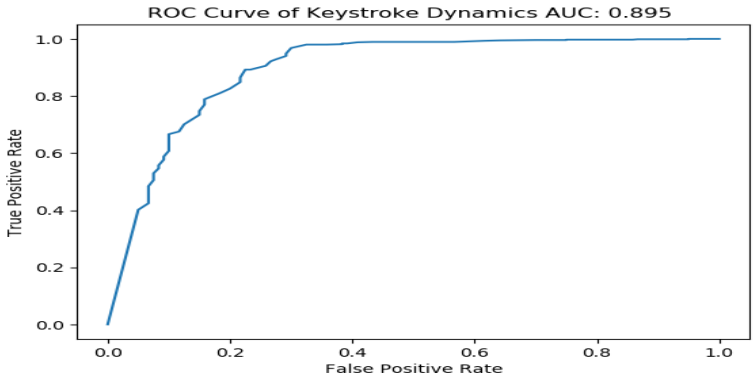
Burada F yaratılan özelliği, T basılan zamanı ve n basılan tuşun sırasını temsil etmektedir. Isolation forest yapay zeka algoritmasını kullanan klavye dinamiği algoritması kullanıcının ilk 20 girişine kadar üretilen datalarla eğitilmektedir. Bundan sonraki tüm girişlerde kullanıcının o anki klavye dinamiğinin bir önceki girişlere uyup uymadığı 0 ile 1 arasında bir skorla hesaplanmaktadır. Eğer o anki giriş 1 veya 1'e yakınsa bir önceki girişlerle yüksek benzerlik gösterdiği sonucu çıkarılmaktadır. Eğer 0 veya 0'a yakınsa kullanıcının gerçek kullanıcı olmadığı sonucu çıkarılmaktadır.

Klavye dinamiği bileşenini analiz ettiğimizde gerçek kullanıcıyı gerçek olmayan girişten, yani saldırı simülasyonu girişimizden, %18 eşit hata oranı(EER) [2] ve %86 eşik değerleriyle(threshold) başarılı bir şekilde ayırdığını gözlemledik. Klavye dinamik algoritmasının normal giriş ve saldırı giriş skorları ve sistemin ROC eğrisi aşağıdaki gibidir.

[2]Burada Tip-1 ve tip-2 hata tipleri bağımsız değildir ve herhangi bir hata tipinde ki düşüş bir diğerinde yükselişe neden olmaktadır. Biyometri gibi anomali sistemlerinde en çok kullanılan performans testlerinden birisi de eşit hata oranı olarak türkçeye çevirebileceğimiz Equal Error Rate(ERR)'tir. Eşit hata oranı tip-1 ve tip-2 hata tiplerinin eşit olduğu oran demektir ve bu gibi sistemlerde optimal başarıyı ifade etmektedir.



Şekil 4.1: Klavye Dinamik bileşeninin gerçek kullanıcı ve saldırgan başarı skorları



Şekil 4.2: Klavye dinamik bileşeni ROC eğrisi.

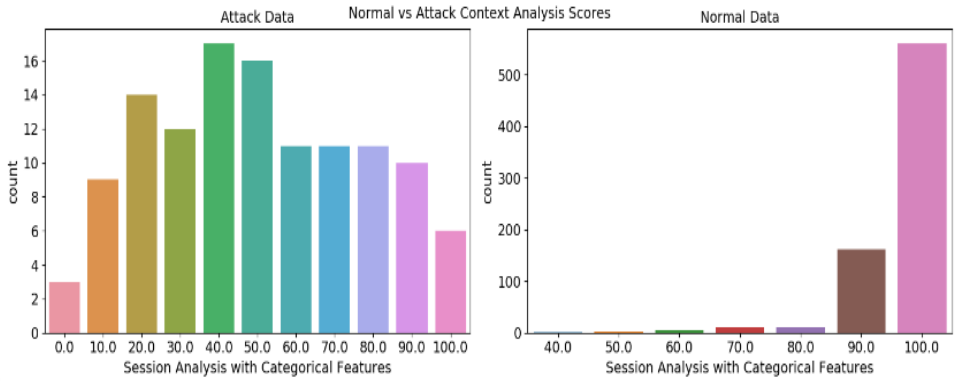
4.2 Bağlamsal Anomali Bileşeni

Bağlamsal anomali bileşeninin eğitileceği datalarda IP adresi veya giriş tarihi gibi değerler olduğu için öncelikle dataların formatının değiştirilmesi gerekmektedir. Bunun için öncelikle yazdığımız bir python kodu ile datamızdaki her IP adresinin internet sağlayıcısı ve şehir bilgilerini çıkardık ve 33 farklı şehir ve 19 farklı internet sağlayıcısı olduğunu bulduk. Giriş zamanını ise 24 saat dilimde sabah(morning), öğle vakti(lunch-time) ve akşam(afternoon) olmak üzere toplam 6 zaman dilimine ayırdık. Tarayıcılar için ise tarayıcıların sadece türünü deneyimize dahil ettik. Örneğin Chrome sürüm v.x tarayıcısını sadece Chrome olarak ele aldık ve bu prosedürü diğer tüm tarayıcılar için uyguladık.

