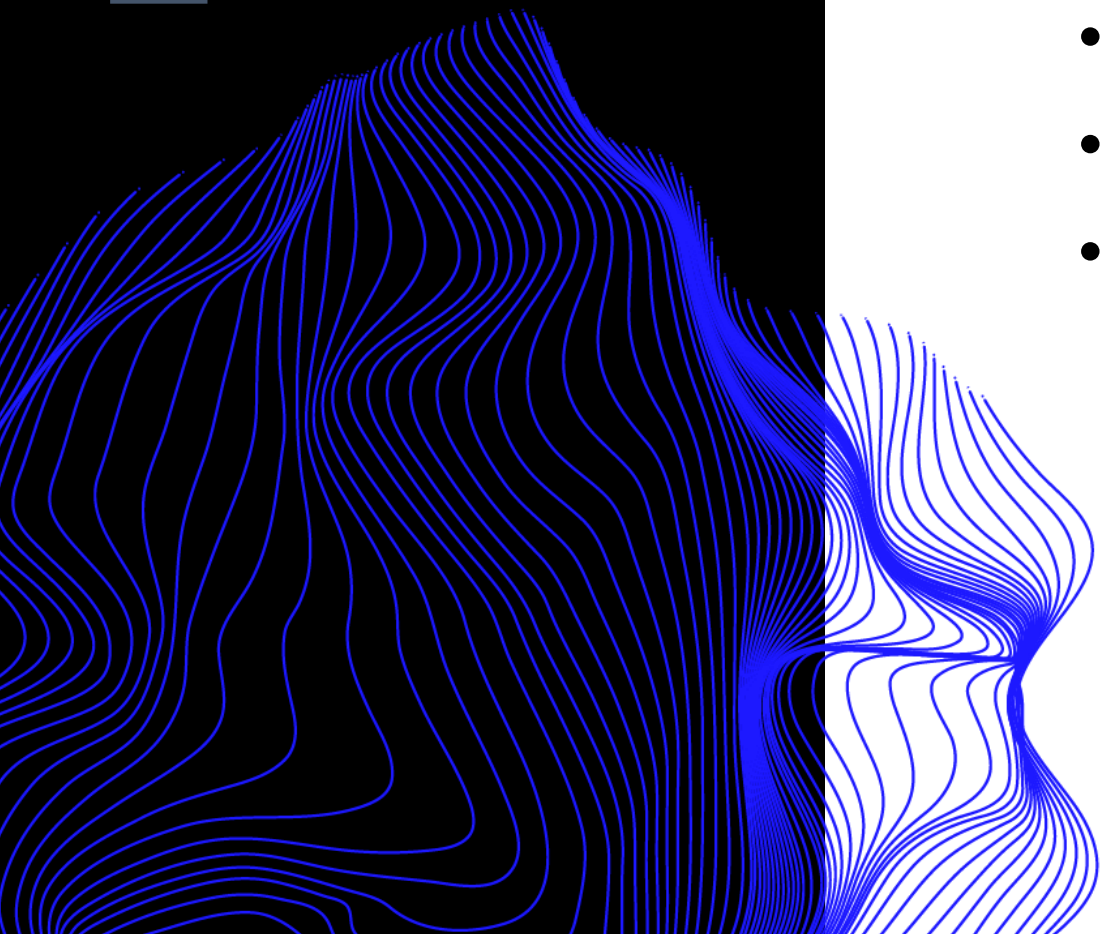
KOBIL

Müşterini Tanı (Know Your Customer)

Yapay Zeka Arf Ödülleri

KOBİL Teknoloji A.Ş.

İçindekiler



Müşterini Tanı

Müşterini Tanı (KYC - Know Your Customer) sistemleri, bir bireyin kimliğini güvenilir ve doğrulanabilir şekilde tespit etmeyi amaçlayan süreçlerdir. Bu sistemler, kullanıcıların kimlik bilgilerini doğrulamak ve sahtecilik girişimlerini önlemek için çeşitli teknolojik modüllerden oluşur. KYC süreçlerinde sıklıkla kullanılan modüller şunlardır:

1. MRZ ve OCR Tabanlı Kimlik Bilgisi Çıkarımı

Kimlik belgelerinin (pasaport, kimlik kartı vb.) makine tarafından okunabilir bölgelerinden (MRZ - Machine Readable Zone) alanından optik karakter tanıma (OCR) teknolojisiyle bilgilerin alınması.

2. NFC ile Elektronik Kimlik Doğrulama

Elektronik kimliklerin (eID) NFC (Yakın Alan İletişimi) teknolojisi kullanılarak doğrulanması ve belgelerdeki güvenlik sertifikalarının kontrol edilmesi ve bilgilerin elde edilmesi.

3. Yüz Doğrulama (Face Recognition)

Kullanıcının yüz verilerinin doğrulanarak kimlik belgesindeki fotoğrafla eşleştirilmesi.

4. Canlılık Denetimi (Liveness Detection)

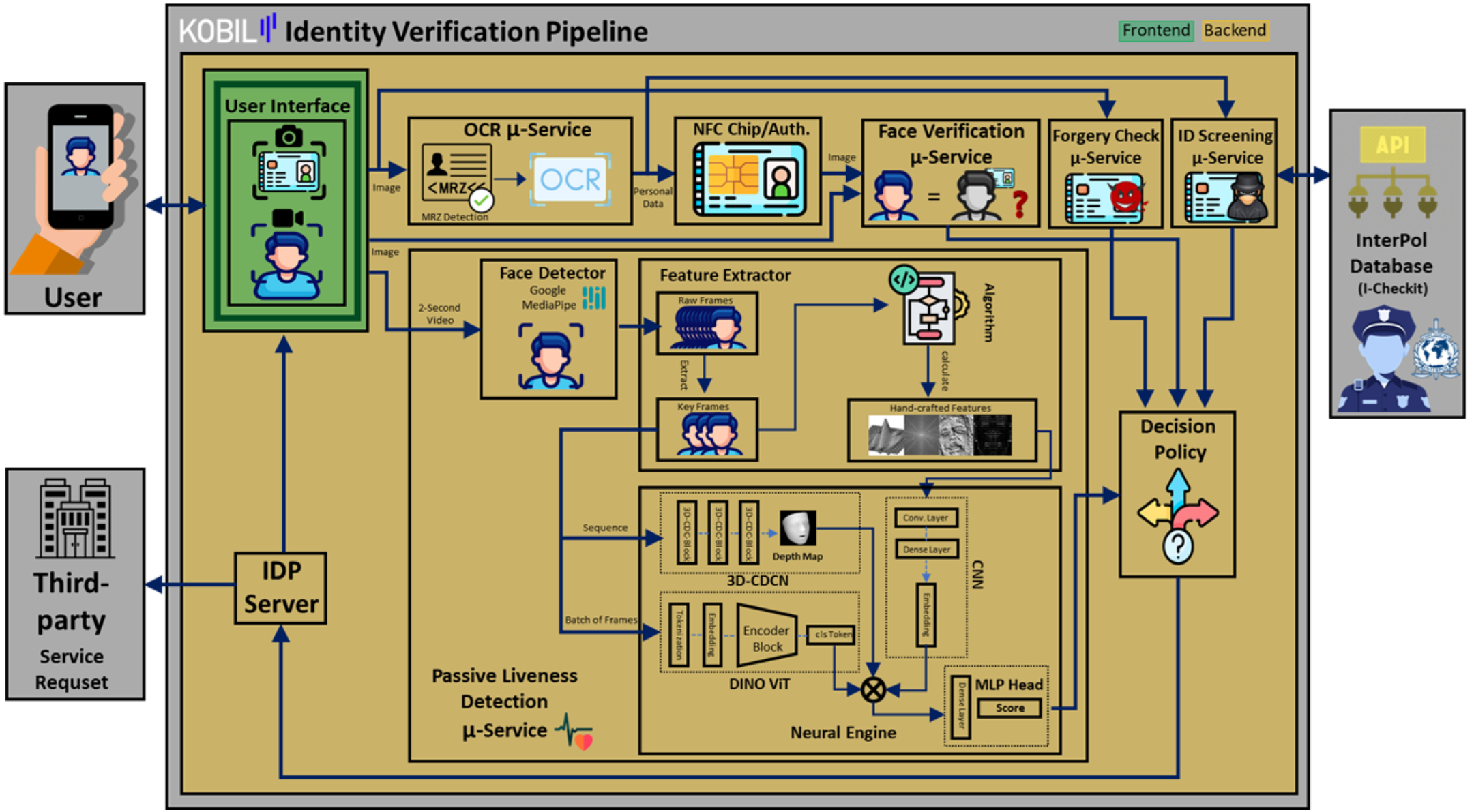
Kullanıcının gerçek bir kişi olduğunu ve statik bir görüntü ya da video kullanılmadığını doğrulamak için aktif ve pasif canlılık kontrol yöntemlerinin uygulanması.

