T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Nebil Vural GÜNDOĞAN

TUŞ VURUŞLARINA DAYALI KİMLİK DOĞRULAMA YÖNTEMLERİ: EVRİMİ, ZORLUKLARI VE GELECEK YÖNELİMLERİNİN KAPSAMLI BİR İNCELEMESİ

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Eylül 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Nebil Vural GÜNDOĞAN
(23SIBE5005)

TUŞ VURUŞLARINA DAYALI KİMLİK DOĞRULAMA YÖNTEMLERİ: EVRİMİ, ZORLUKLARI VE GELECEK YÖNELİMLERİNİN KAPSAMLI BİR İNCELEMESİ

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Eylül 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Nebil Vural GÜNDOĞAN
(23SIBE5005)

TUŞ VURUŞLARINA DAYALI KİMLİK DOĞRULAMA YÖNTEMLERİ: EVRİMİ, ZORLUKLARI VE GELECEK YÖNELİMLERİNİN KAPSAMLI BİR İNCELEMESİ

Tezin Savunulduğu Tarih: 23.09.2025

Tez Danışmanı: Dr. Öğr. Üyesi Barış ÇELİKTAŞ / Işık Üniversitesi

Diğer Jüri Üyeleri: Dr. Öğr. Üyesi Ahmet Feyzi ATEŞ / Işık Üniversitesi

Dr. Öğr. Üyesi Fatih UYSAL / Kafkas Üniversitesi

İSTANBUL, Eylül 2025

ÖZET

TUŞ VURUŞLARINA DAYALI KİMLİK DOĞRULAMA YÖNTEMLERİ: EVRİMİ, ZORLUKLARI VE GELECEK YÖNELİMLERİNİN KAPSAMLI BİR İNCELEMESİ

Tuş vuruşu (keystroke) ile kimlik doğrulama, bireylerin klavye kullanımındaki yazım ritimlerini ve zamanlama desenlerini analiz ederek kimlik doğruluğunu sağlayan sofistike bir davranışsal biyometrik yöntemdir. Bu yöntemin dikkat çekici avantajları arasında, kullanıcıdan ek bir işlem gerektirmemesi, herhangi bir ek donanım ihtiyacı doğurmaması ve maliyet etkinliği bulunmaktadır. Gelişmiş bilişim altyapılarında ve güvenlik hassasiyeti yüksek uygulamalarda, kullanıcıyı tanımak için sürekli izleme ve ikinci faktör doğrulama gerekliliği artarken, tuş vuruşu temelli yöntemler bu gereksinimlere düşük maliyetli ve sezgisel bir çözüm sunmaktadır. Bu çalışma, tuş vuruşu dinamik kimlik doğrulama yöntemleri ile ilgili literatürü sistematik olarak incelemektedir. İlk olarak, farklı setler ve özellikleri gözden geçirilmekte, ardından makine öğrenimi (ML), derin öğrenme (DL) ve hibrit modeller performans, güvenlik ve kullanılabilirlik açısından karşılaştırılmaktadır. Ayrıca, mevcut metodolojiler OWASP Kimlik Doğrulama Hile Sayfası aracılığıyla sunulan kılavuz bağlamında ele alınarak, güvenlik açıkları ve olası saldırılar analiz edilmektedir. Hibrit modellerin, daha yüksek doğruluk ve üstün dayanıklılık açısından otonom ML veya DL yöntemlerinden daha iyi performans gösterdiği ortaya çıkmaktadır. Gelecekteki yönelimler açısından, federatif öğrenme (FL), açıklanabilir yapay zekâ (XAI) ve multimodal biyometrik füzyon, gizlilik, açıklana bilirlik ve platformlar arasında genelleştirile bilirlik açısından daha sağlam çözümler üretme konusunda umut vaat etmektedir. Değerlendirme kapsamında, söz konusu modellerin masaüstü sistemlerde, web tabanlı platformlarda ve mobil cihazlarda sergilediği performanslar karşılaştırmalı olarak analiz edilmiştir. Elde edilen veriler, bazı modellerin

yüksek doğruluk oranlarına ulaştığını ancak kullanıcı deneyiminde sürtünme (friction) oluşturduğunu; diğer modellerin ise kullanıcı dostu yapısına karşın daha düşük güvenlik sunduğunu ortaya koymaktadır. Bu bağlamda, sistem seçiminde güvenlik, doğruluk ve kullanıcı konforu arasında bir denge kurulması gerektiği sonucuna varılmıştır. Bu bağlamda önerdiğimiz hibrit doğrulama çerçevesi, derin sinir ağlarının sınıflandırma yeteneklerini anomali tespit teknikleriyle birleştirmekte ve bağlamsal farkındalığa sahip özellik çıkarımı ile uyarlanabilir eşikleme mekanizmaları kullanmaktadır. Böylelikle, modelimiz hem yeni kullanıcı davranışlarına uyum sağlayabilmekte hem de sahtecilik girişimlerine karşı yüksek hassasiyetle yanıt verebilmektedir. Ayrıca, önerilen çerçevenin farklı kullanım bağlamlarında—örneğin sürekli oturum denetimi veya ikinci faktör doğrulama senaryolarında—uygulanabilirliği değerlendirildiğinde, sistemin ölçeklenebilirliği ve uygulama kolaylığı da ön plana çıkmaktadır. Sonuç olarak, elde edilen bulgular, tuş vuruşu doğrulama sistemlerinin, özellikle diğer biyometrik yöntemlerle bütünleştiğinde veya bağlamsal verilerle desteklendiğinde, yüksek güvenlik gerektiren uygulamalarda etkin, uyarlanabilir ve kullanıcı dostu bir çözüm sunduğunu göstermektedir. Çalışma sadece literatürde bulunan yöntemlerin kapsamlı bir karşılaştırmasını yapmakla kalmayıp, aynı zamanda gelecekteki çalışmalarda metodolojik seçimler için bir kılavuz da çizmektedir.

Anahtar Kelimeler: Tuş Vuruşu Doğrulama, Davranışsal Biyometri, Makine Öğrenimi, Derin Öğrenme Kullanıcı Doğrulama Sistemleri

ABSTRACT

KEYSTROKE DYNAMİCS-BASED AUTHENTİCATİON METHODS: A COMPREHENSİVE REVİEW OF THEİR EVOLUTİON, CHALLENGES, AND FUTURE DİRECTİONS

Keystroke authentication is a sophisticated behavior biometric method that verifies users in accordance with individuals 'typing timing and rhythm patterns while interactingwiththe keyboard. The majör advantages of this technology include that there are no additional user actions needed, no specialized hardware demands,and it is inexpensive. With increasing demand for second-factor authentication and ongoing user monitoring in sophisticated computing systems and high-security solutions,keystroke based systems are introduced as a natural and inexpensive option to fulfill these requirements.This study performs a systematic survey of the literature on keystroke dynamic authentication methods. First, different sets and their features are reviewed, then machine learning (ML), deep learning (DL), and hybrid models are compared relative to their performance, security, and usability. Further, the present methodologies are placed in the context of the guidance offered through the OWASP Authentication Cheat Sheet, presenting an analysis of vulnerabilities and possible attacks. It turns out that the hybrid models outperform autonomous ML or DL methods in returning improved accuracy and superior resilience. As far as future directions are concerned, federated learning (FL), explainable artificial intelligence (XAI), and multimodal biometrics fusion are promising to produce more robust solutions relative to privacy, explainability, and generalizability across platforms. To this end, we propose a hybrid authentication framework that fuses the classification capabilities of deep neural networks with anomaly detection methods, through context-aware feature extraction and adaptive thresholding mechanisms. Our system can learn and adjust to changing user habits and react with high sensitivity to spoofing behavior. In addition, when

evaluated over a range of application scenarios—from continuous session verification to second-factor authentication this framework demonstrates high scalability and feasibility in practice. As a conclusion, the results show that keystroke authentication systems, and particularly when combined with other biometric techniques or augmented with contextual information, provide a secure, versatile, and user-acceptable solution for security-sensitive applications. These study not only attempts a comprehensive comparison of methods available in literature but also draws a guideline for methodological selections in future studies.

Keywords: Keystroke Authentication, Behavioral Biometrics, Machine Learning, Deep Learning

TEŞEKKÜR

Bu yüksek lisans tezinin hazırlanmasında rehberlikleriyle katkı sağlayan tez danışmanım Dr. Öğr. Üyesi Barış ÇELİKTAŞ'a en içten teşekkürlerimi sunarım. Akademik bakış açısı ve motive edici yönlendirmeleri ile çalışmamın her aşamasında desteğini esirgememiştir. Çalışmanın değerlendirmesinde desteklerini eksik etmeyen, Dr. Öğr. Üyesi Ahmet Fevzi ATEŞ ve Dr. Öğr. Üyesi Fatih UYSAL'a. Bu çalışmanın her aşamasında motivasyonumu yüksek tutmama sebep olan ve siber güvenlik programında birlikte fikir alış verişinde olduğum değerli bölüm arkadaşlarım Serhat TAŞ, Serhan GÜNER, Erdem ULUTAŞ, Eyüpcan KILIÇ ve Burak KUBİLAY'a. Son olarak tezli yüksek lisans programına başvurmam için beni cesaretlendiren değerli eşim Nadiye YILDIZ GÜNDOĞAN'a ve akademik yolculuğum boyunca beni koşulsuz şartsız destekleyen Kızım Atlas Rüzgar, Oğlularım Demir Deniz ve Toprak Çınar'a en içten teşekkürlerimi sunarım.

Nebil Vural GÜNDOĞAN

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

KD : Tuş Vuruş Dinamikleri (Keystroke Dynamics).

EER : Eşit Hata Oranı (Equal Error Rate).

FAR : Yanlış Kabul Oranı (False Acceptance Rate)..

FRR : Yanlış Reddetme Oranı (False Rejection Rate).

MLP : Çok Katmanlı Algılayıcı (Multi-Layer Perceptron).

LSTM: Uzun Kısa Süreli Bellek (Long Short-Term Memory).

CNN : Evrişimsel Sinir Ağı (Convolutional Neural Network).

1D CNN: Tek Boyutlu Evrişimsel Sinir Ağı (One-Dimensional Convolutional Neural Network).

SVM : Destek Vektör Makinesi (Support Vector Machine).

HMI : İnsan-Makine Etkileşimleri (Human-Machine Interactions).

OTP : Tek Kullanımlık Şifre (One-Time Password).

MFA : Çok Faktörlü Kimlik Doğrulama (Multi-Factor Authentication).

2FA : İki Faktörlü Kimlik Doğrulama (Two-Factor Authentication).

PIN : Kişisel Kimlik Numarası (Personal Identification Number).

KLM : Tuş Vuruş Seviyesi Modeli (Keystroke-Level Model).

GOMS : Hedefler Operatörler Yöntemler Seçim (Goals Operators Methods Selection).

KLM Temel Operatör Kısaltmaları:

R : Sistem Yanıtı (System Response).

RP : Bırakma-Basma Gecikmesi (Release-Press Latency).

PP : Basma-Basma Gecikmesi (Press-Press Latency).

RR : Bırakma-Bırakma Gecikmesi (Release-Release Latency).

PR : Basma-Bırakma Gecikmesi (Press-Release Latency).

HT : Basılı Tutma Süresi (Hold Time).

BÖLÜM 1

1. GİRİŞ

Geleneksel kimlik doğrulama yöntemleri, özellikle parolalar, uzun süredir bilgisayar sistemlerinin güvenliğini sağlamak amacıyla kullanılmaktadır. Ancak bu yöntemler, kaba kuvvet saldırıları (brute-force), kimlik bilgisi doldurma (credential stuffing) ve oltalama (phishing) gibi saldırılara karşı savunmasız olmaları nedeniyle ciddi güvenlik sorunları taşımaktadır. Bu sorunlar doğrultusunda, davranışsal biyometri tabanlı yöntemler —özellikle tuş vuruş dinamikleri (keystroke dynamics)— güvenliği artıran, maliyet açısından uygun alternatifler olarak öne çıkmaktadır. (Marina Zamsheva vd. 2020)

Tuş vuruş dinamikleri, kullanıcının yazma davranışlarını (örneğin, tuş basma süresi, uçuş süresi ve yazma hızı) analiz ederek, kişiye özel tanımlayıcı özellikleri ortaya koyar. Bu tür davranışsal özellikler, zaman içinde çeşitli makine öğrenmesi ve derin öğrenme teknikleri kullanılarak meşru kullanıcılar ile sahte kullanıcıları ayırt edebilecek doğrulama sistemlerinin geliştirilmesini sağlamıştır. (Ula Tarik Salim vd. 2023) (Erhan Yılmaz vd. 2023). Literatürde çok sayıda tuş vuruşu dinamiği çalışması bulunmasına rağmen, kullanılan veri setleri nedeniyle bu çalışmaların çoğu orantısız ve kolayca karşılaştırılamayan sonuçlar vermektedir. Örneğin, çevresel faktörler (örneğin, deneklerin çalıştığı çalışma ortamı, stres seviyesi) ve ekipman değişkenliği (farklı klavye modelleri, masaüstü bilgisayar ile mobil cihaz arasındaki farklar) veri setlerini tutarsız hale getirmektedir. (Wang, Wu ve ark., 2019). Son yıllarda, daha büyük ve daha eksiksiz veri setlerinin artan kullanılabilirliği, bu tür dengesizliklerin önemli ölçüde azalmasına neden olmuştur. Doğrudan olarak, veri kalitesindeki iyileşme, makine öğrenimi (ML) ve derin öğrenme (DL) modellerinin daha olumlu çıktılar üretmesini mümkün kılmıştır. (Wahab , Hou ve ark., 2025) Ayrıca, DL tabanlı metodolojilerin ve anomali tespit metodolojilerinin uygulanmasına yönelik metodolojilerin birleştirilmesi ve ensemble tabanlı metodolojilerin

kullanılmasına yönelik metodolojilerin birleştirilmesi, çeşitli kullanım uygulamalarında Eşit Hata Oranı (EER) ve sağlamlığın en aza indirilmesinde belirgin ilerlemelerle sonuçlanmıştır (Kim, Lee, , Shin ve ark., 2020; Wahab, Hou, Schuckers ve diğerleri, 2025).