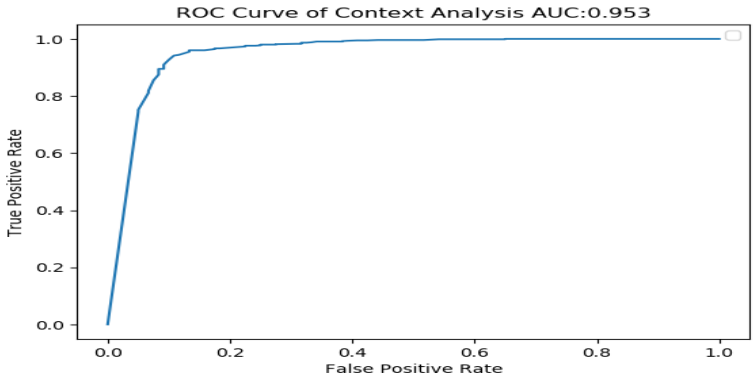
Datamızdan özellikleri çıkardıktan sonra(feature extraction), bu dataların yapay zeka algoritmasına eğitilmesi gerekmektedir. Ancak, bağlamsal anomali algoritmasında kullanılacak datalar işletim sistemi, şehir, internet sağlayıcı gibi kelimelerden oluştukları için bu kategorik dataların yapay zeka algoritmları tarafından anlaşıp analiz edilebilmesi için matematiksel karşılıklarına çevirmemiz gerekmektedir. Bunun için kategorik özellikleri olan datalarda kullanılann one-hot encoding denen bir yöntemi kullandık. Somut bir örnek olarak, kategorik örneklerin matematiksel karşılıkları 1 veya 0 oldukları için, eğer bir giriş X şehrine ait ise, o girişin şehir X özelliği(feature) 1 olmakta ve diğer şehirlerin özelliği 0 olmaktadır. Aynı prosedür diğer tüm özellikler içinde uygulanmıştır.

Bağlamsal anomali bileşenimizin başarısını incelediğimizde bileşenin gerçek kullanıcıyı saldırgandan %9 eşit ağırlık oranı ve %95 eşik değeriyle ayırabildiğini gözlemledik. Bağlamsal anomaliye ait gerçek kullanıcı/saldırgan skorları ve ROC

eğrisi aşağıdaki gibidir.



Şekil 4.3: Bağlamsal Anomali bileşeninin gerçek kullanıcı ve saldırgan başarı skorları



Şekil 4.4: Bağlamsal Anomali bileşeni ROC eğrisi

4.3 Topluluk Modeli

Klavye dinamiği ve bağlamsal anomali bileşenlerimizi oluşturduktan sonra bu iki bileşenden topluluk modeli oluşturduk ve önceki bileşenlerin başarılarılarıyla karşılaştırdık. Bunun için yapay zekada çok kullanılan oylama konvensiyonuna dayanan ağırlıklı ortalama modelini kullandık.

Özetle, topluluk modeli sadece bir yapay zeka bileşeninden gelen olasılıksal skora bakarak karar vermek yerine birden fazla yapay zeka bileşeninden gelen skorlara göre karar vermektedir. Örneğin, iki yapay zeka bileşeninden oluşan topluluk modeli aşağıdaki formül ile ifade edilebilir:

$$y = ax_1 + bx_2$$

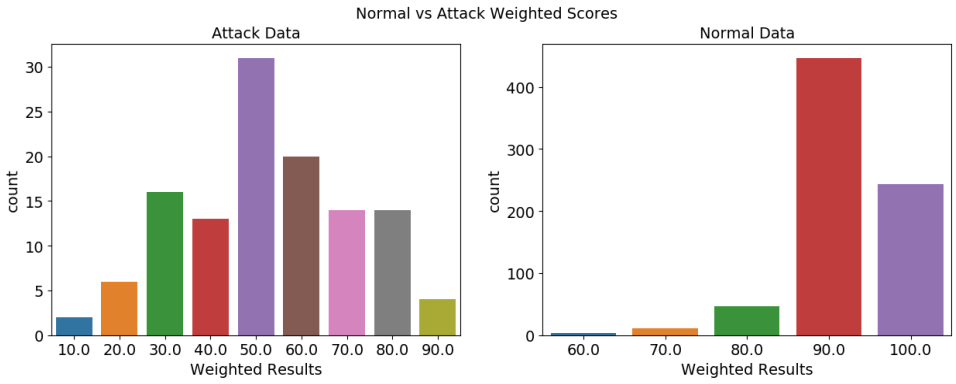
Burada x_1 ve x_2 ile gösterilen değişkenler 0 ile 1 arasında 2 farklı yapay zeka bileşeninden gelen olasılıksal skoru temsil etmektedir. a ve b ile gösterilen değişkenler de bu değişkenlerin katsayıları olmakla beraber aşağıdaki denklemi sağlayarak