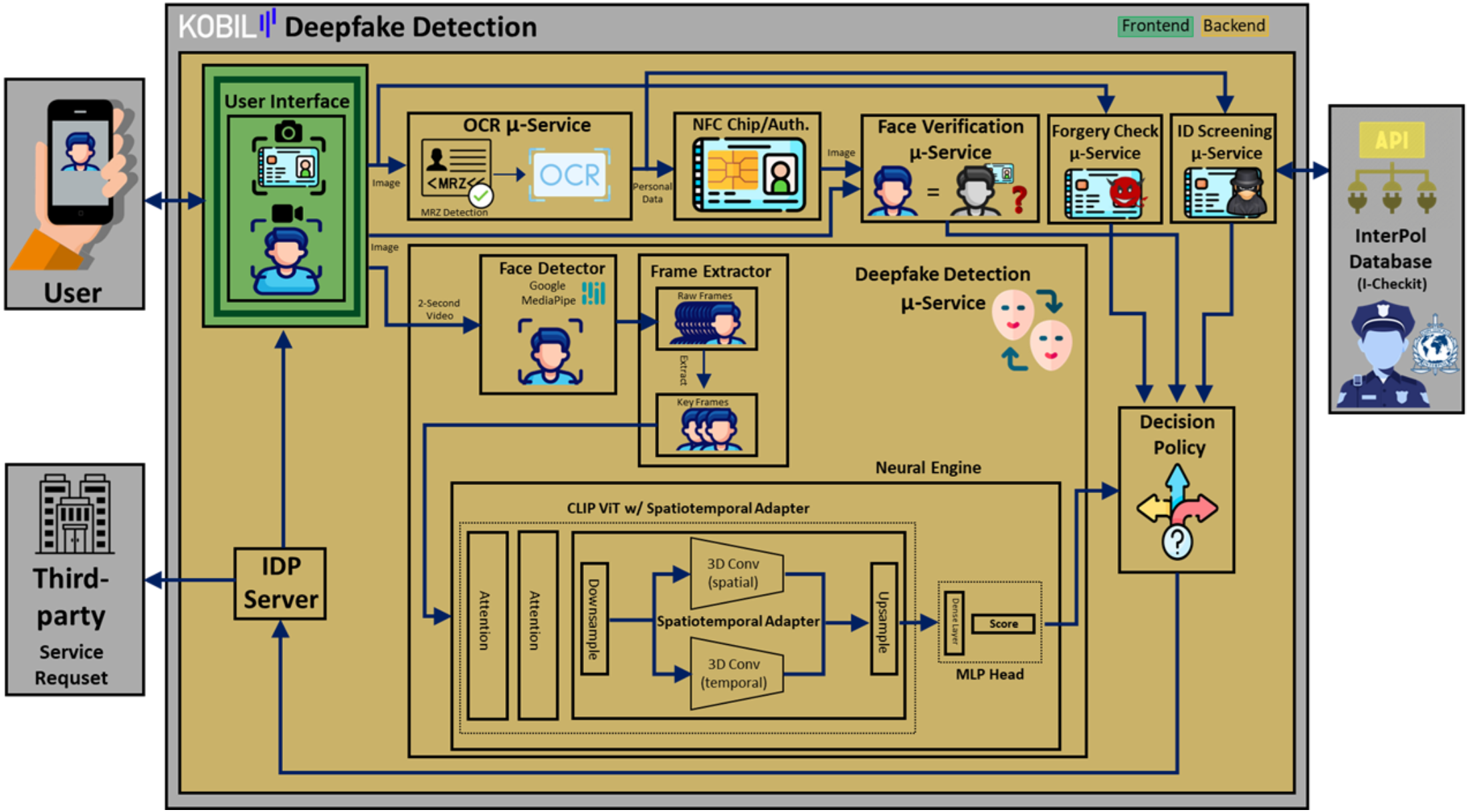
İş Planı

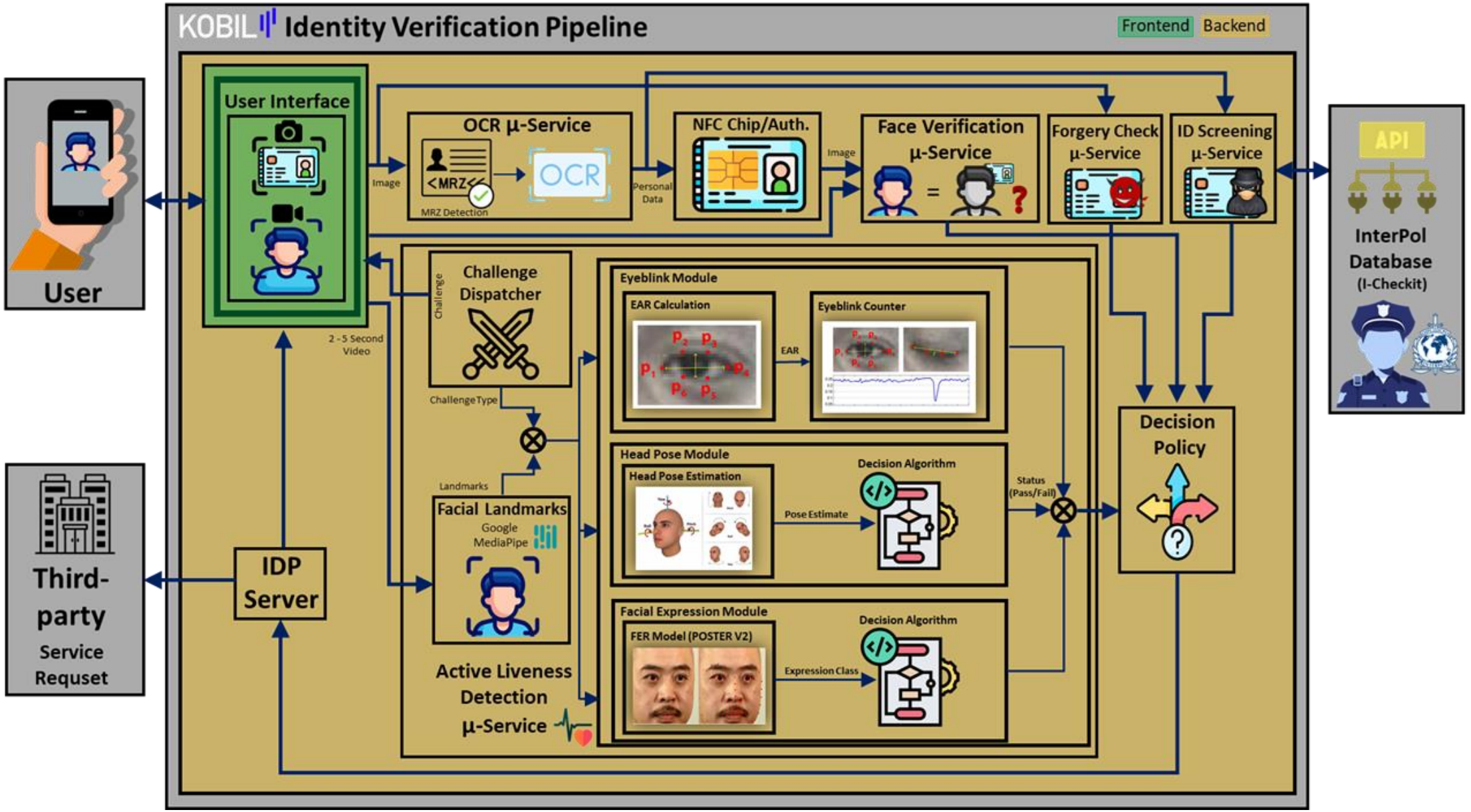
FİRMA ADI		KOBİL Teknoloji A.Ş.
PROJE ADI		Müşterini Tanı / KİMLİK TANILAMA SİSTEMLERİ

SIRA	NO	FAALİYETLER	2021/2				2022/1						2022/2						2023/1						2023/2							
			9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	1	**Mobil cihazlar kullanımıyla yüz tanıma ve canlılık testi sisteminin geliştirilmesi**																														
2	1.1	Yüz tanıma ve canlılık testi yöntem alternatiflerinin araştırılması																														
3	1.2	Yüz tanıma ve canlılık testi yöntem belirleme ve yöntem deneyleri için ön hazırlık																														
4	1.3	Yüz tanıma ve canlılık testi yöntem gerçekleme sonrası oluşan deneysel amaçlı yazılım bileşenleri ve deneyleri																														
5	1.4	Yüz tanıma ve canlılık testi yöntemleriyle ilgili iyileştirmeler/ek yöntemlerin gerçeklemesi ile ortaya çıkacak deney amaçlı yazılım bileşenleri ve deneyleri																														
6	1.5	Yüz tanıma ve canlılık testi için üründe kullanılması kararlaştırılan yöntemlerin sahada çalışacak bileşen ve servisler olarak geliştirilmesi																														
7	1.6	Sahada kullanılmak üzere yüz yanıma ve canlılık testini gerçekleştirilen bileşenler/servislerin kodlanması																														
8	1.7	Yüz tanıma ve canlılık testini gerçekleştirmek üzere canlılık testi yapan bileşenlerin testleri																														
9	1.8	Sahada kullanılmak üzere yüz tanıma ve canlılık testini gerçekleştirilen doğrulanmış bileşenler/servislerin belirlenmesi																														
10	1.9	Yöntemler ve bileşenlerde yapılması gerekli iyileştirmeleri içeren raporlar																														
11	2	**Mobil uç cihazlardan anlık veri alma ve sunucu etkileşimi sisteminin geliştirilmesi**																														
12	2.1	Cihazlara göre veri elde etme ve uygulamanın işleyişindeki farklılıkların ortaya konulmasına yönelik analiz																														
13	2.2	Uç cihazlardaki farklılıkları gözeterek uç cihaz uygulamalarının ve sunucu bileşenlerinin işleyişlerini tanımlayan teknik gereksinimlerin belirlenmesi																														
14	2.3	Uç cihazlardaki farklılıkları gözeterek uç cihaz uygulamalarının ve sunucu bileşenlerinin işleyişlerinin tasarımı																														
15	2.4	Uç cihazlardaki farklılıkları gözeterek geliştirilmiş uç cihaz uygulamaları ve sunucu bileşenlerinin kodlanması																														
16	2.5	Uç cihazlardaki farklılıkları gözeterek geliştirilmiş uç cihaz uygulamaları ve sunucu bileşenleri için testler																														
17	2.6	Uç cihazlardaki farklılıkları gözeterek geliştirilmiş ve doğrulanmış uç cihaz uygulamaları/bileşenleri ve sunucu bileşenlerinin geliştirilmesi																														
18	3	**Veri yönetimi, tümleşik sistem yönetimi ve raporlama alt sistemlerinin geliştirilmesi**																														
19	3.1	Dağıtık Veri Modelleme Analizi																														
20	3.2	Sistem/Bileşen Ayarlarının Yönetilmesi																														
21	3.3	Alt sistemlerin işleyişini ve gerçekleştirilen müşteri işlemlerini özetleyen/ayrıntılarıyla veren raporlama sisteminin geliştirilmesi																														
22	3.4	Dağıtık veri modelini, sistem bileşenlerinin yönetimini ve sistem işleyişinin raporlanmasını sağlayan alt sistemlerin tasarımı																														
23	3.5	Dağıtık veri modelini, sistem bileşenlerinin yönetimini ve sistem işleyişinin raporlanmasını sağlayan alt sistemlerinin kodlanması																														
24	3.6	Dağıtık veri modelini, sistem bileşenlerinin yönetimini ve sistem işleyişinin raporlanmasını sağlayan alt sistemlerinin test ve doğrulaması																														
25	4	**Entegrasyon, sistem doğrulama ve bütünsel iyileştirme**																														
26	4.1	Alt Sistemler arası ve Müşteri Sistemleriyle ve Üzerinde Çalıştığı Platformla Etkileşim																														
27	4.2	Alt Sistemler arası ve Dış Sistemlerle Etkileşimin Ayrıntılandığı Arayüz Tasarımı																														
28	4.3	Sistem Üst Seviye Tasarım																														
29	4.4	Sistemin Kurulumu Teknik İsterlerin belirlenmesi																														
30	4.5	Uçtan uca Sistem Test Dokümanının Hazırlanması																														
31	4.6	Sistemin Kurulum Mekanizmalarının kod yapıları																														
32	4.7	Uçtan uca Sistem Testleri																														
33	4.8	Uçtan uca Sistem doğrulama																														
34	4.9	Uçtan uca iyileştirmelerle ilgili Analiz																														