Bu çalışma, tuş vuruş doğrulama sistemlerinde kullanılan makine öğrenmesi algoritmalarını (k-En Yakın Komşu, Destek Vektör Makineleri ve Rastgele Ormanlar) derin öğrenme modelleriyle karşılaştırmalı olarak analiz etmektedir. Özellikle Konvolüsyonel Sinir Ağları (CNN), Tekrarlayan Sinir Ağları (RNN) ve bunların melez modelleri gibi derin öğrenme teknikleri, ham zaman serisi verilerinden yüksek seviyeli zamansal ve mekânsal özellikleri otomatik olarak çıkarma kapasiteleri nedeniyle avantaj sağlamaktadır. (Sebastián Sznur vd. 2008) (Ula Tarik Salim vd. 2023) (Erhan Yılmaz vd. 2023)

CNN temelli mimariler yerel zamanlama örüntülerini etkili bir biçimde yakalayabilirken, RNN ve Uzun Kısa Süreli Bellek (LSTM) ağları sıralı bağımlılıkları ve yazma davranışına özgü uzun menzilli bağlamsal kalıpları modelleyebilir. (Ula Tarik Salim vd. 2023) Ayrıca, dikkat mekanizmaları (attention) ve artık bağlantılar (residual connections) gibi çağdaş mimari yaklaşımlar, modelin eğitimi sırasında daha hızlı yakınsamayı sağlarken, sınıf içi değişkenlik ve çevresel gürültüye karşı dayanıklılığı da artırmaktadır. (Ula Tarik Salim vd. 2023) (Sebastián Sznur vd. 2008)

Bu çok katmanlı analiz, farklı modellerin tuş vuruş biyometrik sinyallerinin doğrusal olmayan, değişken ve oturum bağımlı doğasına nasıl yaklaştığını değerlendirmeye olanak tanımaktadır. Bulgular, yeterli çeşitlilik ve hacimde tuş vuruş verisiyle eğitilen derin öğrenme modellerinin, geleneksel elle mühendislik gerektiren özellik çıkarımı temelli yöntemlere kıyasla daha yüksek doğruluk, daha düşük Eşit Hata Oranı (EER) ve daha iyi genelleme başarısı sağladığını ortaya koymaktadır. (Erhan Yılmaz vd. 2023) (Sebastián Sznur vd. 2008)

Bu araştırma, kimlik doğrulama metodlarına uygun modelin doğruluğu ve uygulamalar arasındaki çok yönlülüğü ile ilgili soruları ele alarak tuş vuruş biyometrisi alanına önemli katkılarda bulunmaktadır. Derin öğrenme

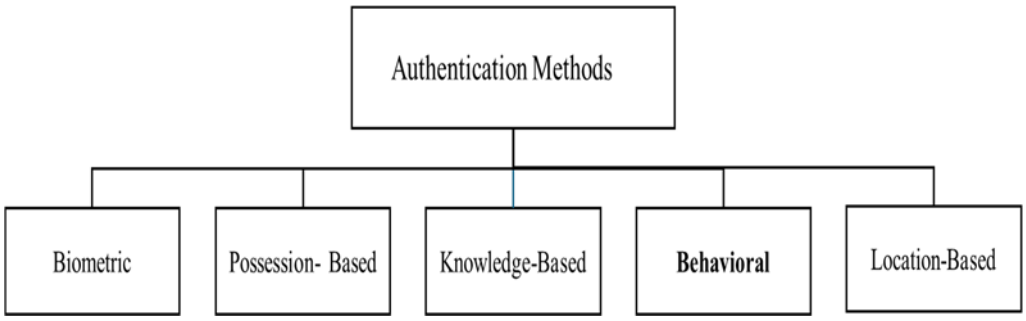
mekanizmaları ile geleneksel makine öğrenimi teknikleri arasındaki içsel yapısal farklılıkların analizi yoluyla, farklı uygulama senaryoları için en uygun model türlerinin belirlenmesine yönelik kapsamlı bir rehber sunmaktadır. Sonuç olarak, yapay zekâ destekli kimlik doğrulama sistemlerinin belirli güvenlik gereksinimlerini karşılama kapasitesi artmakta; böylece, yapay zekâ tabanlı güvenlik önlemlerinin çok amaçlı ve esnek bir biçimde uygulanabilmesi mümkün hâle gelmektedir.

BÖLÜM 2

2. LİTERATÜR

2.1 KİMLİK DOĞRULAMA YÖNTEMLERİNE GENEL BAKIŞ

Çeşitli güvenlik faktörlerine göre sınıflandırılmış farklı kimlik doğrulama yöntemleri Şekil 2.1'de belirtilmiştir.



Şekil 2.1 Doğrulama Yöntemleri

Biyometrik Kimlik Doğrulama: Parmak izi (dermatoglifik), yüz tanıma veya iris tarama gibi benzersiz fizyolojik ya da davranışsal özellikleri kullanarak kimlik doğrulama yapar. Güvenli bir yöntemdir ancak gizlilikle ilgili endişelere yol açabilir. (Soumen Roy vd. 2022)

Nesne Tabanlı Kimlik Doğrulama: Akıllı kartlar, güvenlik anahtarları veya mobil kimlik doğrulayıcı cihazlar gibi fiziksel cihazlara dayanır. Kullanışlı bir özellik olmasına rağmen, bu cihazların kaybolması ya da çalınması durumunda güvenlik riski taşır. (Soumen Roy vd. 2022)

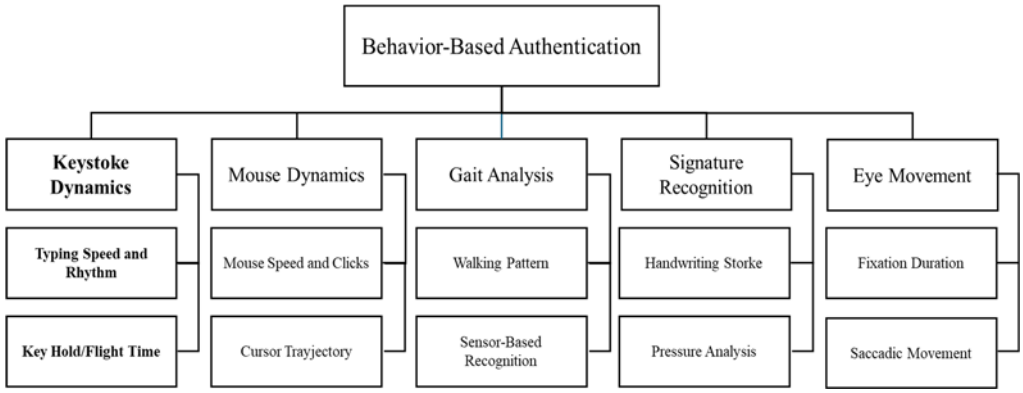
Bilgi Tabanlı Kimlik Doğrulama: Kullanıcılardan şifre veya PIN gibi belirli bilgileri hatırlamaları istenir. Bu yöntem yaygın olarak kullanılmakla birlikte oltalama (phishing) saldırıları ve şifre güvenliği ihlalleri açısından oldukça hassastır. (Soumen Roy vd. 2022)

Davranışsal Kimlik Doğrulama: Kullanıcının klavye yazma ritmi, göz hareketleri, fare kullanımı ya da yürüyüş biçimi gibi etkileşim desenlerini analiz eder. Sürekli kimlik doğrulama sağlar ve kullanıcıdan özel bir eylem gerektirmeksizin güvenliği artırır. (Soumen Roy vd. 2022)

Konum Tabanlı Kimlik Doğrulama: Kimlik doğrulama amacıyla coğrafi konum bilgilerini kullanır ve genellikle güvenliği artırmak amacıyla diğer doğrulama faktörleriyle birlikte çalışır. Geleneksel kimlik doğrulama yöntemlerinden farklı olarak, davranışsal doğrulama uyarlanabilir ve pasif bir yapıya sahiptir. Gerçek zamanlı kullanıcı davranışı analiziyle kimlik doğrulama sürtünmesini azaltırken, kimlik bilgilerini hırsızlık ve yetkisiz kullanıma karşı korur. (Soumen Roy vd. 2022)

2.1.1 Davranışsal Kimlik Doğrulama Taksonomisi

Şekil 2.2 , davranış temelli kimlik doğrulama tekniklerini, biyometrik ve biyometrik olmayan davranışsal özniteliklere göre yapılandırılmış biçimde sınıflandırmaktadır:



Şekil 2.2 Davranışsal Kimlik Doğrulama Taksonomisi

Tuş Vuruş Dinamikleri: Kişilerin yazma biçimlerini —yani yazma hızı, ritmi, tuşa basma ve bırakma süresi gibi— analiz eder. Genellikle pasif bir doğrulama yöntemi olarak kullanılır.

Fare Dinamikleri: Kullanıcının imleç hareketi, tıklama oranı ve imleç yörüngesi gibi davranışsal kalıplarını inceler; bireysel davranışı ayırt etmeye yönelik analizlerde kullanılır.

Yürüyüş Analizi: Hareket sensörlerinden elde edilen veriler aracılığıyla bireylerin yürüme biçimlerini ve adım düzenlerini analiz ederek kimliklerini belirlemeye çalışır.

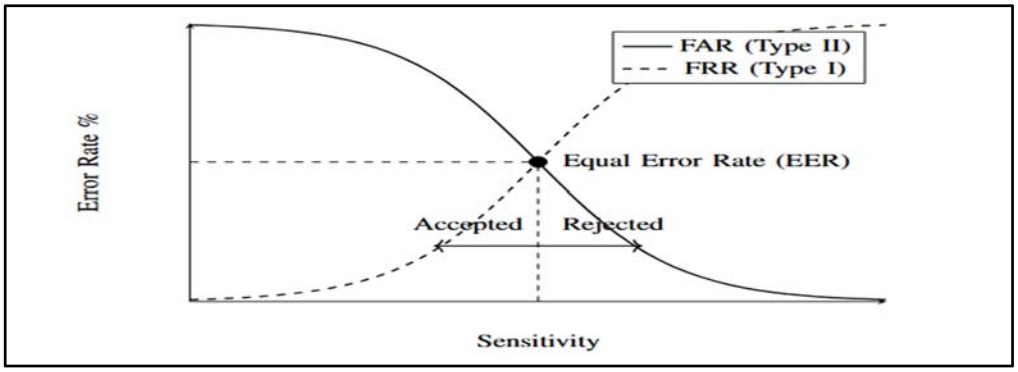
İmza Tanıma: Kullanıcının el yazısı imzasına ait vuruş dinamikleri, basınç dağılımı ve yazma hızı gibi özellikleri değerlendirerek kimliğini belirler.

Göz Hareketi Takibi: Sabit bakış süresi ve sakkadik hareketler gibi açık davranışsal öznitelikleri kaydeder. Genellikle askeri ya da sağlık sistemleri gibi yüksek güvenlik gerektiren ortamlarda kullanılır.

Davranışsal kimlik doğrulama, pasiflik, süreklilik ve doğrulama kolaylığı gibi avantajlar sunar; ayrıca statik doğrulama tekniklerine (ör. şifre) olan bağımlılığı azaltır. Bununla birlikte, çevresel koşullar (ör. göz takibi için ışık), cihaz bağımlılığı (ör. yürüyüş analizinde kullanılan sensörler) ve davranışsal öznitelikleri taklit etmeye çalışan uyarlanabilir saldırganlara karşı korunma gibi çeşitli zorlukları da beraberinde getirir. (Soumen Roy vd. 2022)

2.1.2 FAR-FRR Eğrisi Analizi

Şekil 2.3, biyometrik kimlik doğrulama teknolojilerinde Sahte Kabul Oranı (FAR) ile Sahte Reddetme Oranı (FRR) arasındaki ilişkiyi göstermektedir:



Şekil 2.3 FAR-FRR Eğrisi Analizi

FAR (Type II Error): Düz çizgi, yetkisiz bir kişinin yanlışlıkla sisteme kabul edilme olasılığını ifade eder. Sistem duyarlılığı arttıkça, FAR değeri düşer.

FRR (Type I Error): Kesikli çizgi, yetkili bir kullanıcının hatalı şekilde reddedilme olasılığını temsil eder. Duyarlılık arttıkça, FRR de azalır.

Eşit Hata Oranı (EER): FAR ve FRR'nin kesişim noktasıdır ve her iki hata oranının eşit olduğu eşiği temsil eder. Düşük EER, daha dengeli ve güvenilir bir kimlik doğrulama sistemini ifade eder.

Kabul ve Red Bölgeleri: EER noktasının altındaki yatay ok, karar verme süreçleri açısından güvenlik (düşük FAR) ile kullanılabilirlik (düşük FRR) arasında bir denge kurmayı temsil eder.

Sistem için en uygun duyarlılık düzeyi, özel güvenlik gereksinimlerine bağlıdır. Eğer öncelik güvenlikse, FAR'ın düşürülmesi esastır; kullanıcı dostu uygulamalarda ise FRR'nin azaltılması daha yararlıdır.

İdeal bir sistemin %0 FAR ve %100 Gerçek Kabul Oranı (TAR - True Acceptance Rate) olması beklenir. Ancak, güvenlik (düşük FAR) ve kullanışlılık (yüksek TAR/düşük FRR) arasında her zaman bir denge (trade-off) vardır. Tercih edilen çalışma noktası, uygulamanın güvenlik mi yoksa kullanışlılık mı lehine olacağına bağlıdır.