$$a + b = 1$$

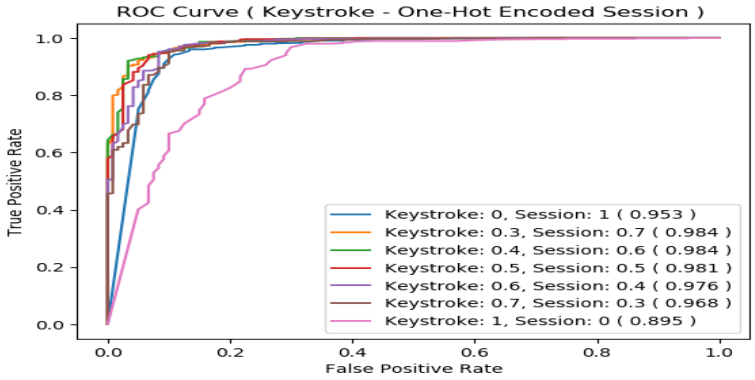
topluluk modelinde çıkan skorun tekrar 0 ile 1 arasında bir olasılık skoru elde edilir.

Deneyimizde klavye dinamiği ve bağlamsal anomali bileşeni(x_1 ve x_2) olmak üzere 2 farklı yapay zeka bileşeni kullandık ve farklı katsayılar(a ve b) ile top-

luluk modelinin performasını diğer 2 modelle karşılaştırdık. Beklediğimiz gibi bir yapay zeka bileşeninin katsayısına 1 diğerine 0 verdiğimiz zaman topluluk modelinde tek bileşen varmış gibi davrandığını ve önceki deneylerimizde elde ettiğimiz sonuçları tekrar gözlemledik. Ama, katsayıları her iki bileşeninde sonuca katkı edebilecek şekilde değiştirdiğimiz zaman önceki tek bileşene sahip modellerde elde ettiğimiz sonuçlardan her zaman daha iyi sonuç verdiğini gözlemledik. Grafikte de görülebileceği gibi en iyi performansı veren modelin katsayıları ise bağlamsal anomali bileşeni için 0.6 ve klavye dinamiği bileşeni için 0.4'dür. Bu katsayılarla topluluk modeli doğru kullanıcıyı saldırgandan %6 eşit hata oranı ve %0.89 ile ayırabildiğini gözlemledik.



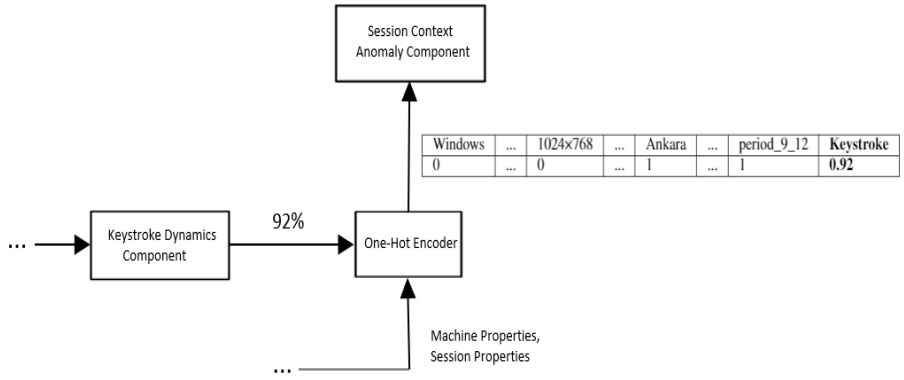
Şekil 4.5: En iyi performans gösteren katsayılarla oluşturulan Topluluk Modelinin gerçek kullanıcı ve salgırgan başarı skorları