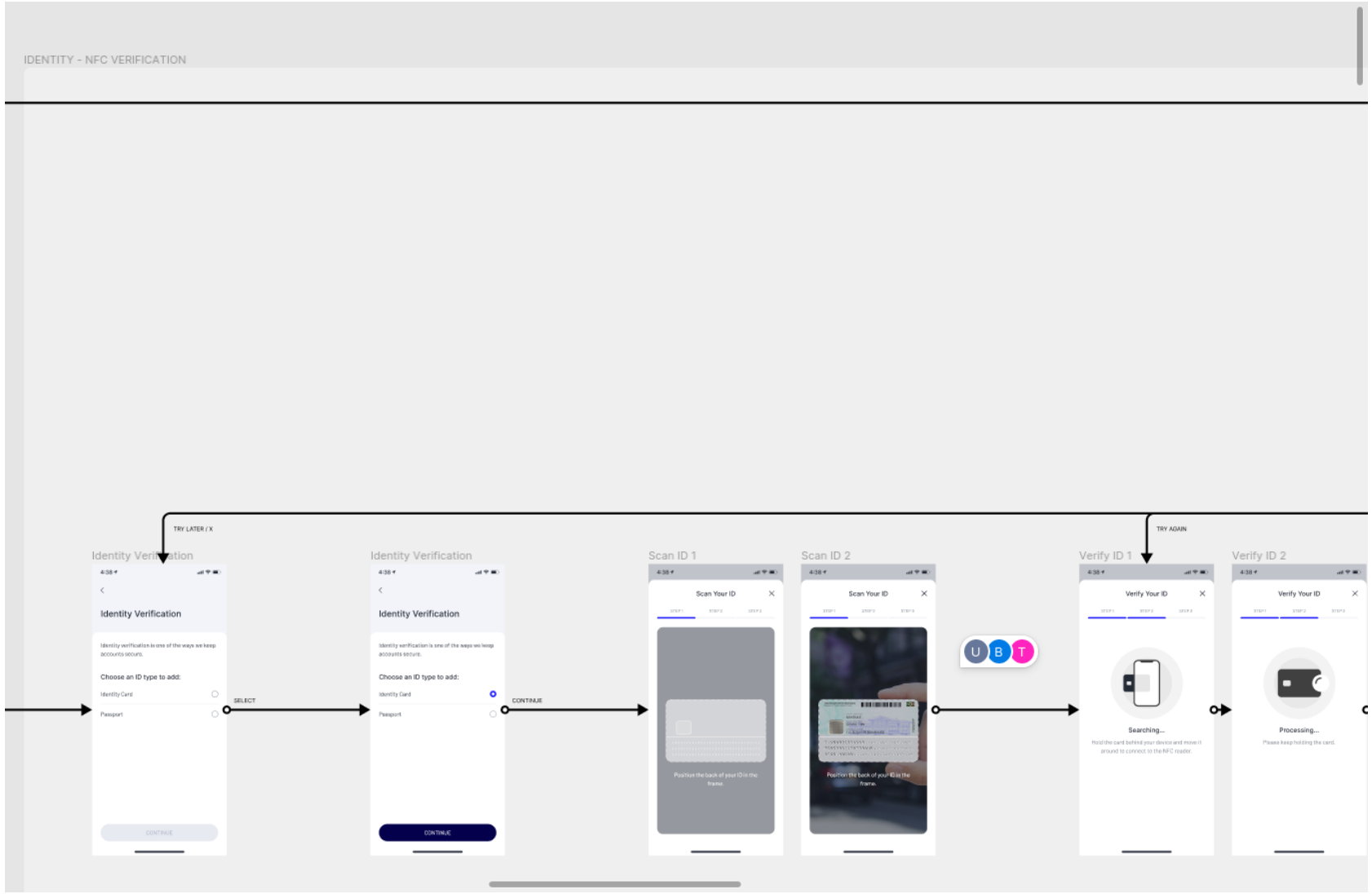
Model Blok Diyagramları

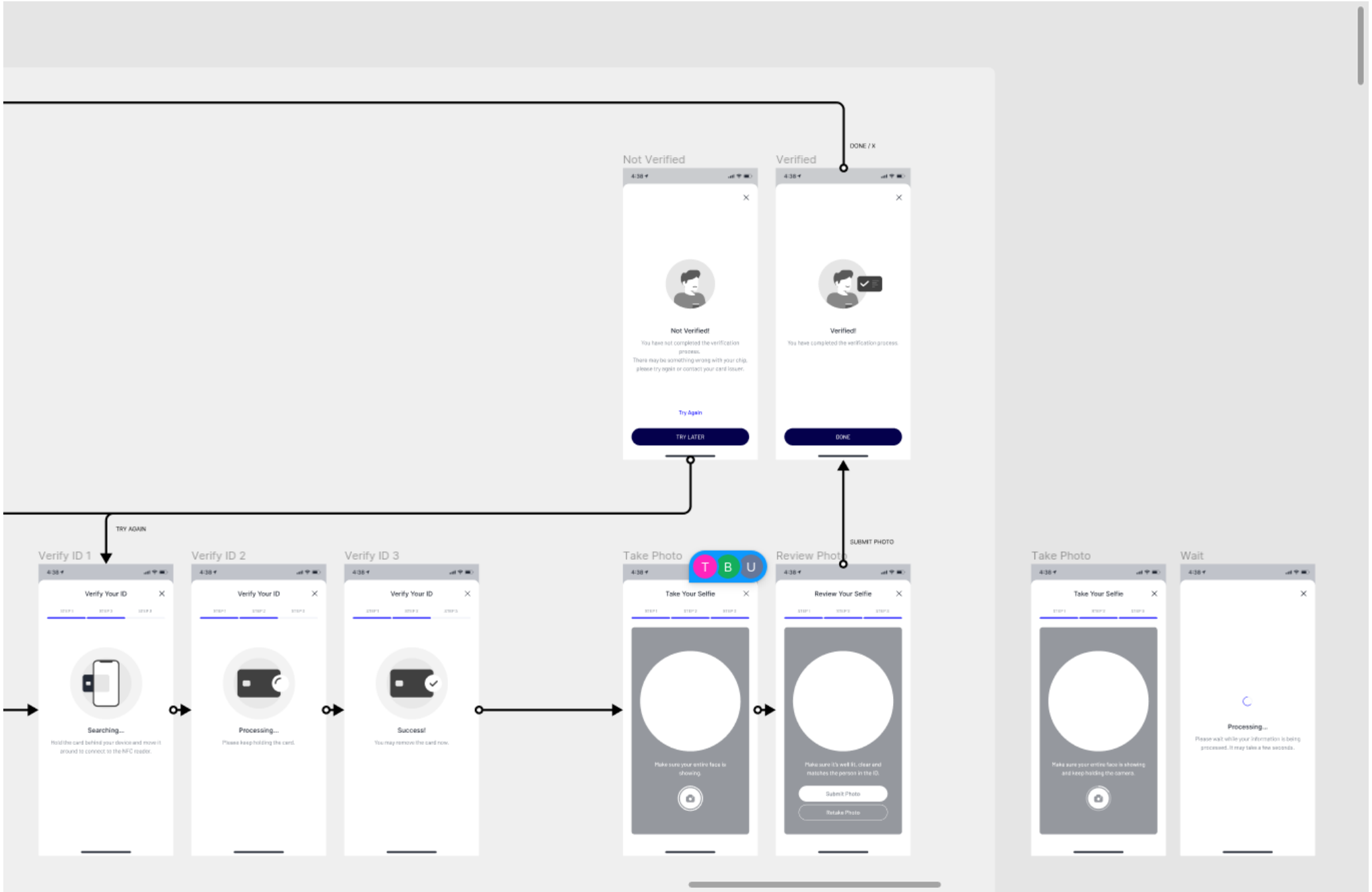


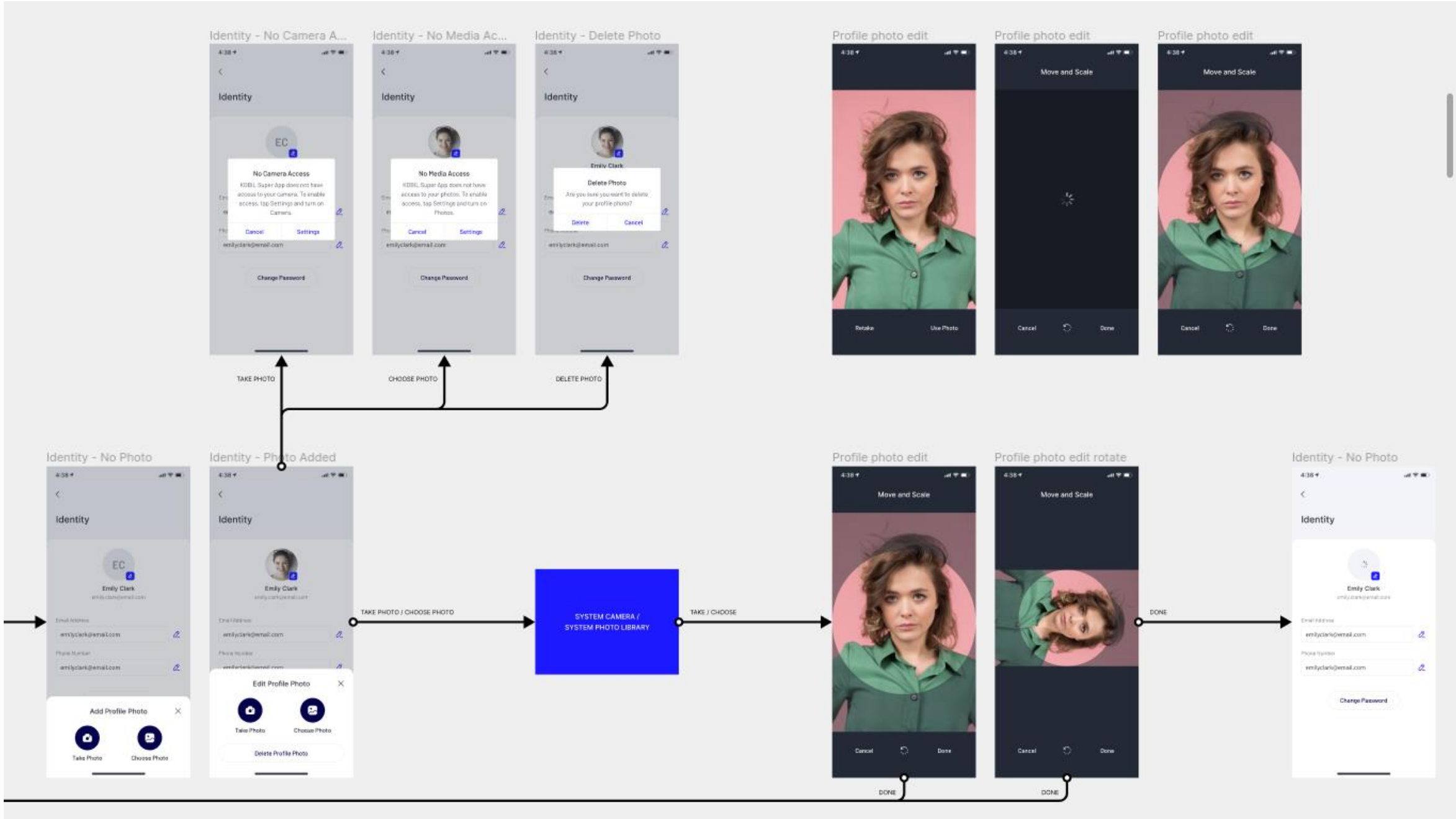

KOBIL Deepfake Detection
Frontend
Backend
User
User Interface
Image
OCR µ-Service
<MRZ
MRZ Detection
OCR
Personal Data
NFC Chip/Auth.
Image
Face Verification µ-Service
=
Forgery Check µ-Service
ID Screening µ-Service
API
InterPol Database (I-Checkit)
Image
2-Second Video
Face Detector
Google MediaPipe
Frame Extractor
Raw Frames
Extract
Key Frames
Deepfake Detection µ-Service
Neural Engine
CLIP ViT w/ Spatiotemporal Adapter
Attention
Attention
Downsample
3D Conv (spatial)
Spatiotemporal Adapter
3D Conv (temporal)
Upsample
Dense Layer
Score
MLP Head
Decision Policy
Third-party Service Requset
IDP Server


KOBIL Identity Verification Pipeline
Frontend
Backend
User
User Interface
2 - 5 Second Video
Image
OCR µ-Service
<MRZ<<
OCR
MRZ Detection
Personal Data
NFC Chip/Auth.
Image
Face Verification µ-Service
Forgery Check µ-Service
ID Screening µ-Service
API
InterPol Database (I-Checkit)
Challenge
Challenge Dispatcher
Challenge Type
Landmarks
Facial Landmarks
Google MediaPipe
Active Liveness Detection µ-Service
Eyeblink Module
EAR Calculation
EAR
Eyeblink Counter
Head Pose Module
Head Pose Estimation
Pose Estimate
Decision Algorithm
Facial Expression Module
FER Model (POSTER V2)
Expression Class
Decision Algorithm
Status (Pass/Fail)
Decision Policy
Third-party Service Requset
IDP Server

Akış Tasarımı




DONE / X
Not Verified
Verified
Not Verified!
You have not completed the verification process.
There may be something wrong with your chip, please try again or contact your card issuer.
Try Again
TRY LATER
Verified!
You have completed the verification process
DONE
TRY AGAIN
SUBMIT PHOTO
Verify ID 1
Verify ID 2
Verify ID 3
Take Photo
Review Photo
Take Photo
Wait
Verify Your ID
Searching...
Hold the card behind your device and move it around to connect to the NFC reader.
Processing...
Please keep holding the card.
Success!
You may remove the card now.
Take Your Selfie
Make sure your entire face is showing.
Review Your Selfie
Make sure it's well lit, clear and matches the person in the ID.
Submit Photo
Retake Photo
Make sure your entire face is showing and keep holding the camera.
Processing...