Hesaplama Nasıl Yapılır.

FAR, FRR ve diğer performans metriklerinin hesaplanması için temel bileşenleri tanımlar:

Gerçek Kabul (TA - True Acceptance): Gerçek kullanıcının doğru şekilde meşru olarak sınıflandırılması.

Gerçek Reddetme (TR - True Reject): Sahte kullanıcının doğru şekilde sahte olarak sınıflandırılması.

Yanlış Kabul (FA - False Acceptance): Sahte kullanıcının yanlışlıkla meşru olarak sınıflandırılması.

Yanlış Reddetme (FR - False Reject): Gerçek kullanıcının yanlışlıkla sahte olarak sınıflandırılması.

Bu tanımlara dayanarak, kaynaklar aşağıdaki formülleri sağlar:

Gerçek Kabul Oranı (TAR): TA / (TA + FR) (Kaynaklardan biri, TAR'ı meşru kullanıcıların hesabına erişim izni verilen yüzdesi olarak tanımlar).

Gerçek Reddetme Oranı (TRR): TR / (TR + FA)

Yanlış Kabul Oranı (FAR): FA / (FA + TR) veya Yanlış Kabul Testlerinin Sayısı / Toplam Test Sayısı (%)

Yanlış Reddetme Oranı (FRR): FR / (FR + TA) veya Yanlış Reddetme Testlerinin Sayısı / Toplam Test Sayısı (%)

EER ise, sistemin eşiğini ayarlayarak FAR ve FRR'nin eşitlendiği noktada bulunur.

2.1.3 Kullanım Senaryoları: FAR veya FRR'nin Daha Önemli Olduğu Durumlar

FAR ile FRR arasında optimum denge, kimlik doğrulama sisteminin kullanılabilirlik ve güvenlik gereksinimlerine bağlıdır. Farklı uygulama alanlarının farklı öncelikleri vardır:

Kamu, finans ve askeri kimlik doğrulama sistemlerinde, yetkisiz erişimi sınırlandırmak kritik önemdedir. Bu tür senaryolarda FAR'ın minimize edilmesi gereklidir, bu da FRR'nin artması pahasına olabilir. Örneğin, askeri veritabanlarında güçlü erişim kontrolü gereklidir. Yanlış kabul (false acceptance), yetkisiz erişime neden olabilir ve bu nedenle güvenlik birincil önceliktir. Kullanıcılar daha fazla reddedilme (yüksek FRR) ile karşılaşabilir ve bu da tekrarlı kimlik doğrulama denemeleri veya alternatif doğrulama yöntemleri gerektirebilir.

Kullanıcı dostu uygulamalarda, örneğin tüketici elektroniği ve çevrim içi hizmet sağlayıcılarında, amaç kullanıcı deneyimini geliştirmek için yanlış reddetmeleri (FRR) azaltmaktır. Cep telefonlarında yüz tanıma gibi sistemlerde FRR'nin düşük tutulması, kullanıcıların cihazlarına erişimlerinin engellenmemesi açısından ön plandadır. FAR hâlâ bir sorun olabilir; ancak tekrar eden başarısız doğrulama denemelerinin yol açtığı kullanıcı memnuniyetsizliği azaltılır. Daha kolay ve hızlı doğrulama karşılığında hafifçe artmış bir FAR kabul edilebilir.

Tıbbi kimlik doğrulama sistemlerinde, örneğin elektronik sağlık kayıtlarına (EHR) erişimde, hem hızlı hem de güvenli doğrulama sağlamak için güvenlik ile kullanılabilirlik dengelenmelidir. Bir hastanedeki doktor doğrulama sisteminin yetkisiz erişimi engellemesi (düşük FAR) ancak acil durumlarda hızlı erişim sağlaması (düşük FRR) gerekir. Bu bağlamda çok faktörlü kimlik doğrulama (MFA) veya acil durum erişim protokolleri gibi uyarlanabilir mekanizmalar değişken duyarlılık seviyelerine sahip olabilir.

Bu analiz, tüm durumlar için geçerli tek bir ideal duyarlılık ayarının olmadığını göstermektedir. Kimlik doğrulama sistemleri, bağlamsal gereksinimlere göre ayarlanabilir güvenlik parametreleriyle tasarlanmalıdır. (Marina Zamsheva vd. 2020) (Baljıt Sıngh Saini vd. 2020)

2.2 TUŞ VURUŞLARINA DAYALI KİMLİK DOĞRULAMA YÖNTEMLERİNİN EVRİMİ

Tuş vuruş dinamikleri, bir kişinin klavye üzerindeki yazma desenlerinin izlenmesine dayanan bir biyometrik değerlendirme türüdür; örneğin, bir tuşa basma süresi ve ardışık iki tuşa basma arasındaki süre gibi. Fizyolojik ve davranışsal yönlere dayanan diğer biyometrik tekniklere benzer şekilde, bu teknik hem kimlik doğrulama hem de kimlik tespiti yeteneğine sahiptir. Özellikle, standart klavyelerle yakalanabilmesi açısından maliyet etkinliği ve verimliliği ile dikkat çekmektedir.(Monrose & Rubin, 2000)

Bu konunun başlangıcı, kullanıcı verimliliği ve insan-bilgisayar etkileşimi (HCI) konularında yapılan keşif niteliğindeki çalışmalara dayanmaktadır. 1899 yılına kadar uzanan Bryan ve Harter'ın çalışması, telgrafın fizyolojik ve psikolojik yönlerini analiz etmiştir. Sonrasında, 1975 yılında IBM'den bir satış temsilcisi olan Spillane, bir dizi tuş düzeni kullanan bir tanımlama cihazı için patent almıştır. 1980'lerde, Card, Moran ve Newell'ın çalışmaları ile geliştirilen Tuş Vuruş Seviyesi Modeli (KLM), bir tuşa basma gibi düşük seviyeli operatörleri kullanarak etkileşimli sistemlerde görevleri tamamlama süresini ölçmek için temel bir yaklaşım sunmuştur. KLM, GOMS modeli (Amaçlar,

Operatörler, Yöntemler ve Seçim kuralları) gibi birçok bilişsel modelle bütünleştirilmiş ve görev analizinde faydalı olmuştur. Bu ilk araştırmalar doğrudan kimlik doğrulamayı hedeflememiş olsa da, yazım stratejileri ve zamanlamalarının akademik araştırmaları için temel oluşturmuştur. (Bryan & Harter, 1899; Spillane, 1975; Card, Moran, & Newell, 1983)

Tuş vuruş dinamiklerinin kimlik doğrulama amacıyla kullanımı, bir parola veya metin girme bağlamında zamansal veriler üzerine yapılan araştırmalardan doğmuştur. Gerçekten de, tuşa basma süresi ve tuşlar arası süre gibi zamansal faktörlerin, kişiye özgü olduğu ve taklit edilmesinin zor olduğu kanıtlanmıştır.(Monrose & Rubin, 1997; Bergadano et al., 2002)

Gelişim sürecinin başlarında, tuş vuruş dinamikleri genellikle "statik doğrulama" olarak adlandırılan modda çalışmaktaydı. Bu yaklaşım, yalnızca belirli bir anda—örneğin giriş sırasında—kimlik doğrulamasına izin verir. Kullanıcıların sabit bir metin (örneğin bir parola veya kişisel tanımlama numarası) yazarken sergilediği zamanlama desenleri bu paradigmanın içinde analiz edilir. Bu alandaki erken araştırmalar, digraf ve trigraf gecikmeleri gibi basit zamanlama parametrelerini, temel istatistiksel yöntemler veya sınıflandırma algoritmalarıyla (örneğin, Öklid mesafesi) birlikte kullanmıştır. Özel bir çalışmada, sayısal tuş takımlarından elde edilen verilerde Öklid mesafesi kullanılmış ve önemli hata oranları raporlanmıştır. (Joyce and Gupta (1990) and Leggett et al. (1991)

Cep telefonlarının evrimi, tuş vuruş dinamiklerinin mobil telefonlarda kullanılmasını mümkün kılmıştır. Erken dönem cep telefonlarında sayısal tuş takımları üzerinde yapılan araştırmalar, bu yöntemin cep telefonu kullanımı üzerinden kullanıcı kimlik doğrulamasında kullanılabilirliğini doğrulamıştır. Araştırmalar, mobil tuş takımlarında veri girmenin daha kısa gecikme süreleri ve daha yüksek doğruluk oranları sağladığını göstermiştir. (Clarke & Furnell, 2007)

Ancak statik doğrulamanın bazı sınırlamaları vardır. Giriş yaptıktan sonra veri giren kişinin değişmesini tespit edemez. Bu zayıflığın üstesinden gelmek için “dinamik” veya “sürekli doğrulama” olarak adlandırılan yöntemler

geliştirilmiştir. Sürekli doğrulamada, kullanıcının kimliği oturum boyunca doğrulanır; bu genellikle serbest metin yazma ritimlerine dayalı desenlerle yapılır. Bu yaklaşım, oturum ele geçirme ve benzeri güvenlik tehditlerini önlemeye yardımcı olabilir. (Ahmed & Traore, 2007)

Zamanla, hem çıkarılan özelliklerin karmaşıklığı hem de sınıflandırma algoritmaları önemli ölçüde gelişmiştir. İlk sistemler temel gecikme değerlerine odaklanırken, daha sonraki çalışmalar tuş basılı kalma süreleri, tuş basıncı ve 146'ya kadar özelliği içeren geniş ölçekli özellik setlerini dahil etmiştir. Ayrıca, en ayırt edici özellikleri izole etmek için özellik seçimi yöntemleri de geliştirilmiştir. (Killourhy & Maxion, 2009)

Sınıflandırma alanında ise geleneksel istatistiksel yöntemlerden, modern makine öğrenimi metodolojilerine geçiş yaşanmıştır. Bu yöntemler arasında en yakın komşu (k-NN), destek vektör makineleri (SVM), rastgele ormanlar (RF) ve sinir ağları (NN) gibi teknikler yer almaktadır. Bu alandaki son gelişmeler, evrişimli sinir ağları (CNN), yinelemeli sinir ağları (RNN), uzun-kısa süreli bellek (LSTM) ve Transformer tabanlı mimariler gibi derin öğrenme yapılarının tanıtılmasıyla gerçekleşmiştir. Örneğin, Çok Katmanlı Algılayıcı (MLP), CNN, LSTM ve TypeFormer gibi yeni Transformer tabanlı mimariler birçok doğrulama görevinde etkileyici doğruluk göstermiştir. (Giot et al., 2011; Acien et al., 2021)

Tuş vuruş dinamiklerinin uygulama alanı, orijinal kimlik doğrulama işlevinin çok ötesine geçmiştir. Bu konudaki araştırmalar artık kullanıcı tanımlama, yumuşak biyometrik özelliklerin (örneğin yaş ve cinsiyet) tahmini, stres gibi duygusal veya bilişsel durumların değerlendirilmesi, Parkinson gibi nöropsikiyatrik durumların belirtileri ve ana dil tespiti gibi konuları kapsamaktadır. Özellikle dil tanımlama bağlamında, serbest metin yazma verilerinin kullanımı, gerçek yazım davranışını daha yakından yansıtan sonuçlar elde edilmesini sağlamaktadır. (Gunetti & Picardi, 2005; Banerjee et al., 2012)

Modern teknolojiye—akıllı telefonlar ve dokunmatik ekranlar gibi—geçiş yeni zorluklar getirmiştir. Geleneksel fiziksel klavyelerin aksine, dokunmatik ekran etkileşimleri—örneğin dokunma süresi ve kaydırma hareketleri gibi—

farklı özellik kümeleri gerektirir ve parmak pozisyonu ile cihaz tutuş gibi faktörlerden etkilenir. Serbest metin girişindeki değişkenlik—duygusal durum veya yorgunluk düzeyi gibi içsel etkilerle ve kullanılan cihaz türü gibi dışsal etkilerle oluşan—sistem performansını etkileyen önemli bir zorluktur. Bu zorluğun üstesinden gelmek için uyarlanabilir modelleme ve gelişmiş özellik mühendisliği yöntemleri geliştirilmiştir. Bazı araştırmalar, çeşitli bağlamsal koşulları simüle etmek için adversarial gürültü örnekleri eklemiş ve böylece modellerin sağlamlığı artırılmıştır. (Acien et al. 2020)

Kamuya açık veri kümelerinin (örneğin CMU, GREYC, Aalto ve SUNY Buffalo) mevcudiyeti ve Keystroke Biometrics Ongoing Competition (KBOC) gibi yarışmaların düzenlenmesi, araştırma alanının gelişimini desteklemiş ve farklı yaklaşımların karşılaştırılmasına olanak sağlamıştır. (Killourhy & Maxion, 2009; KBOC, 2015)

Sonuç olarak, tuş vuruş dinamikleri kimlik doğrulama sistemleri, basit insan-bilgisayar etkileşimi modellerinden, derin öğrenme metodolojilerine dayanan modern çözümlere doğru evrilmiştir. Bu metodolojiler, statik doğrulamadan sürekli doğrulamaya, sabit metin testlerinden serbest metin testlerine ve geleneksel fiziksel klavyelerden dokunmatik ekranlara doğru gelişmiştir. Bu evrimin ana itici güçleri arasında artan güvenlik talepleri, kullanılan cihaz çeşitliliği, kullanıcı deneyimini iyileştirme gereksinimi ve makine öğrenimi ile derin öğrenme teknolojilerindeki ilerlemeler yer almaktadır. Bu yöntemler günümüzde yalnızca kimlik doğrulama için değil, aynı zamanda kullanıcı davranışlarını incelemek ve yumuşak biyometrik ya da bağlamsal özellikleri tahmin etmek için de büyük uygulanabilirliğe sahiptir. (Teh et al., 2013)

2.3 OWASP KİMLİK DOĞRULAMA KILAVUZUNDA TUŞ VURUŞU KİMLİK DOĞRULAMASI

Tuş vuruşu doğrulama, davranışsal biyometri kapsamında yer almakta olup OWASP Kimlik Doğrulama Kılavuzu'ndaki birçok güvenlik kontrolüyle uyumludur:

Katmanlı Güvenlik Yaklaşımı: OWASP, geleneksel parolaların artık yeterli olmadığını, davranışsal biyometrik verilerin ek bir koruma katmanı sunduğunu vurgulamaktadır.