Şekil 4.6: Farklı katsayılara göre Topluluk Modeli ROC eğrisi

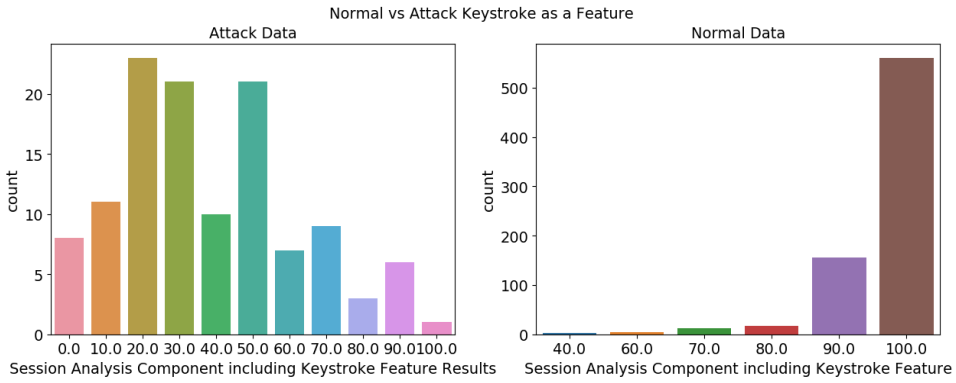
4.4 Özellik Olarak Klavye Dinamiği

Bağlamsal anomali bileşenini eğitmek için kategorik dataları matematiksel karşılıkları olan binary yani 1 veya 0'a çevirmiştik. Bu bölüm için tamamen 0 ve 1'lerden oluşan bu dataset içerisine klavye dinamiği bileşeninden gelen skoru ekleyerek bağlamsal anomali bileşenini fazladan 1 özellik ile tekrar oluşturduk ve bu değiştirilmiş dataset ile bağlamsal anomali bileşenini tekrar eğittik. Örneğin, kullanıcı giriş yaptığı zaman önce klavye dinamiği bileşeni kullanıcının klavye dinaik skorunu hesapladıktan sonra one-hot encoder'dan çıkan binary dataset'ine bu çıkan skoru ekledik. Somut örnek olarak, bu model için klavye dinamiği skoru %92 olan bir kullanıcının data akışı aşağıdaki gibidir.

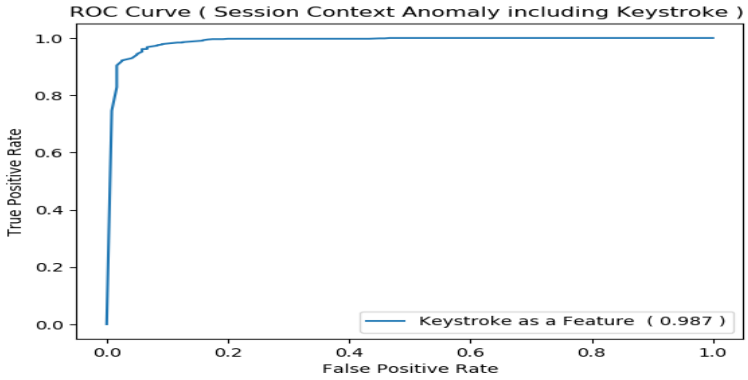


Resim 4.1: Klavye dinamik skorlarının bağlamsal anomali datalarına eklenme örneği.

Bu yaklaşımla içerisinde klavye dinamik skoru olan dataset ile eğitilen bağlamsal anomali bileşeni en iyi katsayılar verilen topluluk modelinden bile daha iyi performans verdiği sonucuna ulaşıldı. Bu değiştirilmiş model doğru kullanıcıyı saldırgandan %5 eşit hata oranı ve %91 eşik değeri ile ayırt edebildiği gözlemlendi.



Şekil 4.7: Klavye dinamik skorunun bağlamsal anomali bileşeni gerçek kullanıcı ve saldırgan başarı skorları



Şekil 4.8: Klavye dinamik skorunun bağlamsal anomali bileşeni içerisinde kullanımı ROC eğrisi

5. DEĞERLENDİRME

Deneyimiz sırasında 2 farklı anomali modeli oluşturduk ve bu modelleri kullanarak birleşimlerinden 2 farklı model daha oluşturduk(Performans karşılaştırması için bkz. Çizelge 5.1). Çizelgeden de görülebileceği gibi, en iyi performans gösteren modelimizin klavye dinamiğini bir özellik olarak kullanan bağlamsal anomali modelimiz(KaaF) olduğunu gözlemledik. Bu modelimizin neden topluluk modelimizden bile daha iyi performans verdiğini incelediğimizde, bir sonuca varırken sadece kullanıcının klavye dinamiği skorunu hesaba katmadığı ayrıca kullanıcıların klavye dinamiği değişimlerinide hesaba kattığını ve klavye dinamik skor değişimleri yüksek olan kullanıcıların klavye dinamik skorlarının öneminin düştüğünü gözlemledik. Klavye dinamik skorunun önemini ölçmek için açık kaynak kodlu bir yapay zeka kütüphanesi olan scikit learn'ün random forest algoritmaları için sağladığı özellik önem(feature importance) methodlarını kullandık. Scikit-learn'ün random forest için bize sunduğu özellik önem hesaplama algoritmalarını özetlemek gerekirse, scikit-learn'de permütasyon önem(permutation importance) ve gini önem(gini importance) olmak üzere 2 tür özellik önem algoritması bulunmaktadır [24]. Permütasyon önem algoritmasında, özelliklerin önemi datasette ki özelliklerin permütasyonu ile modelin performansı karşılaştırılmakta ve bir özelliğin datasetten çıkartılmasının performansa etkisi ile hesaplanmaktadır. Ancak, permütasyon önem algoritması datasetteki özelliklerin korelasyon olmayan bağımsız değişkenler olduğu hipotezine dayanmaktadır ve bizim anomali tespit sistemimizde ki özellikler yüksek korelasyona sahip olduğu için bu önem algoritması bizim için uygun değildir. Öte yandan, gini önem algoritması özelliklerin önemini karar ağaçlarında(decision tree) entropiyi(impurity) ne kadar düşürdüğüne göre