Please wait while your information is being processed. It may take a few seconds.


Identity - No Camera A...
Identity - No Media Ac...
Identity - Delete Photo
Profile photo edit
Profile photo edit
Profile photo edit
Identity
No Camera Access
No Media Access
Delete Photo
Are you sure you want to delete your profile photo?
Change Password
Move and Scale
Retake
Use Photo
Cancel
Done
TAKE PHOTO
CHOOSE PHOTO
DELETE PHOTO
Identity - No Photo
Identity - Photo Added
Profile photo edit
Profile photo edit rotate
Identity - No Photo
Add Profile Photo
Edit Profile Photo
Take Photo
Choose Photo
Delete Profile Photo
TAKE PHOTO / CHOOSE PHOTO
SYSTEM CAMERA / SYSTEM PHOTO LIBRARY
TAKE / CHOOSE
DONE
DONE
DONE

Gerçekleştirilen Başarı Ölçütleri

- Proje kapsamında hedeflenen başarı ölçütleri ve gerçeklenenler Tablo'da sunulmuştur. Her bir başarı ölçütü gelecek bölümlerde ayrıntılı olarak açıklanmıştır.

Başarı Ölçütü	Hedeflenen(%)	Gerçeklenen(%)
Yüz tanıma-sınıflama başarım metriği olarak Accuracy	>=0.95	**0.97**
Yüz tanıma-sınıflama başarım metriği olarak AUC*	>=0.90	**0.99**
Yüz tanıma canlılık testi - sınıflama metriği olarak Accuracy	>=0.90	**0.91**
Yüz tanıma canlılık testi - sınıflama metriği olarak AUC	>=0.86	**0.90**
Kullanıcı için özgünlük denetimi için maksimum süre	<= 45 saniye	**<=20 saniye**

- Her bir modül için çalışma süresi ve boyutları.

Modül	MRZ	OCR	NFC	Yüz Tanıma	Yüz doğrulama	Canlılık testi
Süre	40 ms	250 ms	7-8 sn	40 ms	200 ms	500 ms
Boyut	700 KB	1.7 MB	1 MB	300 KB	3.7 MB	5 MB

Belgelendirme

- **Yazılım Tescilimiz:**

Doğrulama Kodu : a37ab084-b283-4822-9c6b-2c1f8ea60202

T.C.
KÜLTÜR VE TURİZM BAKANLIĞI
TELİF HAKLARI GENEL MÜDÜRLÜĞÜ

BİLGİSAYAR PROGRAMLARINA İLİŞKİN KAYIT-TESCİL BELGESİ

Kayıt-Tescil No: 2023/8070 Kayıt-Tescil Tarihi: 3.02.2023

ESER BİLGİLERİ

Adı	: Süper Uygulamalar İçin Konfigüre Edilebilir Çok Adımlı Doğrulama
Türü	: Bilgisayar Programı, Veritabanı
Kullanıldığı Alanlar	: Süper Uygulamalar, Mobil Uygulamalar
Desteklenen İşletim Sistemleri	: Android, IOS
Dil Seçenekleri	Türkçe, İngilizce
Üretim Tarihi	: 1.08.2022
İlk Aleniyet Tarihi	: 1.11.2022

ESER SAHİPLERİ

Sıra No	İsim / Unvan	T.C. Kimlik / Vergi No	Eser / Hak Sahipliği Türü
1	KOBİL TEKNOLOJİ LİMİTED ŞİRKETİ	5640057447	Asıl Eser Sahibi

Bu belge başvuru sahibinin beyanı esas alınarak düzenlenmiştir.