Sürekli Kimlik Doğrulama: Parola tabanlı doğrulamanın aksine, tuş vuruşu dinamikleri kullanılarak oturum boyunca kullanıcı doğrulaması yapılabilir ve oturum ele geçirme saldırılarına karşı koruma sağlanır. (OWASP Authentication Term Sheet)

Saldırı Yüzeyinin Azaltılması: Tuş vuruşu doğrulama, tasarımı gereği, omuz üzerinden izleme (shoulder surfing) ve tekrar oynatma (replay) saldırılarına karşı geleneksel parolalara göre daha dayanıklıdır.

Kullanıcı kimlik doğrulaması, yalnızca yetkili kişilerin gizli bilgilere ve hizmetlere erişebilmesini sağlamak açısından modern siber güvenlik mekanizmalarının kritik bir bileşenidir. Parola ve jeton tabanlı geleneksel yöntemler uzun süredir kullanılmaktadır, ancak bu yaklaşımlar kaba kuvvet, oltalama, parola tekrar kullanımı ve sosyal mühendislik gibi tehditlere açıktır. Alternatif olarak, biyometrik kimlik doğrulama sistemleri; fiziksel ve davranışsal özellikleri kullanarak güvenli ve etkili bir doğrulama yöntemi sunar.

Biyometrik kimlik doğrulama yöntemleri arasında, tuş vuruşu ile doğrulama öne çıkmaktadır çünkü:

- Müdahale gerektirmez (non-intrusive),
- Sadece standart bir klavye gerektirir,
- Parmak izi veya yüz tanıma gibi yöntemlerin aksine, sürekli izleme ve doğrulama yapılabilir. (OWASP Authentication Term Sheet) (Ahmed Anu Wahab vd. 2023)

2.3.1 Geleneksel Kimlik Doğrulama Mekanizmalarının Sınırlamaları

Şifreler gibi geleneksel kimlik doğrulama yöntemleri, zayıf yönleri iyi bilinmesine rağmen hâlâ yaygın şekilde kullanılmaktadır. Kullanıcılar genellikle zayıf parolalar seçer, aynı kimlik bilgilerini farklı platformlarda tekrar kullanır ve oltalama gibi saldırılara karşı savunmasız kalır. Bu da hesapların ele geçirilmesine yol açar. İki faktörlü kimlik doğrulama (2FA) mekanizmaları—örneğin tek seferlik SMS şifreleri veya donanım belirteçleri—daha sağlam güvenlik sunsa da, kullanılabilirlik sorunları oluşturur...

Parmak izi ve yüz tanıma gibi biyometrik doğrulama sistemleri, yukarıdaki sınırlamaların çoğunu hafifletir; ancak yeni zorluklar da beraberinde getirir. Bu sistemler özel sensörler gerektirir ve bu sensörler, sahteciliğe karşı savunmasız olabilir. Ayrıca, farklı iklim koşullarında her zaman tutarlı performans gösteremeyebilirler. Gizlilik ve veri depolama ile ilgili endişeler ise bu sistemlerin yaygınlaşmasının önünde hâlâ önemli bir engel teşkil etmektedir.

2.3.2 Tuş Vuruşu Kimlik Doğrulamanın Avantajları

Tuş vuruşu doğrulama, hem geleneksel hem de fizyolojik biyometrik yöntemlerin çoğu sınırlamasını ortadan kaldırır. Web uygulamaları üzerinden çalıştığı için özel donanıma ihtiyaç duymaz ve çeşitli platformlarda kolayca erişilebilir ve kullanılabilir. (OWASP Authentication Term Sheet) Ayrıca, yalnızca ilk girişte değil; oturum süresince kullanıcının davranışındaki anomalileri tespit ederek sürekli doğrulama sağlar.

Diğer avantajları şunlardır:

Sezgisel ve kullanıcıyı rahatsız etmeyen bir etkileşim sunar: Parmak izi veya yüz tanımada olduğu gibi doğrudan özel bir kullanıcı girdisi gerektirmez; yalnızca normal yazma davranışı yeterlidir.

Taklit edilmesi zordur: Tuş vuruş dinamikleri davranışa dayalıdır ve parmak izi ya da yüz gibi fiziksel özelliklere göre taklit edilmesi daha zordur. (Ahmed Anu Wahab vd. 2023)

Çok faktörlü kimlik doğrulama için uygundur: Tuş vuruşu doğrulama, mevcut kimlik doğrulama yöntemlerini tamamlayarak kullanılabilirliği azaltmadan ek bir koruma katmanı sunar. (Yuhua Wang vd. 2018)

2.3.3 Keystroke Authentication'ın Farklı Alanlardaki Kullanım Alanları

Keystroke authentication, kullanıcıların klavye kullanım alışkanlıklarını analiz ederek kimlik doğrulama yapan bir davranışsal biyometri yöntemidir. Gerçek dünya uygulamalarında birçok farklı alanda kullanılmaktadır:

Finansal Hizmetler: Banka ve ödeme platformları, çevrimiçi işlemlerde güvenliği artırmak ve yetkisiz hesap erişimlerini önlemek için keystroke authentication'ı kullanabilir. (Erhan Yılmaz vd. 2023)

Kurumsal Güvenlik: Şirketler, kurumsal ve gizli bilgilere erişimi güvence altına almak ve içeriden gelen tehditlere karşı koruma sağlamak için bu mekanizmayı devreye alabilir. (Sebastián Sznur vd. 2008)

Mobil Güvenlik: Akıllı telefonlarda uygulama kilidi ve cihazın genel güvenliği için ek bir güvenlik katmanı olarak kullanılabilir. (E. V. C. Urtiga 2011)

2.3.4 Güvenlik Problemleri ve Potansiyel Zorluklar

Her ne kadar keystroke authentication birçok avantaj sunsa da, bazı güvenlik tehditlerine açıktır:

Taklit Edilebilirlik: Saldırganlar, makine öğrenimi algoritmalarıyla bir kişinin tuş vuruş dinamiklerini taklit etmeye çalışabilir. (Yu Gu vd. 2022)

Davranışsal Değişkenlik: Kullanıcının stres, travma veya fiziksel durumundaki değişiklikler tuşlama alışkanlıklarını etkileyebilir ve yanlış negatif sonuçlara neden olabilir. (Yuhua Wang vd. 2018)

Bu tehditleri hafifletmek amacıyla araştırmacılar derin öğrenmeye dayalı anomali tespiti ve melez kimlik doğrulama yaklaşımları geliştirmektedir. (Ula Tarik Salim vd. 2023)

BÖLÜM 3

3. YÖNTEM

Bu bölümde çalışmanın metodolojik yaklaşımı açıklanmaktadır. Simülasyon tabanlı bu tuş vuruşu dinamikleri (keystroke dynamics) verilerini kullanarak kullanıcı kimlik doğrulama sürecinde geleneksel makine öğrenmesi (ML) algoritmaları ile derin öğrenme (DL) yaklaşımlarının başarım farklılıklarını ortaya koymaktır. Bu kapsamda, hem geleneksel hem de yeni nesil yapay zeka teknikleri aynı veri seti üzerinde test edilerek karşılaştırmalı analiz gerçekleştirilmiştir. Bu çalışma, toplam 20 akademik ve endüstri kaynağına dayanılarak hazırlanmıştır. Kaynaklar arasında hakemli makaleler, teknik raporlar, endüstri beyaz kitapları ve vaka çalışmaları bulunmaktadır. Teorik temel, sürekli biyometrik kimlik doğrulama yaklaşımlarını ele alan çalışmalar (Roy et al., 2022; Lien , Vhaduri, 2023) ve NIST SP 800-63B , OWASP kimlik doğrulama kılavuzları (Grassi et al., 2017) temel alınarak oluşturulmuştur.

Metodolojik yaklaşım, birbirini tamamlayan birkaç aşamadan oluşmaktadır:

Literatür İncelemesi ve Teorik Çerçeve: Tuş vuruşu dinamikleri, davranışsal biyometri ve sürekli kimlik doğrulama yöntemlerini inceleyen kapsamlı bir inceleme yapılmıştır. Sabit metin ve serbest metin kimlik doğrulama yöntemleri karşılaştırılmış; tuş vuruşu süresi (tutma süresi), tuşlar arası uçuş süresi, digraf ve trigraf süreleri gibi temel metriklerin avantajları ve sınırlamaları analiz edilmiştir (Killourhy , Maxion, 2009; Bhatia , Hanmandlu, 2017).

Veri Toplama ve Ön İşleme: Klavye etkileşimlerinden elde edilen zaman damgalı tuş vuruşu ve bırakma olayları, özellik çıkarma işlemi gerçekleştirmek için işlendi. Ön işleme aşamasında, gürültülü veriler filtrelendi, eksik zaman damgaları enterpolasyon yöntemleri kullanılarak düzeltildi ve istatistiksel normalizasyon uygulandı (Kim et al., 2020).

Akış Mimarilerinin Karşılaştırmalı Analizi: Büyük ölçekli oturum verilerini iletmek için kullanılan Apache Kafka, Flink ve Spark Streaming sistemleri incelendi. Kafka'nın en az bir kez semantiği ile Flink'in tam olarak bir kez semantiği arasındaki farklar, 10.000+ oturum/saniye yük altında gecikme (medyan gecikme) ve 99. yüzdelik gecikme ölçümlerine göre değerlendirildi (Cumbane, Gidófalvi, 2019; Confluent, 2025).

Modelleme ve Makine Öğrenimi Yaklaşımı: Klasik makine öğrenimi yöntemleri (k-NN, SVM, Random Forest) ile derin öğrenme tabanlı modeller (CNN, LSTM, Transformer) kullanıcı kimlik doğrulaması için karşılaştırılmıştır. Özellik seçimi ve boyut azaltma için özellik puanlama (Kim et al., 2020) ve diferansiyel evrim tabanlı optimizasyon (Wang et al., 2019) yöntemleri kullanılmıştır.

Değerlendirme Metrikleri: Sistem performansı, EER (Eşit Hata Oranı), FAR (Yanlış Kabul Oranı) ve FRR (Yanlış Reddetme Oranı) metrikleri kullanılarak ölçülmüştür. Ek olarak, sürekli kimlik doğrulama bağlamında, oturum süresi boyunca kümülatif hata oranları ve kullanıcı deneyimi göstergeleri dikkate alınmıştır (Stylios et al., 2023; Stragapede et al., 2024).

Çok Faktörlü Kimlik Doğrulama Senaryosu: MFA (Çok Faktörlü Kimlik Doğrulama) senaryoları, tuş vuruşu biyometrisi ile şifreler ve OTP tabanlı yöntemler entegre edilerek test edilmiştir. Kullanıcı çalışmaları, tuş vuruşu dinamiklerini ek bir faktör olarak entegre etmenin kimlik doğrulama süresini %60'a kadar azalttığını göstermiştir (Wahab et al., 2023).

Araştırma sürecinde, tuş vuruşu dinamiklerinden elde edilen tuşlar arası gecikme süreleri ve tuşlara basılı kalma süreleri gibi zamansal verileri içeren özgün bir veri kümesi oluşturulmuş veya mevcut bir veri kümesi kullanılmıştır. Sonrasında, her bireyin kendine özgü zamansal profilini belirlemek amacıyla öz nitelik çıkarımı (feature extraction) süreci uygulanmıştır.

Makine öğrenmesi tarafında, Destek Vektör Makineleri (SVM), Karar Ağaçları (Decision Trees) ve Rastgele Ormanlar (Random Forest) gibi klasik sınıflandırma algoritmalarından faydalanılmıştır. Bu modellerin performansı;

doğruluk (accuracy), hassasiyet (precision), geri çağırım (recall) ve F1-skor gibi istatistiksel metriklerle değerlendirilmiştir.

Derin öğrenme uygulamaları kapsamında ise, zaman serisi verilerle çalışmada etkili olduğu bilinen yapısal sinir ağı (neural network) modelleri, özellikle Uzun Kısa Süreli Bellek (LSTM) mimarisi ağırlıklı olarak tercih edilmiştir. Bazı deneysel çalışmalarda, Evriltilmiş Sinir Ağları (Convolutional Neural Networks - CNN) ile öznitelik çıkarımı yapılarak, hibrit modeller de test edilmiştir.

Karşılaştırma için kullanılan veri setinin tipik özellikleri örneklerle açıklanmıştır.

1. **Tuşa Basma Süresi (Dwell Time):** Bir tuşa basıldığı an ile aynı tuşun bırakıldığı an arasındaki süre.

   Örnek: Key_A_Press = 1023 ms, Key_A_Release=1080 ms → Dwell_A=57 ms

2. **İki Tuş Arası Uçuş Süresi (Flight Time):** Bir tuş bırakıldıktan sonra diğer tuşa basılana kadar geçen süre.

Alt türleri:

Up-Down (UD): İlk tuşun bırakılma zamanı ile ikinci tuşun basılma zamanı.

Down-Down (DD): İlk tuşun basılma zamanı ile ikinci tuşun basılma zamanı.

Up-Up (UU): İlk tuşun bırakılma zamanı ile ikinci tuşun bırakılma zamanı.

Down-Up (DU): İlk tuşun basılma zamanı ile ikinci tuşun bırakılma zamanı.