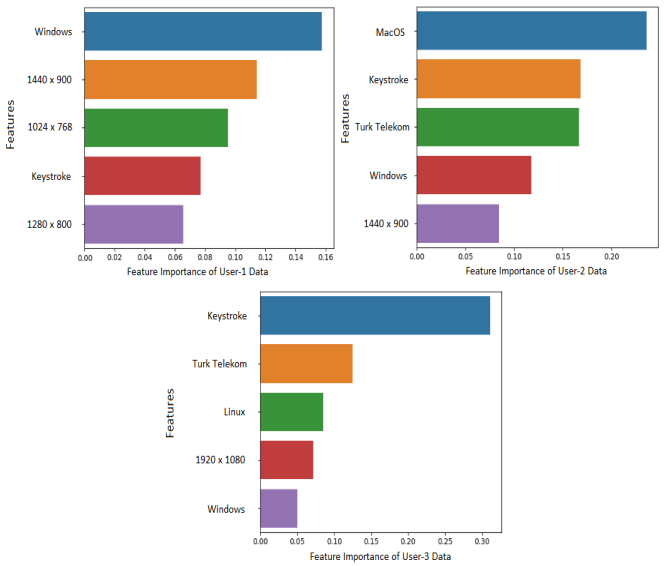
karar vermektedir.

Şekil 5.1'de gösterildiği gibi, gini özellik önemi algoritmasını kullanarak deviasyonu en yüksek, orta ve en düşük öğrencilerin en önemli 5 özelliğini çıkardık. Grafiklerde gösterildiği gibi klavye dinamiği özelliğinin önemi (keystroke) klavye dinamiği deviasyonu artıkça azalma eğiliminde olduğu görülecektir. Ancak, bu iki modeli topluluk modelinde olduğu gibi lineer bir şekilde ele aldığımız zaman, deviasyon bilgisini kaybettiğimiz için daha düşük performans da bir model elde ettik.

Bu modelin eksi yanıysa bağlamsal anomali bileşeni klavye dinamiği bileşeninin sonucunu beklemek zorunda olduğu için bu iki model paralel bir şekilde çalışamamakta ve seri bir şekilde çalışmak zorunda kalmaktadır. Bu özelliğide topluluk modelinden biraz daha yavaş bir model olmasına yol açmaktadır. Ancak, bu gecikme birkaç milisaniye olacağından kullanıcı deneyimini etkilemeyecektir.

Deneyimiz sırasında odaklandığımız noktalar daha çok riske dayalı doğrulama sistemlerinin beraber kullanılmasından elde edeceğimiz performans artışı olduğu için başka senaryolarda faydalı olabilecek bilgileri deneyimize dahil etmedik. Örneğin, bağlamsal anomali sistemlerinde en önemli özelliklerden birisi kullanıcının hangi tarayıcı sürümünü kullandığı bilgisidir. Ancak, deneyimiz sırasında biz bu bilgiyi sadece tarayıcı türü olarak deneyimize dahil ettik ve deneylerimizde tarayıcı sürümüne baktığımız zaman bu bilginin merdiven benzeri bir yapıda olduğunu ve kullanıcı bir kere tarayıcısını güncellediğinde sonraki girişlerinde hiçbir zaman bir önceki sürümle girmediğini gözlemledik. Tarayıcı sürümünün sıralı kategorik datalar sınıfına girdiği için de tarayıcı sürümünün farklı bir şekilde ele

alınabileceğini düşünüyoruz(Örneğin o anki tarayıcı sürümü hiçbir zaman bir önceki girişlerinde ki sürümünden daha az olmayacak gibi). İleride yapabileceğimiz ve bu deneyde uygulamadığımız bir diğer önemli atladığımız bilgide bir kullanıcının kaç defa başarısız deneme girişinde bulunduğu bilgisidir. Bu bilgi örneğin bankacılık gibi uygulamalarda faydalı olabilir ve başarısız bir giriş denemesinden sonra eşik değerinin(threshold) yükseltilmesi gibi çözümler sunabilir.



Şekil 5.1: Standard deviasyon (std) değerlerine göre klavye dinamik skorlarının önemi: std (User-1): 15.04%, std(User-2): 10.49%, std(User-3): 5.16%.