Hak kurucu niteliğe haiz değildir, sadece eser sahibinin belirlenmesinde ispat kolaylığı sağlar.

Serhat DALGIÇ
Bakan a.
Daire Başkanı

➢ Patent Başvurumuz:

T.C.
TÜRK PATENT VE MARKA KURUMU
Patent Dairesi Başkanlığı

Sayı : E-39616753-110-230021159 06.01.2023
Konu : Patent Yazısı - 2022/021339 Numaralı Başvuru

ERDEM KAYA (ERDEM KAYA PATENT VE DAN. A.Ş.)

İlgi : 29/12/2022 tarihli, 2022/021339 numaralı ve TP22-1884 referanslı başvurunuz.

İlgide kayıtlı talebiniz ekindeki patent başvurunuz Kurumumuzca alınmış olup, 29/12/2022 tarih ve 2022/021339 sayı ile Sicile kaydedilmiştir.

Söz konusu başvurunuz, 6769 sayılı Sınai Mülkiyet Kanununun 95 inci maddesinin üçüncü fıkrası ve anılan Kanunun Uygulanmasına Dair Yönetmeliğin 96 ncı maddesinin birinci fıkrası hükümleri uyarınca şekli şartlara uygunluk açısından incelenmiş ve bir eksikliğin olmadığı saptanmıştır.

Ayrıca, başvurunuzla birlikte araştırma talebinde bulunulmadığı görüldüğünden söz konusu Kanunun 96 ncı maddesinin birinci fıkrası ve anılan Kanunun Uygulanmasına Dair Yönetmeliğin 97 nci maddesinin birinci fıkrası hükümleri uyarınca **başvuru tarihinden itibaren on iki ay içinde araştırma ücretinin de ödenerek araştırma talebinde bulunulması** gerekmektedir. Aksi takdirde başvurunuz geri çekilmiş sayılacaktır.

İşbu yazıya konu talebi, Kurumumuzun Elektronik Başvuru Sistemi (epats.turkpatent.gov.tr) üzerinden, Benim Sayfam panelinde Başvuru Sonrası İşlemler menüsü altında yer alan "Araştırma Talebi" işlemini seçerek gerçekleştirebilirsiniz.

Öte yandan başvurunuzun korunması için gerekli olan yıllık ücretler üçüncü yıldan başlamak üzere her yıl vadesinde ödenir. Vade tarihi, başvuru tarihine tekabül eden ay ve gündür. Yıllık ücretler, vadesinde ödenmediği takdirde ek ücretle birlikte vadeyi takip eden altı ay içinde de ödenebilir. Yıllık ücretlerin bu süre içinde de ödenmemesi halinde başvuru geçersiz sayılır.

Başvuru tarihi veya varsa rüçhan tarihinden itibaren on sekiz aylık sürenin dolması veya bu süre dolmadan erken yayın talebiniz üzerine başvurunuz Bültende yayımlanır.

Saygılarımla.

İzlem Cansu TAŞOYAN
Kurum Başkanı a.
Sınai Mülkiyet Uzman Yardımcısı

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Adresi : https://belgedogrulama.turkpatent.gov.tr/bg.aspx?Id=71F5C8D5-1D6B-4301-955A-7F6605B8A7D7

Gani Mahallesi Hipodrom Caddesi No:13 (06560)
Yenimahalle / ANKARA
Telefon No: (0312) 303 1 303 Faks No : (0312) 303 11 73
İnternet Adresi www.turkpatent.gov.tr
Kep Adresi : tpe@hs01.kep.tr

Bilgi İçin: İzlem Cansu TAŞOYAN
Unvan:
Telefon No:
Eposta: izlemcansu.meclis@turkpatent.gov.tr

KOBIL TEKNOLOJİ LTD. ŞTİ. (Teknopark İstanbul)		Tarih: 10.01.2023
İşlem Tipi: Patent araştırma ve inc. talebi	**Başvuru Konusu:** super app	
Ülke: TÜRKİYE	**Başvuru No:** 2022/021339	**EKP Ref:** TP22-1884
Son Durum: Şekilsel İnceleme Tamamlandı	**Tamamlanma Yüzdesi:** 15	

Sayın **Deniz KUMLU**,

Yukarıda bahsedilen, 2022/021339 numaralı patentinizin şekilsel incelemesinin sorunsuzca tamamlanmış olduğunu bildirmekten memnuniyet duyarız. Bu aşamadan sonraki devam eden süreçte ilgili buluşunuzun Resmi Araştırma ve İnceleme talebi işlemlerinin yapılması gerekmektedir. Araştırma talebi işleminin başvuru tarihinden itibaren 12 ay içerisinde gerçekleştirmesi gerekmekte olup, aksi taktirde başvurunuz iptal olmaktadır.

Sürecin hızlı ilerlemesi için yasal sürenin sonuna kadar işlemin bekletilmemesini aynı zamanda araştırma ve inceleme işlemlerinin birlikte yapılmasını önermekteyiz. Bu aşamada sadece araştırma talebi işlemi istemeniz durumunda tarafımıza bildirmenizi rica ederiz.

Bu bilgiler doğrultusunda işlemin gerçekleştirilmesi için patent araştırma ve inceleme talebi harç ve hizmet bedeli KDV Dahil 5380,80 TL ödeme yapmanız gerekmektedir.

Not: 6769 sayılı SMK'nın "Çalışan Buluşlarına, Yükseköğretim Kurumlarında Gerçekleştirilen Buluşlara Ve Kamu Destekli Projelerde Ortaya Çıkan Buluşlara Dair Yönetmelik" inin Madde 7(2)'sinde belirtildiği gibi her hizmet buluşu için buluşçulara net asgari ücretten az olmayan bir "teşvik ödülü" ödemesi yapılması zorunlu hale geldi. Buluş, birden çok çalışan tarafından gerçekleştirilmişse teşvik ödülü buluşu yapanlar arasında katkı payları oranında bölüştürülebilmektedir. Bildirim tarihinden itibaren 2 ay içinde buluşçulara gerekli ödemenin yapılması gerekmektedir.

Herhangi bir sorunuz olması durumunda bizimle istediğiniz zaman irtibata geçebilirsiniz.

Konuyu bilginize sunar, iyi çalışmalar dileriz.

Erdem Kaya Patent A.Ş.

Patent Birimi

KOBIL TEKNOLOJİ LTD. ŞTİ. (Teknopark İstanbul)		Tarih: 22.11.2023
İşlem Tipi: Yurtdışı PCT başvurunuz yapıldı	**Başvuru Konusu:** super app	
Ülke: WIPO	**Başvuru No:** PCT/TR2023/051369	**EKP Ref:** YP23-312-WO
Son Durum: Başvuru Yapıldı	**Tamamlanma Yüzdesi:** 10	

Sayın **Deniz KUMLU**,

Yukarıda detayları verilen PCT başvurusu 22.11.2023 günü itibarıyla Türk Patent ve Marka Kurumu'na yapılmıştır. Ekte başvuru evrakları dikkatinize sunulmuştur.

Resmi başvuru numaranız PCT/TR2023/051369 şeklinde kaydedilmiştir.

Bundan sonraki sürece ilişkin bilgi ekteki süreç-maliyeti şemamızda dikkatinize sunulmuştur.

Konuyu bilginize sunar, iyi çalışmalar dileriz.

Erdem Kaya Patent A.Ş.

Yurtdışı İşlemler Birimi

➢ İSO Belgelerimiz:

NAVIGA CERTIFICATION

SERTİFİKA | ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

CERTIFICATE OF REGISTRATION

This certificate has been awarded to the company

KOBIL TEKNOLOJI LIMITED SIRKETI

Sanayi Mah. Teknopark Bulvari 7C K:3 34906 Pendik, ISTANBUL

To certify that the implemented Biometric Presentation Attack Detection Standart complies with

ISO/IEC 30107-3:2017

For the activities described below

ISO/IEC 30107-3:2017 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 1 on the Android phones and iPhones, 2D Print and 3D Scan

Certificate No.: **23500112**
Date of Certificate : **03.04.2023**
Expiry Date: **02.04.2025**

İstanbul, 3.04.2023

This certificate is valid for above address(es) and scope upon compliance with Naviga procedure(s), instruction(s) and the above mentioned standard and successful completion of regular surveillance audits.

The validity of this certificate can be checked through QR code by TURKAK database or TBDS certificate no. under QR code on www.navigaltd.com/sertifika-sorgulama webpage.

NAVIGA ULUSLARARASI BELGELENDİRME VE EĞİTİM HİZMETLERİ LTD. ŞTİ.
Yenibosna Merkez Mah. 29 Ekim Cad. No:35 Kat:1 Bahçelievler-İSTANBUL
Tel: 0212 482 9656 Fax: 0212 482 9424 www.navigaltd.com - info@navigaltd.com

FR.069 REV.04 10.03.2017

➢ Yayınlarımız:

A Novel BlazeFace Based Pre-processing for MobileFaceNet in Face Verification

Necmettin Bayar*, Kübra Güzel*, and Deniz Kumlu*
*Artificial Intelligence Department, KOBIL Systems, Istanbul, Turkey
necmettin.bayar@kobil.com

***Abstract*—Face verification is an important security step on mobile devices and many other systems, thus it has to work with high accuracy. Besides the importance of the accuracy in the face verification model, its weight and computational complexity play crucial roles especially in mobile devices. In this study, we aimed to provide novel contribution as pre-processing step for MobileFaceNet without affecting its accuracy. With this contribution, overall pipeline has smaller weight and faster inference time by comparison to the available pre-processing models for MobileFaceNet such as multi task cascaded convolutional neural network (MTCNN) and RetinaFace. The face verification test results show the superiority of our proposed model compared to the state-of-the-art models in terms of weight and speed.**

***Keywords*—BlazeFace; face verification; face alignment; facial landmarks; MobileFaceNet**

I. Introduction

Face verification (one-to-one process) and face recognition (one-to-many process) are popular in computer vision and image processing community. They are generally utilized for security purposes to identify or verify on-boarding (registration or login) people to certain application or system. In the last decade, there are huge increases in the number of mobile device users. Thus, many applications are developed which require face verification or recognition models for various purposes such as locking device screen, login to the secure application, mobile payment, banking application and many others can be given as examples of cases where face verification is required [1, 2].