Örnek:

Key_H_Release=1090 ms, Key_E_Press=1120 ms → Flight_UD_H_E = 30 ms

3. **Digraph (İki Harf Kombinasyonu Süresi)**: İki ardışık tuşun basılmasından oluşan çiftin toplam yazılma süresi (DD veya UD üzerinden hesaplanabilir). (Baljıt Sıngh Saini vd. 2020)

   Örnek: Key_T_Press = 1300 ms, Key_H_Press = 1380 ms → Digraph_TH_DD = 80 ms

4. **Trigraph (Üçlü Harf Kombinasyonu) :** Üç ardışık tuşun toplam yazım süresi ve ilişkisel zamanlamaları. (Ula Tarik Salim vd. 2023)

Örnek: "T", "H", "E" için:

Dwell_T, Flight_TH, Dwell_H, Flight_HE, Dwell_E

5. **Hold Patterns:** Aynı tuşa birden fazla kez basma aralıkları (örneğin "aaaaaa" gibi tekrarlar). (Erhan Yılmaz vd. 2023)

Özellik: Ritimli ya da kesintili basma davranışlarını yansıtır.

6. **Yazım Hızı (Typing Speed):** Dakikadaki karakter sayısı (Characters Per Minute - CPM) (Aythamı Morales vd. 2016)

Örnek: 50 kelime/dk hızla yazan bir kullanıcı → yaklaşık 250-300 CPM

7. **Yanlış Basılan Tuşlar / Backspace Kullanımı:** Hatalı yazım sıklığı ve düzeltme alışkanlığı. (Ahmed Anu Wahab vd. 2023)

Örnek: Backspace kullanımı: 8 defa, Delete kullanımı: 3 defa

8. **Özel Tuşlar ve Kısayolların Kullanımı:** Shift, Caps Lock, Ctrl, Alt gibi modifikasyon tuşlarının ne sıklıkla ve nasıl kullanıldığı.

Örnek: Shift + L, Ctrl + Z gibi kombinasyonlar.

9. **Periyodik Davranış Desenleri:** Örneğin bir kullanıcının her yeni kelime başında kısa bir duraklama yapması.

Kelime aralarında (Space tuşunda) düzenli zamanlama aralıkları.

Her iki yaklaşım için kullanılan aynı veri seti kullanılarak, ön işleme, model eğitimi ve test aşamaları eşzamanlı olarak yürütülmüş; sonuçlar tablolar ve grafikler ile görselleştirilerek aralarındaki farklılıklar ölçülmüştür. Elde edilen bulgular, makine öğrenmesi yöntemlerinin düşük hacimli veri kümelerinde daha stabil sonuçlar üretebildiğini, buna karşın derin öğrenme modellerinin büyük veri kümelerinde çok daha yüksek doğrulukla çalıştığını ortaya koymuştur.

3.1 TUŞ VURUŞ DİNAMİKLERİNDE GELENEKSEL MAKİNE ÖĞRENMESİ ALGORİTMALARI

Tuş vuruş dinamikleri alanında, kullanıcı kimlik doğrulama ve anomali tespiti amacıyla geleneksel makine öğrenmesi teknikleri yaygın olarak kullanılmaktadır. Bu alanda en sık tercih edilen algoritmalar arasında k-En Yakın Komşu (k-NN), Destek Vektör Makineleri (SVM) ve Rastgele Ormanlar

(Random Forest) yer almaktadır. Bu algoritmalar, yazma davranışlarından elde edilen biyometrik özelliklerle ilişkili kalıpları tanıma becerileri sayesinde popülerlik kazanmıştır. (Killourhy & Maxion, 2009)

Buna ek olarak, bu alanda kullanılan diğer yerleşik algoritmalar şunlardır:

- Naive Bayes sınıflayıcıları
- Bagging tabanlı topluluk (ensemble) yöntemleri
- Karar Ağaçları (Decision Trees)
- Bayes Ağları (BayesNet)
- Evrensel Arkaplan Modelleri ile bütünleştirilmiş Gauss Karışım Modelleri (GMM-UBM)
- Tek Sınıflı Destek Vektör Veri Tanımlama yöntemi (One-Class SVDD)
- Manhattan ölçekli ve Mahalanobis tabanlı En Yakın Komşu sınıflayıcıları
- Z-puanı (Z-score) tabanlı aykırı değer tespiti yöntemleri (Teh et al., vd. 2013; Mondal & Bours, 2015)

Ayrıca, Tablo 3.1'de görüldüğü gibi, Öklid Mesafesi (Euclidean Distance) ve diğer ölçüme dayalı mesafe fonksiyonları, tuş vuruşlarındaki zamansal ve mekânsal varyasyonları anlamlandırmak için sıkça kullanılmaktadır. (Killourhy & Maxion, 2009)

Tablo 3.1 ML Modellerinin Karşılaştırması

ML Modeli	Doğruluk Oranı (EER/AUC)	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar
GMM (Gauss Karışım Modelleri)	AUC: 0,914, EER: 0,132 (Aalto). Genellikle en düşük EER değerine sahiptir.	Bir parametre seti (λ={w i,ui,Σ i}) ile ifade edilir.	Genellikle 200 örnek gibi daha büyük eğitim setleri gerektirir.	Orta ila Yüksek (büyük kümeler için)	Yazma kalıplarını modellemek ve tek sınıf sınıflandırma sında kullanılır.

Tablo 3.1 (Devamı) ML Modellerinin Karşılaştırması

ML Modeli	Doğruluk Oranı (EER/AUC)	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar
Mahalanobis Mesafesi Tabanlı Sınıflandırma	EER: 0,096 (CMU). AUC: 0,914, EER: 0,132 (Aalto). Küçük eğitim setlerinde iyi performans gösterir.	Kullanıcının ortalama özellik vektörü hesaplanır. Eğitim/test verileri bölünür (%70/%30). Değişen özellik sayısı veya alt kümeler için uygun değildir.	Küçük eğitim setleriyle kullanılabilir.	Düşük (Basit istatistiksel algoritma)	Bekleme Süresi (H), Yukarı-Aşağı Süresi (UD), Aşağı-Aşağı Süresi (DD) gibi zamanlama özelliklerini kullanır. Anomali tespiti için kullanılır.
MLP (Çok Katmanlı Perceptron)	Doğruluk: %97,17, EER: %2 (Tuş vuruşu). Doğruluk (Füzyon): %98,4, EER: %1,6. Başarı: %99,0 (Tek), %99,6 (Kombine) (Mayda, Demir).	Giriş verileri üzerinde eğitilmiştir.	Mayda ve Demir'in çalışmasında, denek başına 100 veri noktası; birleştirilmiş verilerle 10 veri noktası kadar az sayıda veriyle başarılı sonuçlar elde edilebilir.	Orta ila Yüksek	Tuş basma süresi ve tuşlar arası geçiş süresi gibi özellikler kullanılır.
LSTM (Uzun Kısa Süreli Bellek)	Doğruluk: %96,1, EER: %3 (Tuş vuruşu). Doğruluk (Birleştirme): %95,1, EER: %4,7.	Ağırlıklar (W), yinelenen ağırlıklar (RW) ve önyargılar (b) ile yapılandırılır. Uzun tuş vuruşu dizileri için zamansal bağımlılıkları yakalamada etkilidir.	Yeterli miktarda kaydedilmiş veri ve tuş vuruşu dizisi uzunluğu önemlidir.	Orta ila Yüksek	Tuş vuruşu verilerinden zamansal ve bağlamsal ilişkileri öğrenir. HL, IL, PL, RL ve ASCII kodu gibi özellikler kullanılır.

Tablo 3.1 (Devamı) ML Modellerinin Karşılaştırması

ML Modeli	Doğruluk Oranı (EER/AUC)	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar
Transformer tabanlı ağlar (ör. TypeFormer)	EER: %0,0186 (Çift kodlayıcı, 10 kaydedilmiş örnek). EER: %3,25 (TypeFormer, 5 kayıt oturumu). TypeNet'e göre %5,95 mutlak EER iyileşmesi.	Kendi kendine dikkat mekanizması kullanır. Farklı kayıp fonksiyonları (Üçlü, toplu üçlü, WDCL kaybı) ve mesafe ölçütleri (Öklid, Manhattan, Kosinüs) incelenir.	Büyük miktarda eğitim verisi gerektirir; küçük veri kümeleri için transfer öğrenimi gerekebilir. Kayıtlı veri miktarı ve dizi uzunluğu arttıkça performans artar.	Yüksek	RNN'lerin ölçeklenebilirlik sorunlarını ortadan kaldırır. HL, IL, PL, RL ve ASCII kodu gibi özellikler kullanılır.
k-NN (k-En Yakın Komşu)	EER: 0,096 (Killourhy , Maxion, 2009).	Mesafe tabanlı bir sınıflandırıcıdır.	Kaynaklarda doğrudan belirtilmemiştir.	Düşük ila Orta	Kullanıcı davranış analizi ve anomali tespitinde kullanılır.
RF (Rastgele Orman)	Başarı: %99,6 (Tek ve Kombine) (Mayda, Demir).	Karar ağaçlarına dayalı bir topluluk öğrenme yöntemi.	Kaynaklarda doğrudan belirtilmemiştir.	Düşük ila Orta	Kullanıcı davranış analizi ve anomali tespitinde kullanılır. Özellik önemini değerlendirmek için kullanılır.
SVM (Destek Vektör Makineleri)	Başarı: %99,4 (Tek), %99,8 (Kombine) (Mayda, Demir).	Optimum karar sınırları oluşturur.	Kaynaklarda doğrudan belirtilmemiştir.	Orta	Kullanıcı davranış analizi ve anomali tespitinde kullanılır. Tek sınıf sınıflandırması için de kullanılır

Tablo 3.1 (Devamı) ML Modellerinin Karşılaştırması

ML Modeli	Doğruluk Oranı (EER/AUC)	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar
ITAD (Örnek Tabanlı Kuyruk Alanı Yoğunluğu)	EER: %1,3 (CU mobil). EER: %7,8 (Clarkson II, 200 diyagram).	Yeni bir örnek tabanlı grafiksel karşılaştırma algoritması.	Kullanıcıları doğrulamak için gereken tuş vuruşu sayısını azaltmayı amaçlar. Küçük veri kümelerinde başarılıdır.	Düşük ila Orta	Tuş vuruşu özelliklerinin monogramları ve digramları tanımlama için yararlı bulunmuştur.
Öklid Mesafesi	FAR: %12,97, FRR: %2,25 (Mobil sayısal tuş takımı, 8 karakter)	İki n boyutlu vektör arasındaki mesafeyi hesaplar.	Örnek sayısı arttıkça hata oranları azalır.	Düşük (Basit ve hızlı)	Kullanıcının tuş basma/bırakma sürelerini ve tuşlar arası geçiş sürelerini kullanır.
Kalıntı CNN (Önerilen Yöntem)	EER: %0,0066, Doğruluk: %99,3 (CMU).	Derin öğrenme ve Evrişimli Sinir Ağları (CNN) kullanır. Paralel hesaplama ile hızlandırılmıştır.	CMU veri setinde değerlendirilmiştir.	Yüksek (ancak hızlandırılmış).	Bekleme süresi, uçuş süresi ve anahtar geçiş süresi gibi zamansal özellikleri kullanır.

Kullanılan bu algoritmalar, özellikle özellik altkümeleri üzerinden genelleme yapabilme, gürültülü biyometrik verilerle başa çıkabilme ve hem gerçek zamanlı hem de çevrimdışı (offline) kimlik doğrulama uygulamalarında güçlü performans sunabilme yeteneklerine göre seçilmiştir. (Ahmed & Traore, 2007; Mondal & Bours, 2015)

3.1.1 K-En Yakın Komşu (k-NN)

k-En Yakın Komşu (k-NN) algoritması, yeni bir veri noktasını, eğitim verisinden elde edilen en yakın k komşusu arasındaki baskın sınıfa atayarak sınıflandırmayı mümkün kılar. Tuş vuruş dinamikleri bağlamında, bir bireyin yazım deseni (paterni), veritabanında saklanan desenlerle karşılaştırılır ve en yakın kullanıcıların benzer özelliklerini en iyi şekilde tanımlayan sınıfa atanır. Bu benzerlik genellikle Öklid Mesafesi (Euclidean Distance) gibi uzaklık ölçümleriyle değerlendirilir.

Çeşitli araştırmalar, k-NN algoritmasının tuş vuruş dinamiklerini kullanan kimlik doğrulama uygulamalarında kullanılabilirliğini doğrulamıştır. Modelin sadeliği, parametrik olmayan yapısı ve desen tanıma yeteneği, onu davranışsal biyometrik sistemler için etkili bir temel model hâline getirmektedir. (Killourhy, K. S., & Maxion, R. A. 2009) ; (Teh, P. S., Teoh 2013)

3.1.2 Destek Vektör Makineleri (SVM)

Destek Vektör Makineleri (SVM), farklı veri sınıflarını en iyi şekilde ayıran bir veya daha fazla hiper düzlemi bulmayı amaçlayan güçlü bir sınıflandırma yöntemidir. Verilerin doğrusal olarak ayrılması mümkün olmadığında, Radyal Tabanlı Fonksiyon (RBF) gibi çekirdek fonksiyonları kullanılarak veriler daha yüksek boyutlu uzaylara dönüştürülür ve bu sayede sınıflandırma daha etkili hâle gelir.