Çizelge 5.1: Performans özeti - Gerçek Giriş (752 test datası), Saldırı Simülasyon Girişi (120 test datası) (KaaF keystroke as a feature kısaltmasıdır).

Metrics	Keystroke	Session	Weighted	KaaF
Equal Error Rate (EER)	18.67 %	9.1 %	6.3 %	5.29 %
EER Threshold	86 %	95 %	89 %	91 %
Precision (Legitimate)	96.51 %	98.42 %	99.01 %	99.16 %
Recall (Legitimate)	80.98 %	90.96 %	93.22 %	94.41 %
F1-Score (Legitimate)	88.07 %	94.54 %	96.03 %	96.73 %
Precision (Attack)	40.66 %	61.58 %	68.90 %	73.08 %
Recall (Attack)	81.67 %	90.83 %	94.17 %	95 %
F1-Score (Attack)	54.29 %	73.40 %	79.58 %	82.61 %
Accuracy	81.08 %	90.94 %	93.35 %	94.5 %

5.1 Karşılaşılan zorluklar

Klavye dinamiğinin nispeten kötü performans vermesinin en büyük nedeni gizlilik gerekçesiyle her kullanıcıya bizim seçtiğimiz bir şifreyi vermemiz ve alışık oldukları kendi şifrelerini seçmelerine izin vermediğimiz için verilen şifreyi yazma konusunda saldırgandan sadece biraz daha tecrübeli olmalarıdır. Ancak, kullanıcılar yazarken daha rahat yazabildikleri kendi şifrelerini seçebildikleri senaryolarda saldırganla aralarında çok daha fazla bir fark olacağı görüşündeyiz.

Deneylerimiz sırasında websitemize bağlanan tüm kullanıcıların birkaç istisna dışında sürekli Ankara'dan bağlandıklarını ve bağlamsal değişkenlerin bir banka uygulanmasında olacağı gibi yüksek olmadığını gözlemledik. Banka uygulaması gibi geniş bir kitle tarafından kullanılan bir uygulamada bağlamsal anomali bileşenimizin daha az performansa sahip olacağını düşünüyoruz.

Deneyimizi uygularken karşılaştığımız zorluklar açısından, bazı kullanıcıların tarayıcılarında şifre yöneticisi veya html form otomatik doldurma özelliğinin etkinleştirdiklerini gözlemledik. Klavye dinamiği bileşenimiz kullanıcı adı ve şifre alanlarının kullanıcı tarafından doldurulmasını gerektirdiğinden, deneyimizi gerçekleştirmek için otomatik doldurma özelliği olsa bile gerekli alanları silmemiz gerekti ve kullanıcılardan kimlik bilgilerini tekrar girmeleri istendi. Bu gereksinim, klavye dinamiği bileşenlerinin genel dezavantajlarından biri olduğunu düşünüyoruz.

Diğer karşılaştığımız zorluk ise, akıllı telefonların klavyelerinin tuş basma ve tuş çekme olaylarını desteklememesi ve bu olayların aynı anda tetiklenmesidir. Tuş

basma ve tuş çekme olaylarının aynı anda tetiklenmesi klavye dinamiği bileşeni bölümünde bahsettiğimiz yaratılan 2 özellikten birisini sıfırladığı için büyük bir performans kaybına yol açmaktadır. Bu sorunu çözmek akıllı telefon klavyelerinin yeniden yazılmasını veya sadece akıllı telefonlara özel bir deney dizaynı gerektirdiği için bu sorunu gelecek çalışmalarımızda ele almaya karar verdik.

6. SONUÇ VE ÖNERİLER

Günümüzde zayıf şifreye sahip veya çalıntı hesapları korumak için en sık kullanılan yöntem iki faktörlü doğrulama güvenlik mekanizmasıdır. İki faktörlü doğrulama, her ne kadar hesapların çalınmasına karşı etkili bir yöntem olsada, kullanışsızlığı yüzünden kullanıcılar tarafından tercih edilen bir güvenlik mekanizması değildir. Şifre tabanlı sistemleri daha kullanışlı bir güvenlik mekanizmasıyla korumak siber güvenlik araştırmaları için çok önemli bir yer teşkil etmektedir ve daha kullanışlı bir anomali tespit sistemiyle iki faktörlü doğrulama sadece girişte bir anomali tespit edildiğinde aktif hale getirilerek sistem hem daha güvenli hem de daha kullanışlı hale getirilebilir.