Generally, face verification is mostly used by mobile devices, however it is also largely employed in embedded devices which are mostly used for security reasons in industrial application. Formerly, face verification was done by heavy deep convolutional neural networks (CNN) [3]. These networks have many parameters, which imply a huge number of model weights and higher computational times [1]. Since the mobile and embedded devices have limited storage capacity, and low computing power, these heavy CNN based approaches are not suitable for the mobile and embedded devices. On the other hand, using these heavy models in the mobile applications showed that the user experience reduces considerably.

To alleviate the size and computational time of the heavy models, lightweight and fast models are proposed. These models have fewer layers compared to older ones and using depth-wise separable convolution to achieve fast implementation on mobile devices [4]. MobileFaceNet is one of the common and frequently used face verification models on mobile devices. By comparing the many other light weight models, MobileFaceNet achieves higher accuracy and its size is only around 4 MB. Besides, it has 99.5% accuracy on well known labeled faces in the wild (LFW) dataset [4].

Face verification process begins with face detection stage. In the conventional MobileFaceNet, Multi Task Cascaded Convolutional Neural Network (MTCNN) is used for detection purposes and MTCNN also provides 5 facial points on the detected human face [5]. These facial points are used to align face image with respect to reference facial points. MobileFaceNet has different model types which contain different input sizes and the best result are obtained by 112x112 input size. In the input of MobileFaceNet, it requires faces that are aligned and resized to 112x112. Then, MobileFaceNet extracts embedding vectors from pre-processed input images [4].

In the final step, similarity of 2 embedding vectors are checked by cosine similarity metric. If the similarity is over the predefined threshold value, face verification process is completed successfully, otherwise verification process has failed. In order to detect facial landmarks MobileFaceNet uses MTCNN as mentioned before. MTCNN has 3 different sub-models, each of them having different roles for detection. However, using three different networks increases the computational complexity of the model. Some of the MobileFaceNet implementation uses RetinaFace instead of MTCNN. In their work, it is shown that RetinaFace outperforms MTCNN on the LFW and other datasets. Retinaface is single stage face detection model which does not contain two different mechanisms such as proposal and refinement. Thus, it is faster and lighter compared to MTCNN [6].

Recently proposed BlazeFace model is specifically tailored for face detection with landmarks in mobile graphical processing unit (GPU) implementation [7]. In this paper, authors aim to replace pre-processing part of the MobileFaceNet by using BlazeFace instead of MTCNN model. BlazeFace can detect faces in less than milliseconds and inference time does not change by size of the input image. Thus, by using BlazeFace instead of MTCNN can achieve lightweight and faster verification by removing the dependency to input image size [7].

The paper is organized as follows; in section I, related works for face detection and alignment are presented. Section II is dedicated to pre-processing step with MTCNN and RetinaFace models. In Section III, proposed methods are explained in detail and in Section IV experimental results are presented.

2022 45th International Conference on Telecommunications and Signal Processing (TSP) | 978-1-6654-6948-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/TSP55681.2022.9851255

Research Article

MobileMRZNet: Efficient and Lightweight MRZ Detection for Mobile Devices

Necmettin Bayar, Kubra Guzel and Deniz Kumlu

***Abstract*—The Machine Readable Zone (MRZ) is a standardized section found on identification documents (IDs) that adhere to the International Civil Aviation Association (ICAO) Document 9303. The MRZ region contains sensitive personal information about the document holder, and a portion of this information is utilized to establish communication between the passive chip within the ID and a mobile device via Near Field Communication (NFC) protocol. This communication is crucial as the data retrieved from the ID's chip is subsequently used in authentication steps such as face or fingerprint recognition. Thus, accurate detection of the personal information within the MRZ region is vital. In this research study, we propose a fast and lightweight approach for MRZ region detection called MobileMRZNet, which is based on the BlazeFace model. The MobileMRZNet architecture is specifically designed for mobile Graphical Processing Units (GPUs) and enables rapid and precise detection of MRZ regions. To train and evaluate the model, a dataset consisting of both simulated and real data was created using Turkish national IDs. The BlazeFace model was reconfigured and trained specifically for MRZ region detection. The detector, based on BlazeFace and trained on augmented real and simulated data, demonstrates excellent generalization capabilities for deployment with real IDs. Both qualitative and quantitative results confirm the superiority of our proposed method. The mean Intersection over Union (IoU) for the first frame, without utilizing any layout alignment for IDs, achieves an accuracy of approximately 81\%. For character recognition, the method achieves 100\% accuracy after three consecutive frames. The model operates in less than 10 milliseconds on a mobile device, and its size is around 400 KB, making it significantly fast, lightweight, and robust compared to any existing MRZ detection methods.**

Index Terms—**Biometric identification, Blazeface model, ID Cards, MRZ Detection, Travel Documents.**

I. Introduction

IDENTITY DOCUMENTS (IDs) play a vital role in ensuring national security and enabling citizens to engage in various activities such as voting, traveling, and accessing government and private sector benefits. The accurate verification of IDs allows governments to effectively monitor their citizens, identify illegal immigrants, prevent identity theft, track criminals, monitor terrorism activities, and identify individuals who may pose a risk to national security. Moreover, governments provide services specifically tailored to their citizens, and IDs serve as a means to streamline service delivery by ensuring that only eligible citizens receive these services, minimizing any potential errors or misuse by non-citizens.

When the brief history of IDs are checked, it is evident that they first appeared around 1876. However, they did not become widely accessible until the early 20th century [1]. The introduction of photographic IDs occurred in 1915, following the well-known Lody-Spy scandal [2]. Prior to 1985, there was no global standardization for IDs. It was in 1985 that ISO/IEC 7810 established standardized guidelines for the shape, size, and content of IDs, which were further refined in 1988 through ISO/IEC 7816. As technology advanced, radio frequency identification (RFID) chips were integrated into IDs, enabling the storage of sensitive personal information alongside biometric data like photographs and fingerprints. The most recent standards for IDs are defined by the International Civil Aviation Association (ICAO), and the majority of countries worldwide have aligned their ID systems with these standards [3].

The International Civil Aviation Organization (ICAO) document 9303 establishes the standardized guidelines for machine-readable travel documents, including national IDs, passports, and more. Presently, over 190 countries have adopted these standards and incorporate machine-readable zones (MRZs) within their respective IDs.

The MRZ is a specific section on IDs that contains sensitive personal information about the document holder. It is designed to streamline and expedite the scanning process for government-issued documents such as IDs and passports. The information within the MRZ can be read using optical character recognition (OCR) methods, such as the Tesseract OCR engine, as the characters in the MRZ region have a unique font called OCR-B. To enhance the accuracy and performance of the OCR engine, it is crucial to accurately detect the exact MRZ region on IDs beforehand [4].

The MRZ region is commonly used as part of the authentication process, with some of its information utilized to access the chip within IDs via the Near Field Communication (NFC) module of mobile phones. NFC comprises a collection of short-range wireless technologies that establish a reliable

Necmettin Bayar, is with Artificial Intelligence Department, Kobil Technology, Istanbul, Turkey, (e-mail: necmettin.bayar@kobil.com).
https://orcid.org/0000-0003-2367-828X

Kubra Guzel, is with Artificial Intelligence Department, Kobil Technology, Istanbul, Turkey, (e-mail: kubra.guzel@kobil.com).
https://orcid.org/0009-0002-8401-6983

Deniz Kumlu, is with Artificial Intelligence Department, Kobil Technology, Istanbul, Turkey, (e-mail: deniz.kumlu@kobil.com).
https://orcid.org/0000-0002-7192-7466
Manuscript received Jan 08, 2024; accepted Apr 15, 2024.
DOI: 10.17694/bajece.1416404