Tuş vuruş dinamikleri alanında, SVM algoritmaları farklı kullanıcıların özgün yazım desenleri arasında karar sınırlarını tanımlamak için yaygın olarak kullanılmaktadır. Deneysel çalışmalar, farklı test senaryolarında SVM'nin yüksek doğruluk oranları elde ettiğini göstermektedir. Özellikle bir çalışmada, birleştirilmiş özellik vektörleri ile yapılan sınıflandırmada %99.8 doğruluk oranına ulaşılmıştır. Ayrıca, Tek Sınıflı SVM (One-Class SVM) yöntemi, yalnızca gerçek kullanıcı verilerinin eğitim için mevcut olduğu durumlarda anomali tespiti ve kimlik doğrulama görevlerinde de kullanılmıştır. (Killourhy,

K. S., & Maxion, R. A. 2009). ; (Revett, K., de Magalhães 2008).;(Mondal, S., & Bours, P. 2015).

3.1.3 Rastgele Ormanlar (Random Forest)

Rastgele Orman (Random Forest), çok sayıda karar ağacının çıktısını birleştirerek daha kararlı bir sınıflandırma sonucu elde eden bir topluluk öğrenmesi (ensemble learning) yaklaşımıdır. Her bir ağaç, veri kümesinin rastgele bir örneklemi kullanılarak bootstrap aggregating (bagging) yöntemi ile oluşturulur. Nihai karar, tüm ağaçların çoğunluk oyuna göre verilir. Random Forest, tek bir karar ağacı modeline kıyasla daha yüksek doğruluk ve aşırı öğrenmeye (overfitting) karşı daha fazla dayanıklılık göstermektedir.

Random Forest algoritmaları, tuş vuruş dinamikleri alanında yoğun bir şekilde kullanılmış ve umut verici sonuçlar elde edilmiştir. Bir çalışmada, Random Forest algoritmasının tek oturumlu veri ile yapılan testlerde %99.6 doğruluk oranı elde ettiği ve diğer standart makine öğrenmesi algoritmalarından daha iyi performans gösterdiği belirtilmiştir. (Killourhy, K. S., & Maxion, R. A. 2009).

3.1.4 Geleneksel Makine Öğrenmesinde Öznitelik Mühendisliği

Geleneksel makine öğrenmesi algoritmalarının karakteristik bir yönü, ham giriş verilerinden özniteliklerin kasıtlı olarak seçilmesi veya çıkarılmasına dayanmalarıdır. Bu öznitelikler daha sonra öğrenme algoritmalarının girdisi olarak kullanılır. Tuş vuruş dinamikleri bağlamında ise, doğrudan ham zamanlama verilerinin kullanılması yerine, genellikle istatistiksel özetler (örneğin ortalama, standart sapma) veya tuş olaylarının zamansal sıralamaları gibi mühendislik ürünü öznitelikler tercih edilir.

Deneysel araştırmalar, özelliklerin seçimi ve kombinasyonunun, sınıflandırma görevlerinin doğruluğunu önemli ölçüde etkilediğini göstermiştir. Örneğin, uçuş süresi (flight time) ve basılı tutma süresi (dwell time) gibi zamanlama tabanlı özniteliklerin kullanımı, kimlik tanıma başarımını artırmıştır. Geleneksel algoritmalar genellikle daha az hesaplama gücü gerektirir ve küçük

veri kümeleri ile de etkili bir şekilde çalışabilir; ancak, bu algoritmaların genel başarıları büyük ölçüde başarılı öznitelik mühendisliği tekniklerine bağlıdır. (Teh, P. S., Teoh, 2013). ; (Banerjee, S., & Woodard, D. L. 2012).

3.2 DERİN ÖĞRENME MODELLERİ

Son yıllarda, tuş vuruş dinamikleri alanındaki araştırmalarda derin öğrenme modellerinin kullanımı büyük bir ivme kazanmıştır. Bu artışın başlıca nedeni, söz konusu modellerin karmaşık örüntü tanıma problemlerini çözmedeki olağanüstü başarısıdır. Derin öğrenme modelleri, çok katmanlı yapay sinir ağları aracılığıyla, ham veriden hiyerarşik temsilleri otomatik olarak çıkarma yeteneğine sahiptir. Tablo 3.2'de DL modellerinin Karşılaştırıması detaylı olarak ele alınmaktadır.

3.2.1 Çok Katmanlı Algılayıcı (Multilayer Perceptron, MLP)

Çok Katmanlı Algılayıcı (MLP), bir veya daha fazla gizli katman içeren temel bir ileri beslemeli (feedforward) sinir ağı yapısıdır. Tuş vuruş dinamikleri alanında MLP, hem sürekli (continuous) hem de statik doğrulama (static authentication) senaryolarında kullanılmaktadır. Özellikle bir çalışmada, MLP'nin tekil oturum verilerinde %99.0, çoklu oturum verilerinde ise %99.6 doğruluk oranına ulaştığı rapor edilmiştir. Bu durum, MLP'nin etkinliğini açıkça ortaya koymaktadır. (Revett, K., de Magalhães, 2008).

Tablo 3.2 DL Modellerinin Karşılaştırması

DL Modeli	Doğruluk / EER	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar	Ek Notlar
MLP (Çok Katmanlı Perceptron)	Tek Veri Doğruluğu: %97,17 (Keystroke Dynamics). %99,0 (Mayda ve Demir). Birleştirilmiş Veri Doğruluğu: %98,4 (Mayda ve Demir). %99,6 (Mayda ve Demir).	Giriş verileriyle eğitilmiştir. Optimal karar sınırları oluşturulur [Analiz].	Mayda ve Demir'in çalışmasında, her denek için 100 veri noktası. Sadece 10 birleşik veri noktasıyla başarılı sonuçlar elde edilebilir.	Orta	Tuş basma süresi ve tuşlar arası geçiş süresi gibi özellikler. Sabit boyutlu girdi nedeniyle sürekli ve anlık zamansal verilerin (ör. nefes alma) işlenmesinde zorluk.	Genellikle istatistiksel yöntemlerden daha iyi performans gösterir. Genellikle sabit boyutlu (sabit metin) girdi kullanılır.
LSTM (Uzun Kısa Süreli Bellek)	Doğruluk: %96,1, EER: %3 (Tuş Vuruşu Dinamikleri). Füzyon Doğruluğu: %95,1, EER: %4,7.	Ağırlıklar (W) ve yinelenen ağırlıklar (RW) ile yapılandırılır. Uzun tuş vuruşu dizileri için zamansal bağımlılıkları yakalamada etkilidir.	Yeterli miktarda kaydedilmiş veri ve tuş vuruşu dizisi uzunluğu önemlidir.	Orta ila Yüksek	Tuş vuruşu verilerinden zamansal ve bağlamsal ilişkileri öğrenir. HL, IL, PL, RL ve ASCII kodu gibi özellikler kullanılır. Büyük bir gecikmeyle gerçekleşse bile bağımlılıkları yakalar.	Transformatör tabanlı modeller genellikle LSTM'den daha iyi performans gösterir. Mobil cihazlarda da kullanılır.

Tablo 3.2 (Devamı) DL Modellerinin Karşılaştırması

DL Modeli	Doğruluk / EER	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar	Ek Notlar
CNN (Konvolüsyonel Sinir Ağı)	EER: %0,0066. Doğruluk: %99,3 (CMU, Residual CNN kullanılarak CMU veri setinde). Çeker ve Upadhya (2017): EER: 0,085. Doğruluk: %94.	Derin öğrenme ve Evrişimli Sinir Ağları (CNN) kullanır. Paralel hesaplama ile hızlandırılmıştır. Tek bir giriş görüntüsü içinde farklı desenleri öğrenebilir.	CMU veri seti üzerinde değerlendirilmiştir. Farklı yapılandırmalarla eğitilebilir.	Yüksek (Potansiyel Olarak Hızlandırılmış)	Bekleme süresi, uçuş süresi ve anahtar geçiş süresi gibi zamansal özellikleri kullanır. Hem görüntü tabanlı hem de zamansal verilerden kalıpları öğrenir.	Mevcut çalışmalar arasında en iyi performansa sahip olduğu iddia edilmektedir. Mobil cihazlarda da kullanılır.
Transformatör tabanlı ağlar (ör. TypeFormer)	EER: %0,0186 (Çift kodlayıcı, 10 kayıt örneği). EER: %0,0163. SVM uyumluluğu: Hayır. TypeFormer: EER: %3,25 (5 kayıt oturumu), EER: %3,50 (50 ham girdi). TypeNet EER iyileştirmesi: %5,95.	Kendi kendine dikkat mekanizması kullanır. Farklı kayıp fonksiyonları (Üçlü, toplu üçlü, WDCL kaybı) ve mesafe ölçütleri (Öklid, Manhattan, Kosinüs) incelenir. RNN'lerin ölçeklenebilirlik sorunlarını aşar.	Büyük miktarda eğitim verisi gerektirir; küçük veri kümeleri için (ör. Aalto masaüstü, 58.000 karakter) transfer öğrenimi gerekebilir. Kayıtlı veri miktarı ve dizi uzunluğu arttıkça performans artar.	Yüksek	HL, IL, PL, RL ve ASCII kodu gibi özellikler kullanılır. Zamansal ve bağlamsal bağımlılıkları yakalar. Uzun ve değişken tuş vuruşu dizilerini etkili bir şekilde modelleyebilir.	Serbest metin tuş vuruşu kimlik doğrulamasında yeni bir standart belirlemiştir. Sağlam özellikleri çıkarır.

Tablo 3.2 (Devamı) DL Modellerinin Karşılaştırması

DL Modeli	Doğruluk / EER	Eğitim Süreci	Veri Gereksinimi	Hesaplama Maliyeti	Özellikler ve Açıklamalar	Ek Notlar
Derin Sinir Ağları (DNN)	Genel olarak istatistiksel yöntemlere kıyasla daha iyi performans sağlar.	Verilerdeki karmaşık kalıpları ve zamansal bağımlılıkları öğrenme yeteneğine sahiptir.	Genellikle büyük miktarda eğitim verisi gerektirir.	Yüksek	Karmaşık ağ yapıları ve karmaşık özellik mühendisliği kullanır.	Tuş vuruşu biyometrik kimlik doğrulama performansını önemli ölçüde artırmıştır.

3.2.2 Tekrarlayan Sinir Ağları (RNN) ve Uzun Kısa Süreli Bellek (LSTM) Mimarileri

Tekrarlayan Sinir Ağları (RNN) ve bunların gelişmiş bir türü olan Uzun Kısa Süreli Bellek (LSTM) ağları, sıralı verileri analiz etmek için tasarlanmış mimarilerdir. Bu yapılar, bir dizinin önceki öğelerinden gelen bilgileri bellekte tutma kapasitesine sahiptir. Tuş vuruş dinamikleri, doğası gereği sürekli ve sıralı olaylardan oluştuğu için, bu tür modeller, yazım davranışının zamansal bağımlılıklarını anlamada oldukça uygundur.

Özellikle LSTM ağları, yazma desenlerinin zamana dayalı özelliklerini modellemede yüksek doğruluk oranları göstermiştir. Bu nedenle, tuş vuruş bilgisine dayalı biyometrik kimlik doğrulama sistemlerinde oldukça etkili bulunmuşlardır. (Acien, A., Morales, A., Ferrer, 2021). ; (Monaco, J. V., Tappert, 2015).

3.2.3 Konvolüsyonel Sinir Ağları (CNN)

Konvolüsyonel Sinir Ağları (CNN) genellikle görüntü işleme alanında yaygın olarak kullanılsa da, 1-boyutlu (1D) varyantları, tuş vuruş dinamikleri gibi sıralı verilerdeki yerel örüntüleri (örneğin kısa tuş dizileri arasındaki ilişkiler) yakalamak amacıyla uyarlanmıştır. Bu modeller, özellikle kullanıcıya özgü yazım davranışlarını ayırt etmek için gerekli olan zamansal korelasyonları belirlemede oldukça etkilidir.

Ayrıca, bazı hibrit yaklaşımlar geliştirilmiştir. Bu yöntemlerde, CNN modelleri ile Tekrarlayan Sinir Ağları (RNN) veya Uzun Kısa Süreli Bellek (LSTM) katmanları birleştirilerek, hem yerel örüntüler (CNN ile) hem de zamansal bağımlılıklar (RNN/LSTM ile) birlikte modellenmektedir. Bu da, karmaşık yazım davranışı senaryolarında genel tanıma performansının artırılmasına olanak tanır. (Acien, A., Morales, A., Ferrer, 2021).

3.2.4 Transformer Tabanlı Modeller

Doğal dil işleme (NLP) alanındaki başarılarının ardından, Transformer mimarileri yakın zamanda tuş vuruş dinamikleri analizi için yeniden uyarlanmıştır. Bu modeller, dikkat mekanizmaları (attention mechanisms) kullanarak sıralı verilerdeki uzun mesafeli bağımlılıkları etkili biçimde modelleyebilme kapasitesine sahiptir; bu durum, geleneksel RNN tabanlı modellerin sıklıkla zorlandığı bir alandır.

Yakın tarihli önemli bir çalışmada, mobil cihazlardan elde edilen serbest metin tuş vuruş verileri üzerinde çalışan ve Transformer mimarisi temelli yeni bir model olan TypeFormer tanıtılmış ve değerlendirilmiştir. Bu model, %3.25 EER (Equal Error Rate) ile alanın en iyi (SOTA) performansını göstermiştir. Bu, mobil serbest metin doğrulama sistemleri alanında dikkate değer bir ilerleme olarak değerlendirilmektedir. (Acien, A., Morales, A., Ferrer, 2021).

3.2.5 Tuş Vuruş Biyometriğinde Derin Öğrenmenin Avantajları ve Sınırlamaları

Derin öğrenme modellerinin en büyük avantajlarından biri, ham duyusal verilerden veya temel ölçümlerden (örneğin tuşa basma ve bırakma süreleri gibi) karmaşık ve ayırt edici öznitelikleri otomatik olarak öğrenebilmesidir. Bu özellik, geleneksel makine öğrenmesi yaklaşımlarında genellikle ihtiyaç duyulan manuel öznitelik mühendisliği gereksinimini büyük ölçüde azaltır.

Çeşitli çalışmalar, derin öğrenme algoritmalarının, özellikle mobil arayüzler gibi değişkenliğin yüksek olduğu ve karmaşık örüntüler içeren senaryolarda, geleneksel istatistiksel veya makine öğrenmesi yöntemlerine göre daha yüksek başarı oranları sağladığını göstermektedir.