Bu tezde gerçekçi bir senaryoya uygun bir şekilde oluşturduğumuz bir websitesi ile kullanışlılığa bir etkisi olmadan güvenliği artıran klavye dinamiği ve bağlamsal anomali tespit bileşenlerini test ettik ve bu bileşenleri birleştirmenin performansa etkilerini araştırdık. Bulgularımız bu iki bileşenin birleştirilmesiyle oluşturulan sistemin sadece bir anomali bileşenine sahip bileşenden daha iyi performans verdiği gösterdi. Ayrıca, klavye dinamiğinden çıkan skorları bağlamsal anomali bileşenine bir özellik olarak eğittiğimizde bağlamsal anomali bileşeni klavye dinami-

ğindeki sapmalara göre de karar verebildiği için 2 bileşeni lineer olarak ele alan topluluk modelinden daha iyi performans verdiğini gözlemledik.

KAYNAKLAR

[1] **C. Herley and P. van Oorschot**, "A research agenda acknowledging the persistence of passwords," IEEE Security & Privacy, vol. 10, no. 1, pp. 28–36, 2012.

[2] **D. E. Denning and P. F. MacDoran**, "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, vol. 1996, no. 2, pp. 12–16, 1996.

[3] **P. Eckersley**, "How unique is your web browser?" in Privacy Enhancing Technologies Symposium (PETS). Springer pp. 1–18, 2010

[4] **H. Khan, A. Atwater, and U. Hengartner**, "A comparative evaluation of implicit authentication schemes," in RAID. Springer, pp. 255–275, 2014.

[5] **Freeman, D. Dürmuth, M. Biggio, Battista**, Who are you? A statistical approach to measuring user authenticity. Proc of NDSS, 1-15, 2016.

[6] **Florencio, Dinei Herley, Cormac**, A large-scale study of web password habits. 16th International World Wide Web Conference, 657-666, 2007.

[7] **Khan, Hassan Hengartner, Urs Vogel, Daniel**, Targeted Mimicry Attacks on Touch Input Based, Implicit Authentication Schemes. 387-398, 2016.

[8] **C. Bo, L. Zhang, X.-Y. Li, Q. Huang, and Y. Wang**, Silentsense: silent user identification via touch and movement behavioral biometrics. In 19th Annual International Conference on Mobile Computing & Networking. ACM, 2013.

[9] https://sozluk.gov.tr/. Son erişim 12/7/2020

[10] https://www.collinsdictionary.com/dictionary/french-english/chiffrer/. Son erişim 12/7/2020

[11] https://translate.google.com/#view=home&op=translate&sl=fr&tl=en&text=chiffrer Son erişim 12/7/2020

[12] **Z. Dong, R. D. Perera, R. Chandramouli, and K. Subbalakshmi**, "Network measurement based modeling and optimization for IP geolocation," Computer Networks, vol. 56, no. 1, pp. 85–98, 2012

[13] **Wiefling, Stephan Lo Iacono, Luigi Dürmuth, Markus**, Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild, 2019 .

[14] **Siadati H. and Memon N.**, Detecting structurally anomalous logins within enterprise networks. In CCS 2017 - Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1273-1284, 2017.

[15] **E. Shi, Y. Niu, M. Jakobsson, and R. Chow**, Implicit authentication through learning user behavior. In Information Security. Springer, 2011.

[16] **Solano J., Camacho L., Correa A., Deiro C., Vargas J., Ochoa M**, Risk-Based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics. In: Zhou J. et al. (eds) Applied Cryptography and Network Security Workshops, ACNS, vol 11605, 2019

[17] **M. Jakobsson, E. Shi, and R. Chow** "Implicit authentication for mobile devices," in 4th USENIX Workshop on Hot Topics in Security (HotSec '09), Montreal, Canada, 2009.

[18] **A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann**, Touch me once and I know it's you!: Implicit authentication based on touch screen patterns. In Annual Conference on Human Factors in Computing Systems. ACM, 2012.

[19] **A. Adams and M. A. Sasse**, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, 1999

[20] **B. Draffin, J. Zhu, and J. Zhang**, Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction. In Mobile Computing, Applications, and Services. Springer, 2014.

[21] **M. Shahzad, A. X. Liu, and A. Samuel**, Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In 19th Annual International Conference on Mobile Computing & Networking. ACM, 2013.

[22] **Joseph Bonneau**, Authentication is machine learning. https://www.lightbluetouchpaper.org/2012/12/14/authentication-is-machine - learning/. Son erişim 03/19/2020.

[23] **M. Hearn**, An update on our war against account hijackers. Google Security Team Blog, Feb 2013. Son erişim 03/19/2020.

[24] https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html/. Son erişim 6/30/2020.

[25] **M. V. Wilkes**, Time-sharing computer systems. New York

[26] **W.H. Gates III**, Keynote Presentation, RSA Conference, 2004.

[27] **Cormac Herley, P.C. van Oorschot, and Andrew S. Patrick**, Passwords: If We're So Smart, Why Are We Still Using Them? In FC '09: The 13th International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2009. Springer-Verlag Elsevier, 1968.