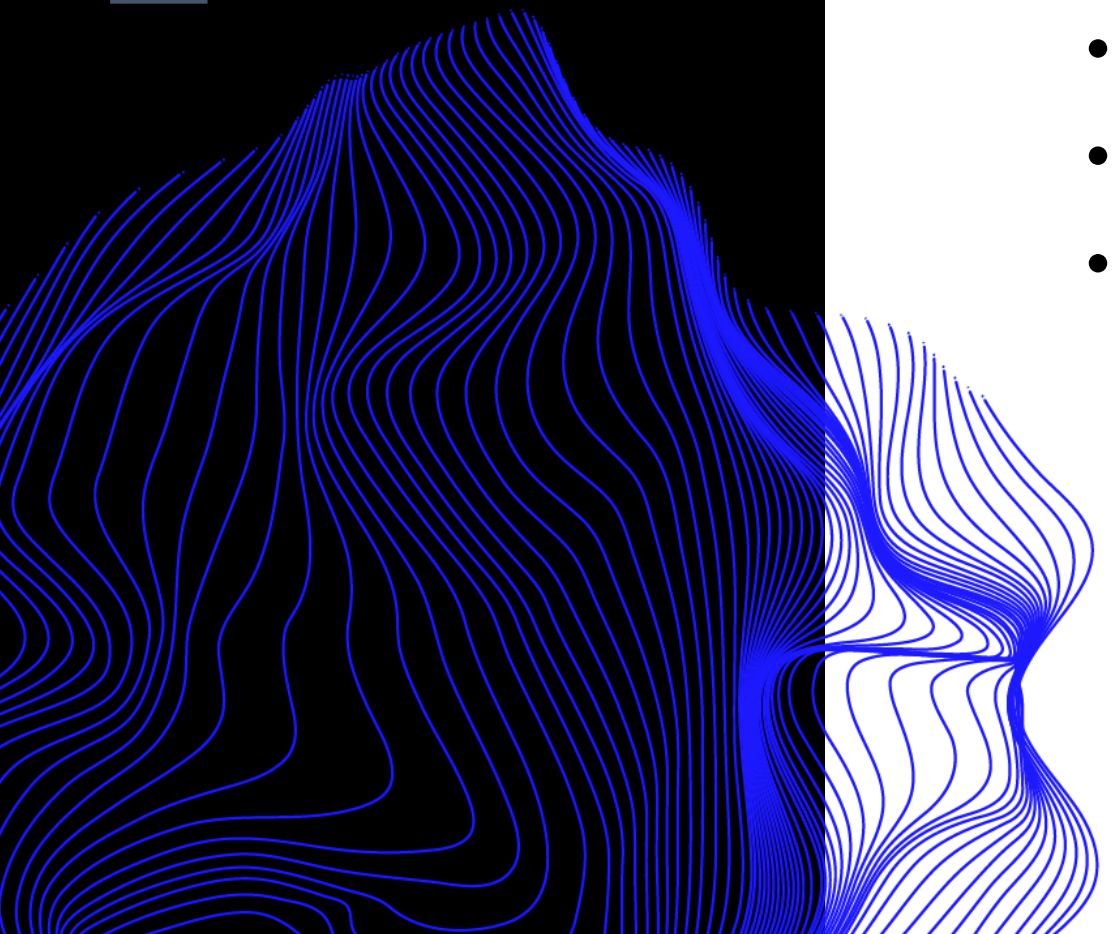
KOBIL

Davranış Analizi

Yapay Zeka Arf Ödülleri

KOBİL Teknoloji A.Ş.

İçindekiler



Davranış Analizi

Mobil cihazlardan elde edilen biyometrik davranış verilerine dayalı olarak sürekli doğrulama sistemleri geliştirilmiştir. Bu sistem, kullanıcının uygulama üzerindeki güvenliğini artırmayı hedefleyen, gerçek zamanlı analiz gerçekleştiren yapay zeka tabanlı bir çözümdür. Sürekli doğrulama mekanizması, kullanıcının kimliğini her 5 saniyede bir güncelleyerek güvenlik tehditlerini proaktif bir şekilde önler. Proje kapsamında yapılan çalışmalar, uluslararası bir konferansta yayımlanarak akademik alanda da katkı sağlamıştır.

Kullanılan Özellikler:

1. Klavye Vuruş Dinamikleri (Keystroke Dynamics)

Kullanıcının klavye üzerinde yazarken sergilediği ritim, hız ve basış süresi gibi benzersiz davranışların analizi.

2. Ekran Etkileşimleri (Screen Interactions):

Kullanıcının dokunmatik ekran üzerindeki kaydırma, dokunma ve tıklama gibi hareketlerinin izlenmesi ve değerlendirilmesi.

3. Sensör Verileri (Accelerometer, Magnetometer ve Gyroscope):

Cihazın hareket, yön ve manyetik alan verilerini ölçen sensörlerden toplanan verilerle kullanıcı davranışlarının tespiti.

- Bu özellikler, kullanıcı kimliğinin doğru ve güvenilir bir şekilde doğrulanması için güçlü bir temel oluşturur.

İş Planı

FİRMA ADI	KOBİL Teknoloji A.Ş.
PROJE ADI	Mobil Cihazlar Davranış Analizi

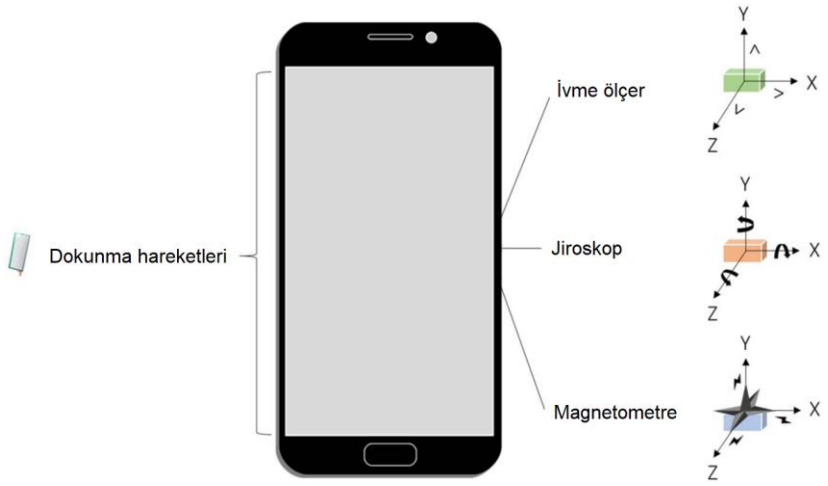
SIRA	NO	FAALİYETLER
1	1	**Davranış Biyometriğini Belirlemek için Sensör Verisi Toplama-Saklama Alt Sisteminin Geliştirilmesi ve Veri**
2	1.1	Açık kaynak sensör verilerini kullanarak, farklı sensörlerden gelen verilerin birbirilerine bağımlılıklarının analizini ve verilerin zamana bağlı değişiminin analizini içeren Teknik
3	1.2	Android platformlarında veri toplama ile ilgili Teknik Analiz Raporu
4	1.3	iOS platformlarında veri toplama ile ilgili Teknik Analiz Raporu
5	1.4	Açık kaynak sensör verilerini kullanarak, farklı sensörlerden gelen verilerin birbirilerine bağımlılıklarının analizini ve verilerin zamana bağlı değişiminin analizini içeren Teknik
6	1.5	Android Platformlarında veri toplama Alt Sistemi Tasarım Belgesi
7	1.6	iOS platformlarında veri toplama Alt Sistemi Tasarım Belgesi
8	1.7	Android Platformlarında veri Aktarma Alt Sisteminin Tasarım Belgesi
9	1.8	iOS Platformlarında veri aktarma Alt Sisteminin Tasarım Belgesi
10	1.9	Android Platformunda veri toplama ve aktarım yapan Alt Sistemlerin Doğrulanmış Halleri
11	1.10	iOS Platformunda veri toplama ve aktarım yapan Alt Sistemlerin Doğrulanmış Halleri
12	1.11	Hem açık kaynak sensör verilerini hem de doğrudan kullanıcılardan alınan sernsör verilerini kullanarak, farklı sensörlerden gelen verilerin birbirilerine bağımlılıklarının analizini
13	1.12	Yapılması önerilen ek analiz yöntemlerinin içeren Teknik Rapor
14	2	**Davranış Biometriğinin Modellenmesi ve Davranış Farklılığına Göre Şüphelinin Algılanmasını Sağlayan Alt**
15	2.1	Mobil Cihazlar üzerindeki sensör verileri kullanılarak kişiye özgü davranışların modellenmesinde kullanılan yöntemlerin
16	2.2	Davranış verisinden davranış özet vektörünün çıkarılması – (Faz-1) ile ilgili çalışmaları içeren Teknik Rapor
17	2.3	Davranış özet vektörleri kullanılarak kullanıcının özgünlük denetimini sağlayan sınıflayıcı alternatiflerinin denenmesi-
18	2.4	Davranış verisinden davranış özet vektörünün çıkarılması – (Faz-2) ile ilgili çalışmaları içeren Teknik Rapor
19	2.5	Davranış özet vektörleri kullanılarak kullanıcının özgünlük denetimini sağlayan sınıflayıcı alternatiflerinin denenmesi-
20	2.6	Başarılı olduğu düşünülen yöntemlerin Android üzerinde prototip olarak gerçeklenmesi
21	2.7	Başarılı görülen yöntemin mobil cihazlar üzerindeki yazılımsal çözümünün tasarım belgesi.
22	2.8	Başarılı görülen yöntemin mobil cihazlar (Android, ve iOS) üzerindeki yazılımsal çözümünün gerçeklenmiş hali.
23	2.9	Yapılması gereken ek çalışma ve iyileştirmelere ilişkin Teknik Rapor
24	3	**Davranış Biyometriğinin Modellenmesi İçin Gerekli Yardımcı Sistemlerin Geliştirilmesi**
25	3.1	Kullanıcının davranış biçimlerinde istatistik niteliği taşıyan bilgilerin anonim bir şekilde merkezi sistemde toplanarak kullanıcılar arasındaki farklılıkların sürekli olarak
26	3.2	Kullanıcı davranışının özetlenmesinin otomasyonunu ve sınıflayıcı bileşenlerin otomasyonunu sağlayan bileşenlerinin
27	3.3	Kullanıcının davranış biçimlerinde istatistik niteliği taşıyan bilgilerin anonim bir şekilde merkezi sistemde toplanarak kullanıcılar arasındaki farklılıkların sürekli olarak
28	3.4	Kullanıcı davranışının özetlenmesinin otomasyonunu ve sınıflayıcı bileşenlerin otomasyonunu sağlayan bileşenlerinin
29	3.5	Kullanıcının davranış biçimlerinde istatistik niteliği taşıyan bilgilerin anonim bir şekilde merkezi sistemde toplanarak kullanıcılar arasındaki farklılıkların sürekli olarak
30	3.6	Kullanıcı davranışının özetlenmesinin otomasyonunu ve sınıflayıcı bileşenlerin otomasyonunu sağlayan bileşenlerinin
31	3.7	Yapılması gereken ek çalışma ve iyileştirmelere ilişkin Teknik Rapor
32	4	**Alt sistemler arasındaki Etkileşimin Planlanmaması, Entegrasyon, Sistem Yönetimi/Raporlama, Sistem Doğrulama, Ürün Dokümantasyonu**
33	4.1	Alt Sistemler arası Etkileşime Yönelik Analiz Dokümanı
34	4.2	Sistem Üst Seviye Tasarım Dokümanı
35	4.3	Alt Sistemler arası Sistemlerle Etkileşimin Ayrıntılandığı Arayüz Spesifikasyon Dokümanı
36	4.4	Temel Sistem Yönetimi Alt Sistemi
37	4.5	Temel Sistem Raporlama Alt Sistemi
39	4.7	Uçtan uca Sistem Test Raporu
40	4.8	Uçtan uca Çalışan Doğrulanmış Sistem
41	4.9	Uçtan uca entegrasyonlarla iyileştirmelerle ilgili Analiz Raporu
42	4.10	Ürün kullanım dokümantasyonu