Genellikle, büyük ölçekli eğitim veri kümeleri ve önemli düzeyde hesaplama gücü gerektirirler. Bu nedenle, derin öğrenme modelleri daha çok verinin bol olduğu ve işlem kaynaklarının yeterli olduğu durumlar için uygundur. (Acien, A., Morales, A., Ferrer, 2021). ; (Acien, A., Galbally, J., Morales, A., & Fierrez, J. 2022).

Aşağıdaki tablo, kaynaklara dayanarak geleneksel makine öğrenmesi algoritmaları ile derin öğrenme modellerinin tuş vuruş dinamikleri bağlamındaki genel karşılaştırmasını sunmaktadır.

Akademik kaynaklar, sinir ağı tabanlı sınıflayıcıların – özellikle derin öğrenme modellerinin – tuş vuruş dinamikleri uygulamalarının geniş bir yelpazesinde istatistiksel (geleneksel) sınıflandırma yöntemlerine kıyasla daha iyi performans gösterdiğini belirtmektedir. (Teh, Teoh ve Yue, 2013; Banerjee & Woodard, 2012). Bu durum özellikle serbest metin, mobil giriş ya da cihazlar arası senaryolar gibi kullanıcı davranışında yüksek değişkenlik ve karmaşıklığın bulunduğu durumlarda geçerlidir. Bu tür senaryolarda, derin öğrenme modellerinin uyarlanabilir yapıları önemli avantajlar sağlamaktadır. (Acien et al., 2021).

Özellikle Transformer tabanlı modeller (örneğin TypeFormer), mobil serbest metin senaryolarında alanın en iyi (SOTA) performansını göstermiştir. Bu model, %3.25 EER (Equal Error Rate) gibi düşük hata oranları elde ederek önemli bir başarıya imza atmıştır. Transformer mimarileri, girdi dizilerindeki uzun menzilli bağımlılıkları etkili bir şekilde modelleyebilen dikkat mekanizmalarından (attention mechanisms) faydalanır. Bu yetenek, geleneksel modellerin genellikle yakalayamadığı ilişkileri öğrenmelerine olanak tanır.

Tablo 3-3'de de belirttildiği gibi, tüm bu avantajlara rağmen, SVM ve Random Forest gibi geleneksel makine öğrenmesi algoritmaları, özellikle kontrollü ortamlarda (örneğin sabit metin senaryolarında) ve iyi tanımlanmış özniteliklerin mevcut olduğu durumlarda hâlâ son derece başarılı sonuçlar verebilmektedir. Ayrıca, One-Class SVM veya mesafeye dayalı yöntemler gibi anomali tespiti yaklaşımları, yalnızca gerçek kullanıcı verisinin mevcut olduğu ya da yetkisiz erişimin düşük veriyle tespit edilmesi gereken doğrulama senaryolarında son derece yararlı olabilir. (Killourhy & Maxion, 2009; Teh et al., 2013).

Tablo 3.3 ML ve DL modellerinin karşılaştırması

Özellik / Algoritma Türü	Geleneksel Makine Öğrenimi	Derin Öğrenme Modelleri
Örnek Algoritmalar	k-NN, SVM, Rastgele Orman, Naif Bayes, Karar Ağacı, Bagging, Mesafeye Dayalı (Öklid), Anomali Algılama Algoritmaları	MLP, CNN, RNN, LSTM, Dönüştürücüler, DBN
Özellik Mühendisliği	Genellikle manuel özellik çıkarma/seçimi gerektirir.	Otomatik özellik öğrenme/çıkarma yeteneği.
Veri Gereksinimi Eğilimi	Genellikle DL'den daha az veri gerektirir, ancak yeterli veri performansı etkiler.	Genellikle daha fazla veri gerektirir, ancak doğru şekilde işlendiğinde daha az veriyle de başarılı olur.
Performans Eğilimi (Kaynaklara Göre)	Çalışmaya göre değişir, bazı durumlarda yüksek başarı gösterir (99,6% RF, 99,8% SVM). Zorlu senaryolarda genellikle DL'den daha düşüktür.	Genellikle geleneksel yöntemlerden daha yüksek başarı gösterir. DL modelleriyle (ör. Transformer) elde edilen SOTA (State-of-the-Art) sonuçları.
Sıralı Verilerin Uygunluğu	Doğrudan uygun değildir, özellik mühendisliği gerektirir.	Son derece uygundur (ör. RNN, LSTM, Transformers), zamansal bağımlılıkları modelleyebilir.
Karmaşıklık / Model Geliştirme	Genellikle DL'den daha basittir ve daha az hesaplama gücü gerektirir.	Daha karmaşıktır, eğitimi daha fazla hesaplama gücü ve zaman gerektirir.

3.3 TUŞ VURUŞ DİNAMİKLERİNDE YENİ GÜVENLİK TRENDLERİ; KİMLİK DOĞRULAMA VE YAPAY ZEKÂ TABANLI GÜVENLİK YAKLAŞIMLARI

Tuş vuruşu dinamikleriyle kimlik doğrulama sistemleri, gelişen teknolojilerle birlikte sürekli evrim geçirmektedir. Güvenlik paradigmalarının ve teknolojilerinin kesişimi, bu alanda daha esnek ve güvenli doğrulama mekanizmalarının geliştirilmesini mümkün kılmaktadır. Önümüzdeki yıllarda aşağıdaki alanlarda önemli gelişmeler beklenmektedir:

3.3.1 Gelecekte Görünen Güvenlik Trendleri

3.3.1.1 Zero-Trust Mimarisi (ZTA):

Sürekli doğrulama prensibine dayalı bu yapı, her kullanıcı oturumunun dinamik olarak doğrulanmasını sağlar. Bu model, özellikle kimlik bilgisini kötüye kullanım riskini azaltmada etkilidir. (NIST SP 800-207 Zero Trust Architecture)

3.3.1.2 Blockchain Tabanlı Kimlik Doğrulama

Merkeziyetsiz (decentralized) kimlik doğrulama** yapıları sayesinde, verinin manipüle edilmesi veya izinsiz erişim gibi risklerin önüne geçilebilir. (Zyskind et al., 2015)

3.3.1.3 Kuantum-Dirençli Biyometrik Doğrulama

Kafes tabanlı kriptografi (lattice-based cryptography) gibi kuantum sonrası (post-quantum) şifreleme yöntemleriyle biyometrik veriler, kuantum bilgisayarların oluşturabileceği tehditlerden korunabilir. (Chen et al., 2016 – NIST PQC project overview)

3.3.2 Yapay Zekâ Tabanlı Güvenlik Çözümleri

3.3.2.1 Tuş Vuruşu Doğrulamada Derin Öğrenme (Deep Learning):

CNN ve LSTM gibi modeller, yazım alışkanlıklarındaki küçük değişimleri tanıyarak sınıflandırma doğruluğunu artırır. (Acien et al., 2021 – TypeNet)

3.3.2.2 Federated Learning ile Güvenli Model Eğitimi:

Merkezi olmayan (federated) yapay zekâ eğitimi, kullanıcı verilerini sunucuda depolamadan, modelin kişisel gizliliğe zarar vermeden öğrenmesini sağlar. (Yang et al., 2019)

3.3.2.3 Otonom ve Adaptif Güvenlik Modelleri:

Yapay zekâ destekli anomali tespiti, yeni saldırı örüntülerine karşı sürekli adapte olur ve gerçek zamanlı tehdit önleme sağlar. (Creech & Hu, 2014)

Tuş vuruşu dinamiklerinin gelecekteki gücü, gelişmiş yapay zekâ sistemleri ile yeni nesil güvenlik stratejilerinin entegrasyonuna bağlıdır. Derin öğrenme, federated learning ve blokzincir teknolojilerinin birlikte kullanılması, bu biyometrik yöntemin sofistike siber güvenlik mimarilerinin temelini oluşturmasını sağlayabilir.

3.4 TUŞ VURUŞU ANALİZİNDE GÜÇLÜ YÖNLER, ZAYIF NOKTALAR VE ARAŞTIRMA BOŞLUKLARI

3.4.1 Avantajlar ve Dezavantajlar

Tuş vuruşu doğrulama, bireyleri yazım ritimlerine göre tanıyan davranışsal bir biyometrik yöntemdir. Öne çıkan avantajlar şunlardır: (Teh et al., 2013; Banerjee & Woodard, 2012)

- Düşük maliyetlidir, ek donanıma ihtiyaç duymaz.
- Sürekli doğrulama sağlar.
- Makine öğrenmesi modelleriyle esneklik sunar.

Ancak aşağıdaki önemli sınırlamalara da sahiptir:

- Serbest metin senaryolarında yüksek yanlış kabul oranı (FAR) görülebilir.
- Shoulder-surfing (yan bakışla izleme) saldırılarına karşı savunmasızdır.
- Kullanıcının ekolojik (ortam) ve psikolojik durumları , doğrulama sonuçlarını etkileyebilir. (Monaco et al., 2015)

BÖLÜM 4

4. BULGULAR

Tuş vuruş dinamiklerine dayalı kullanıcı kimlik doğrulama sistemlerinin güvenilirliği, kullanıcının o anki stres, yorgunluk, duygusal durum ve dikkat dağınıklığı gibi geçici fiziksel ve zihinsel durumlarından önemli ölçüde etkilenmektedir; bu durum, özellikle serbest metin yazma ve sürekli kimlik doğrulama senaryolarında modellerin sağlamlığı açısından kritik bir zorluk teşkil etmektedir.

4.1 TUŞ VURUŞ DİNAMİKLERİNİN ÖZELLİKLERİ VE GEÇİCİ DURUMLARA DUYARLILIĞI

Tuş vuruş dinamikleri, davranışsal analiz temelli bir biyometrik tekniktir ve bir kişinin klavye üzerindeki tuşlara basma süresi, basılı tutma süresi ve tuşlar arası geçiş gecikmesi gibi zamansal özellikleri analiz eder.

Parmak izi veya iris gibi fizyolojik biyometrik yöntemlerin aksine, davranışsal biyometrik özellikler, kullanıcının o anki bilişsel ve duygusal durumunu da yansıtabilir. Güncel literatür, stres, yorgunluk ve duygusal dalgalanmalar gibi geçici durumların tuş vuruş dinamiklerini etkileyebileceğini göstermektedir (Banerjee & Woodard, 2012; Killourhy & Maxion, 2009). Bazı çalışmalar, yorgunluk ve kıyafet değişiklikleri gibi kullanıcı davranışlarını dolaylı yoldan etkileyen faktörlerin sistem performansını etkileyebileceğini belirtmiştir. Diğer çalışmalarda ise doğrudan stresin tuşlama davranışı üzerindeki etkisi araştırılmıştır. Araştırmacılar ayrıca, derin nefes alma, dikkat dağınıklığı veya konuşma gibi durumların kullanıcının normal davranışlarından sapmasına neden olduğunu gözlemlemiştir. Mobil ortamlarda, kullanıcının duygusal durumu, biyometrik doğrulama için önemli bir çevresel zorluk olarak tanımlanmaktadır.

4.2 BU ZORLUĞUN ÖNEMİ

Bu geçici durumların neden olduğu varyasyonlar, kullanıcının "ideal" ya da eğitim sırasında oluşturulan profilinden sapmasına yol açar ve kimlik doğrulama sistemleri açısından büyük bir zorluk teşkil eder. Sistem bu tür bir sapmayı güvenlik tehdidi olarak algılarsa, bu durum yanlış reddetmelere neden olabilir (FRR – False Rejection Rate artar). Öte yandan, sistem bu sapmalara karşı aşırı toleranslı hale getirilirse, sahte kullanıcıların kabul edilmesi riski doğar (FAR – False Acceptance Rate artar).

Bu problem özellikle serbest metin senaryolarında kritiktir çünkü kullanıcı tarafından yazılan içerik önceden bilinmez ve varyasyonu yönetmek daha zordur. Sürekli doğrulama sistemlerinde, kullanıcı uzun süre boyunca izlendiği için bu geçici durumların etkisi daha belirgin hale gelir. Bazı çalışmalar, statik doğrulama sistemlerinin sınırlı ve önceden tanımlı girdilere dayandığını, dinamik doğrulama sistemlerinin ise tüm etkileşimi göz önünde bulundurduğunu belirtmektedir. Ayrıca, mobil sürekli doğrulama sistemlerinde kontrolsüz ve değişken veri edinim koşulları, süreci daha da zorlaştırmaktadır.

4.3 LİTERATÜRDE BU ZORLUĞUN ELE ALINIŞI VE ARAŞTIRMA YÖNLERİ

4.3.1 Etkinin Anlaşılması ve Ölçülmesi

Gelecekteki çalışmalar, stres, yorgunluk ve dikkat dağınıklığı gibi geçici durumların, tuş basılı tutma süresi, tuşlar arası gecikme süresi ve digram zamanlaması gibi tuş vuruş özelliklerine olan etkilerini nicel olarak ölçmeye odaklanabilir (Revett et al., 2008). Banerjee & Woodard (2012),

4.3.2 Güçlü Temeller Üzerine Modeller Geliştirilmesi

Davranışsal değişkenliğin etkisini azaltmak için yeni makine öğrenmesi yaklaşımları veya birleştirilmiş sınıflayıcı modeller geliştirilebilir. Farklı sınıflayıcılardan gelen skorların birleştirilmesi, sistemin dayanıklılığını

artırabilir. (Killourhy & Maxion (2009), farklı sınıflayıcıların davranışsal varyasyonlara karşı gösterdiği dayanıklılığı karşılaştırmıştır.