[28] **R. Morris and K. Thompson**, Password security: a case history. Commun. ACM, 22(11):594–597, 1979.

[29] https://github.com/ivan-homoliak-sutd/twos/. Son erişim 12/7/2020

[30] http://www.openwall.com/john/. Son erişim 12/7/2020

[31] The Internet Worm's dictionary attack is described in **Eugene Spafford**'s article "Crisis and Aftermath", Communications of the ACM vol. 32, no. 6, 1989.

[32] **Philippe Oechslin**, Making a Faster Cryptanalytic Time-Memory Trade-Off . Advances in Cryptology - CRYPTO 2003, 2003.

[33] **D. Klein**, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," in Proceedings of the 2nd USENIX Security Workshop, pp. 5–14, 1990.

[34] **Alma Whitten and J. D. Tygar**, Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99). USENIX Association, USA, 14, 1999.

[35] **B. Schneier**, Secrets and Lies: Digital Security in a Networked World. John Wiley and Sons, 2000.

[36] **Cranor, Lorrie**, A Framework for Reasoning About the Human in the Loop. Proceedings of the 1st Conference on Usability, Psychology, and Security, 2008.

[37] **Sunshine, Joshua Egelman, Serge Almuhimedi, Hazim Atri, Neha Cranor**, Lorrie, Crying Wolf: An Empirical Study of SSL Warning Effectiveness. 399-416, 2009.

[38] **C. E. Shannon**, "A mathematical theory of communication. Bell System Tech. J., Vol. 27, July, October, 1948

ÖZGEÇMİŞ

Ad-Soyad : Oğuzhan Salman

Uyruğu : TC

Doğum Tarihi ve Yeri : 01-01-1990, İskenderun

E-posta : osalman@etu.edu.tr

ÖĞRENİM DURUMU:

• **Lisans** : 2016, Bilkent Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği

• **Yüksek Lisans** : 2020, TOBB ETÜ, Mühendislik Fakültesi, Bilgisayar Mühendisliği

MESLEKİ DENEYİM:

Yıl	**Yer**	**Görev**
2018-2020	TÜBİTAK	Araştırma Görevlisi
2016-2018	Cybersoft	Fullstack Developer

Ödüller ve Sertifikalar:

- Tübitak Antalya Fizik Olimpiyatları Hasan Çolak Anadolu Lisesi Katılımcısı
- 2003 Türkiye Satranç Federasyonu Alanya Satranç Turnuvası Birinciliği
- 2004 Antalya Kolejler Satranç Turnuvası Birinciliği
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms - Stanford Online
  https://coursera.org/share/cd42296cc3643978dc25378d38c93222

- Crytography I - Stanford Online
  Link: https://coursera.org/share/55ac4035111a3456cc74b6850f52719d

- Introduction to TensorFlow for Artificial Intelligence, Machine Learning, and Deep Learning - deeplearning.ai
  Link: https://coursera.org/share/88d9318ed8b8d524244b9fbdc1b9e033

- Deep Learning Specialization - deeplearning.ai
  Kurs 1: Neural Networks and Deep Learning
  Kurs 2: Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization
  Kurs 3: Structuring Machine Learning Projects
  Kurs 4: Convolutional Neural Networks
  Kurs 5: Sequence Models
  Link: https://coursera.org/share/2ba1e4524e2ccc151967aaf1d0c08c08

- Mathematics for Machine Learning Specialization - Imperial College London
  Kurs 1: Mathematics for Machine Learning: Linear Algebra
  Kurs 2: Mathematics for Machine Learning: Multivariate Calculus
  Kurs 3: Mathematics for Machine Learning: PCA
  Link: https://coursera.org/share/5ba6b0972095e0ddab95dde93e0b387b

- Pluralsight.com'dan Alınan Sertifikalar
  - Ethical Hacking - Level: Expert (Score: 231, 92nd Percentile)
  - Web Application Security - Level: Expert (Score: 229, 91st Percentile)
  - Javascript Core Language - Level: Expert (Score: 202, 81st Percentile)
  - Node.js - Level: Expert (Score: 240, 94th Percentile)
  - C# Coding Practices - Level: Expert (Score: 203, 82nd Percentile)
  - C# - Level: Proficient (Score: 191, 75th Percentile)
  - Network Forensics - Level: Proficient (Score: 115, 28th percentile)

  Tüm Kurslar ve Sertifikalar:
  https://app.pluralsight.com/profile/oguzhan-salman-9c

YABANCI DİL: İngilizce(İleri), Fransızca(İyi)

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Bıcakci, K., Salman, O, Uzunay, Y., Tan, M.**, 2020. Analysis and Evaluation of Keystroke Dynamics as a Feature of Contextual Authentication: ISCTURKEY - Anatolian Crypt 2020, Information Security and Cryptography Conference