4.3.3 Adaptif Öğrenme Stratejilerinin Uygulanması

Adaptif biyometrik sistemler, zaman içinde kullanıcının doğal varyasyonlarını öğrenebilir ve kimlik doğrulama şablonlarını dinamik olarak güncelleyebilir. Bu tür sistemlerin değerlendirilmesi için IUSR (Impostor Update Selection Rate) ve GUMR (Genuine Update Miss Rate) gibi performans ölçütleri önerilmiştir. (Morales et al. 2016) bu metrikleri, adaptif şablon güncelleme bağlamında tanıtmıştır.

4.3.4 Veri Ön İşleme Yöntemleri

Geçici durumların neden olduğu değişkenlik, veri normalizasyonu veya birleştirme teknikleri ile azaltılabilir. Örneğin, ardışık tuş vuruşlarının ortalamasının alınması sınıflandırma stabilitesini artırabilir. (Monaco et al. 2015), tuş dizilerinin pencereleme yöntemiyle işlenmesinin sınıflandırma başarımını artırdığını göstermiştir.

4.3.5 Dayanıklı (Robust) Özelliklerin Belirlenmesi

Araştırmalar, geçici durumlardan daha az etkilenen veya bu durumlara özgü örüntüleri yakalayabilen tuş vuruş özelliklerini belirlemeyi hedefleyebilir. Bazı yaklaşımlar, meşru kullanıcıların varyasyonlarının sahtekâr kullanıcılarla ne ölçüde örtüştüğünü ölçmek için özellik puanlama yöntemleri önermektedir. (Teh et al. 2013), bu tür sağlam özniteliklerin istatistiksel değerlendirmesini ele almıştır.

SONUÇ VE ÖNERİLER

KAPSAMLI DEĞERLENDİRME

Bu çalışma, geleneksel kimlik doğrulama yöntemlerinin güvenlik açıklarını incelemiş ve davranışsal tabanlı bir biyometrik yöntem olan "tuş vuruş dinamiklerinin" teorik temellerini ele almıştır. Araştırmalarda gerçekleştirilen deneyler sonucunda, Eşit Hata Oranı (Equal Error Rate - EER) gibi performans metriklerinde 0.0066 gibi oldukça düşük değerler elde edildiği görülmüştür. Bu durum, hem doğruluk hem de günlük kullanım açısından tuş vuruş dinamiklerinin gerçek dünya ortamlarında uygulanabilirliğini ortaya koymaktadır.

Destek Vektör Makineleri (SVM), Konvolüsyonel Sinir Ağları (CNN) ve Rastgele Orman (RF) gibi çeşitli sınıflandırma algoritmaları karşılaştırılmış ve sonuçlar, derin öğrenme temelli mimarilerin geleneksel yaklaşımlara kıyasla daha üstün performans sergilediğini ortaya koymuştur. Ancak bu modellerin, mobil ya da gömülü sistemler gibi kaynak kısıtlı ortamlardaki uygulanabilirliği, hesaplama gücü, yapısal karmaşıklık ve enerji tüketimi gibi etmenler göz önünde bulundurularak daha ayrıntılı şekilde değerlendirilmelidir.

GELENEKSEL YÖNTEMLERLE KARŞILAŞTIRMALI ANALİZ

Geleneksel bilgi temelli kimlik doğrulama paradigmaları (şifreler, PIN'ler, token'lar gibi), yetkisiz erişimlere karşı sınırlı koruma sunmaktadır. Bu tür kimlik bilgileri çoğu zaman tahmin edilebilir ya da ele geçirilebilir niteliktedir. Buna karşın, tuş vuruş dinamikleri, bireylerin yazma biçimlerindeki motor davranış örüntülerini analiz ederek kimlik doğrulama sağlar ve taklit edilmesi son derece zordur. Bu bulgu, Morales ve arkadaşlarının (2016) düzenlediği Keystroke Biometrics Ongoing Competition kapsamında sistemlerin %5.32'ye kadar düşük EER değerleri elde etmesiyle de desteklenmiştir.

Ayrıca, shoulder-surfing (yan bakışla izleme) ve keylogging (tuş kaydedici) saldırılarına karşı dayanıklılık, özellikle Zhou et al. (2023) tarafından mobil cihazlarda yapılan dokunmatik tabanlı çalışmalarda gözlemlenmiştir. Bu nedenle, tuş vuruş dinamiklerinin geleneksel yöntemlerle birlikte kullanılması, sistem güvenliğini anlamlı ölçüde artırmaktadır.

GÜVENLİK VE MAHREMİYET HUSUSLARI

OWASP Authentication Cheat Sheet rehberine göre, kimlik doğrulama sistemlerinin yalnızca teknik doğruluk açısından değil, aynı zamanda kullanıcı mahremiyetine gösterdiği saygı bakımından da değerlendirilmesi gerekir. Bu bağlamda, tuş vuruş dinamikleri, parmak izi veya yüz fotoğrafı gibi fiziksel biyometrik veriler yerine kullanıcının etkileşim örüntülerine dayandığı için mahremiyet açısından daha avantajlı kabul edilmektedir.

Bu davranışsal veriler, anonimleştirilmiş biçimde saklanabilir ve kullanıcıdan ek bir donanımsal giriş gerektirmediği için daha esnek ve sürdürülebilir veri koruma politikalarına olanak tanır. Ancak zamanla yazım davranışı yeniden tanımlanabilir hâle gelebileceğinden, veri minimizasyonu ve yaşam döngüsü yönetimi gibi stratejilerin uygulanması, GDPR gibi düzenlemelere uyum açısından gereklidir.

TUŞ VURUŞ DİNAMİKLERİNDE GELECEĞE YÖNELİK GELİŞMELER

Araştırma sonuçları, tuş vuruş dinamikleri sistemlerinin çok çeşitli uygulamalarda etkili biçimde kullanılabileceğini göstermektedir:

Mobil Cihazlar: Kullanıcının yürürken, otururken veya uzanırken gerçekleştirdiği etkileşim farklılık gösterdiğinden, bağlamsal farkındalığa sahip adaptif modellerin geliştirilmesi önemlidir.

Sürekli Doğrulama (Continuous Authentication): Kullanıcının oturum süresince yazım desenlerinin sürekli izlenmesi, uzun oturumlar sırasında

masquerade attack (başkasının yerine geçme saldırıları) gibi tehditleri tespit edebilir.

İki Faktörlü Kimlik Doğrulama (2FA): Tuş vuruş verisinin OTP gibi güvenlik protokolleriyle entegre edilmesi, güvenliği artırmanın yanında kullanıcı deneyimini de geliştirir. Ahmed Wahab et al. (2023) tarafından yapılan bir kullanıcı çalışmasında, bu entegrasyonun giriş süresini kısalttığı ve güvenliği artırdığı gösterilmiştir.

Donanım Kısıtlı Sistemler: Donanım gücü sınırlı olan sistemler için optimize edilmiş tuş vuruş modelleri, etkili ve uygun maliyetli güvenlik çözümleri sağlayabilir.

SINIRLILIKLAR VE GELECEKTEKİ ARAŞTIRMA YÖNLERİ

Bu araştırmada kullanılan deneysel tasarım, sabit metin (fixed-text) doğrulama yaklaşımına dayanmaktadır. Bu nedenle, modelin serbest metin (free-text) senaryolarındaki gücü ölçülememiştir. Morales et al. (2016) da benzer şekilde sabit metin kullanmış ve bunun mevcut literatürde yaygın bir eksiklik olduğunu belirtmiştir. Bu nedenle, gelecekte yapılacak çalışmaların serbest metin veri setlerini kullanması, yöntemin gerçek dünya uygulamalarıyla daha uyumlu hale getirilmesini sağlayacaktır.

SONUÇ

Bu çalışma üç ana bulguyu vurgulamaktadır. İlk olarak, ML ve DL yaklaşımlarının karşılaştırılması, klasik ML modellerinin küçük veri kümelerinde kabul edilebilir bir doğruluk sağlarken, RNN'ler ve Transformatörler gibi DL mimarilerinin, özellikle serbest metin senaryolarında Eşit Hata Oranlarını (EER) önemli ölçüde azalttığını göstermektedir. İkincisi, ML ve DL'yi birleştiren hibrit modeller en iyi dengeyi sağlayarak %98'in üzerinde doğruluk oranlarına ulaşır ve EER'yi %50'ye kadar azaltır, böylece sağlamlık ve kullanılabilirlik açısından bağımsız yöntemlerden daha iyi

performans gösterir. Üçüncüsü, pratik uygulamalar, tuş vuruşu dinamiklerinin OTP'lere olan bağımlılığı azaltarak ve kullanıcı sürtünmesini düşürerek çok faktörlü kimlik doğrulama (MFA) ve sürekli kimlik doğrulamaya anlamlı bir şekilde katkıda bulunduğunu göstermektedir.

Geleceğe bakıldığında, iki umut verici araştırma yönü öne çıkmaktadır. İlk olarak, gizlilik koruma teknikleriyle birleştirilen federatif öğrenme, ham biyometrik verileri ifşa etmeden güvenliği artırabilir ve mevzuata uygunluğu sağlayabilir. İkincisi, açıklanabilir yapay zeka (XAI) ile zenginleştirilmiş çok modlu kimlik doğrulama, şeffaf karar verme sağlarken yorumlanabilirlik, adalet ve dayanıklılık sorunlarını da çözebilir.

Özetle, bu alanın geleceği tek başına bir çözüm olarak tuş vuruşu dinamiklerinde değil, çok modlu, uç özellikli ve XAI destekli kimlik doğrulama sistemlerinde yatmaktadır.

KAYNAKLAR

Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Banerjee, S., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. Journal of Pattern Recognition Research, 7(1), 116–139. https://doi.org/10.13176/11.438

Barra, S., Castiglione, A., Narducci, F., De Marsico, M., & Nappi, M. (2019). Biometric data on the edge for secure, smart and user tailored access to cloud services. Future Generation Computer Systems, 101, 534–541. https://doi.org/10.1016/j.future.2019.06.019

Bhatia, A., & Hanmandlu, M. (2017). Keystroke dynamics based authentication using information sets. Journal of Modern Physics, 8(9), 1557–1583. https://doi.org/10.4236/jmp.2017.89094

Hazan, I., Margalit, O., & Rokach, L. (2019). Securing keystroke dynamics from replay attacks. Applied Soft Computing, 85, 105798. https://doi.org/10.1016/j.asoc.2019.105798

Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, 125–134. https://doi.org/10.1109/DSN.2009.5270346

Lien, C.-W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of IoT: A survey. ACM Computing Surveys, 56(1), Article 14. https://doi.org/10.1145/3603705

Liu, W., Chen, M., Jiang, X., Chen, W., Zeng, S., Ren, Z., Guo, H., & Yu, H. (2025). Dynamic keystroke-password recognition based on piezoelectric-triboelectric coupling sensor array with crosstalk-free for authentication system. Nano Energy, 136, 110667. https://doi.org/10.1016/j.nanoen.2025.110667

Morales, A., Fierrez, J., Tolosana, R., Ortega-Garcia, J., Galbally, J., Gomez-Barrero, M., Anjos, A., & Marcel, S. (2016). Keystroke biometrics ongoing competition. IEEE Access, 4, 7736–7746. https://doi.org/10.1109/ACCESS.2016.2626718

Revett, K. (2009). Behavioral biometrics: A remote access approach. Springer. https://doi.org/10.1007/978-1-84882-385-3

Roy, S., Saha, A., & Mahata, A. (2022). A systematic literature review on latest keystroke dynamics based models. IEEE Access, 10, 92191–92235. https://doi.org/10.1109/ACCESS.2022.3197756

Saini, B. S., Chauhan, M., & Mahajan, R. (2020). A three-step authentication model for mobile phone user using keystroke dynamics. IEEE Access, 8, 125909–125920. https://doi.org/10.1109/ACCESS.2020.3008019

Salim, U. T., Qaddoori, S. L., & Allayla, N. M. (2024). Building a keystroke dynamic recognition system using an improved accelerated method. Journal of Optimization & Decision Making, 3(1), 389–397.

Sitová, Z., Zhao, H., Šeděnka, J., Yang, G., Peng, G., Zhou, Y., & Xu, K. (2015). HMM-based behavior biometrics for continuous authentication of smartphone users. IEEE Transactions on Information Forensics and Security, 11(4), 877–892. https://doi.org/10.1109/TIFS.2015.2503266

Stylios, I., Chatzis, S., Thanou, O., & Kokolakis, S. (2023). Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues. Computers & Security, 132, 103363. https://doi.org/10.1016/j.cose.2023.103363

Wahab, A. A., Hou, D., & Schuckers, S. (2023). A user study of keystroke dynamics as second factor in web MFA. Proceedings of the 13th ACM Conference on Data and Application Security and Privacy (CODASPY ’23), 1–12. https://doi.org/10.1145/3577923.3583642

Wahab, A. A., Hou, D., & Schuckers, S. (2023). 2D-2FA: A new dimension in two-factor authentication. Proceedings of the 13th ACM Conference on Data and Application Security and Privacy (CODASPY ’23), 1–8. https://doi.org/10.1145/3577923.3583642

Wang, Y., Wu, C., Zheng, K., & Wang, X. (2019). Improving reliability: User authentication on smartphones using keystroke biometrics. IEEE Access, 7, 26218–26232. https://doi.org/10.1109/ACCESS.2019.2891603

Yılmaz, E., & Can, Ö. (2023). Keystroke biometric data for identity verification: Performance analysis of machine learning algorithms. Journal of Computer Science (IDAP 2023), 143–150. https://doi.org/10.53070/bbd.1345519

Zhou, L., Wang, K., Lai, J., & Zhang, D. (2023). A comparison of a touch-gesture- and a keystroke-based password method: Toward shoulder-surfing resistant mobile user authentication. IEEE Transactions on Human-Machine Systems, 53(2), 303–315. https://doi.org/10.1109/THMS.2023.3236328

ÖZGEÇMİŞ