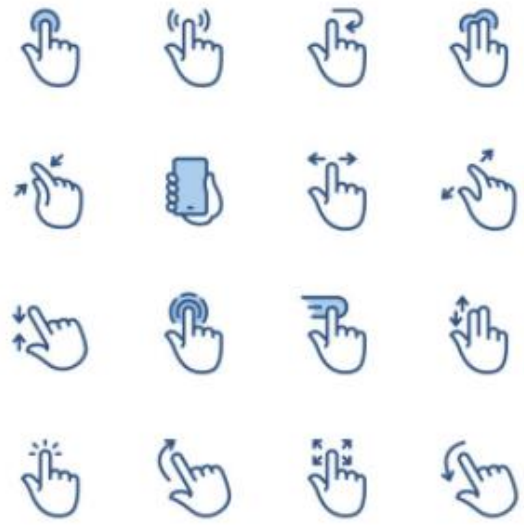
Veri Toplama

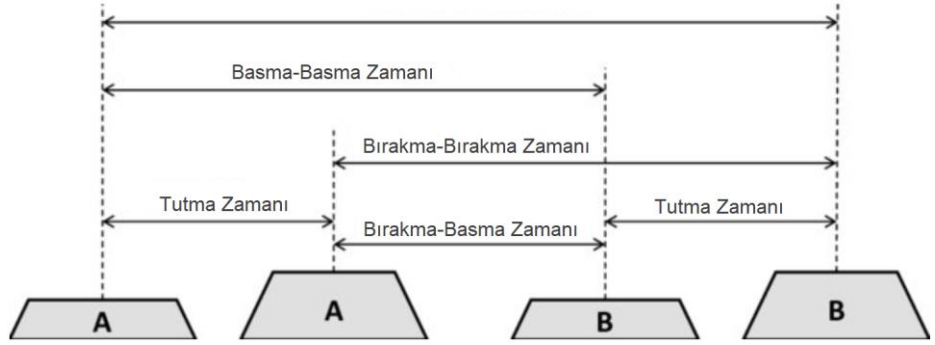
- Literatür taramasında pek çok makale, kendi veri setlerini kullanmıştır.

Veri Seti	Yıl	Vuruş Dinamiği	Sensör	Parmak Hareketleri	Gönüllü Sayısı
HMOG	2016	Var	İvmeölçer, Jiroskop, Manyetometre	Var	100
BrainRun	2019	Yok	İvmeölçer, Jiroskop, Manyetometre	Var	2218
AALTO Mobile	2019	Var	Yok	Yok	37.370
DAKOTA	2021	Yok	İvmeölçer, Jiroskop, Manyetometre	Var	45
HuMIdb*	2020	Var	İvmeölçer, Jiroskop, Manyetometre	Var	599

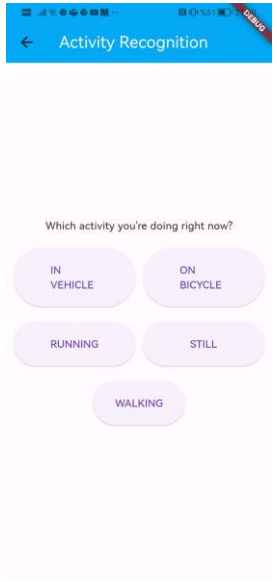
* Bu veri seti için istekte bulunulmuş ve yakın zamanda elde edilecektir.

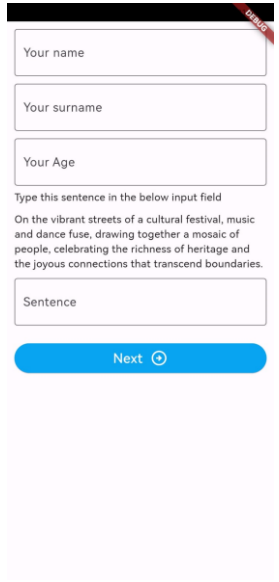


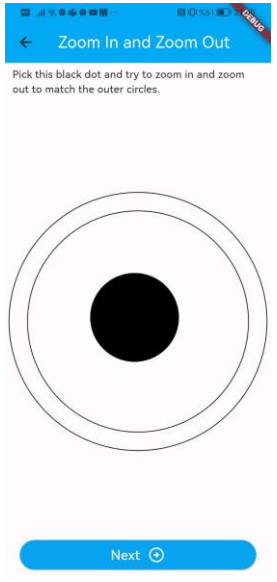


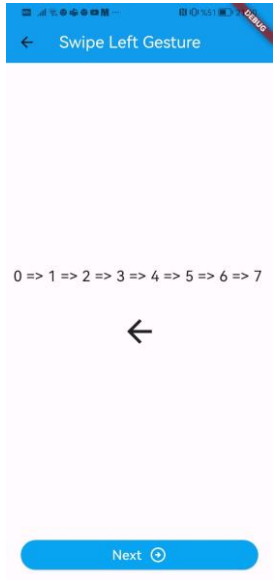


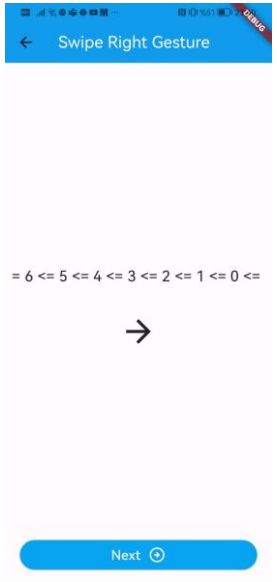
➢ Veri Toplama Uygulama

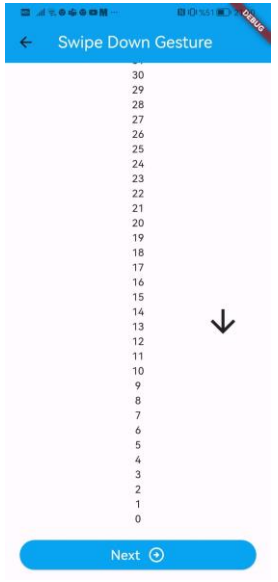


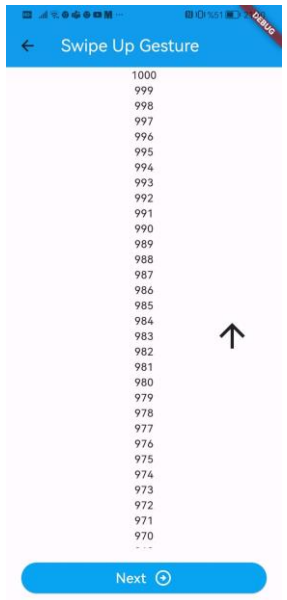


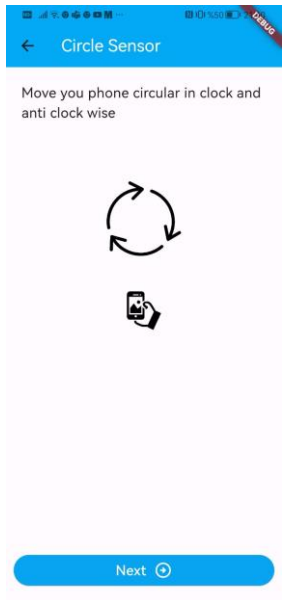


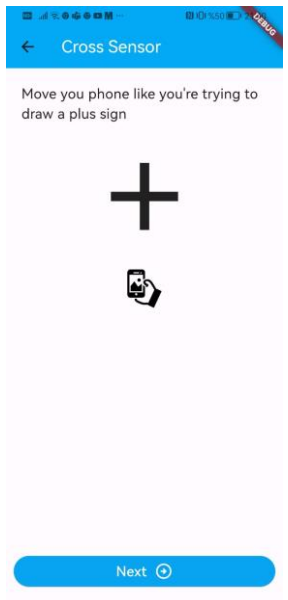


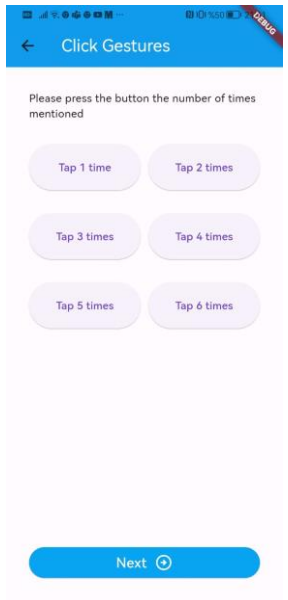


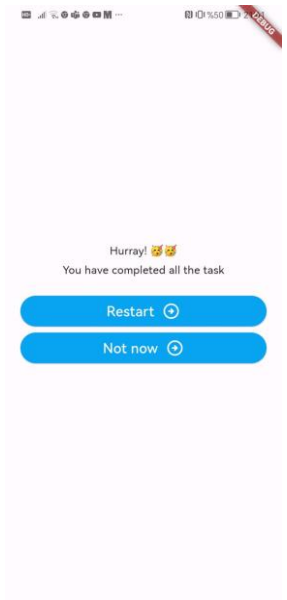






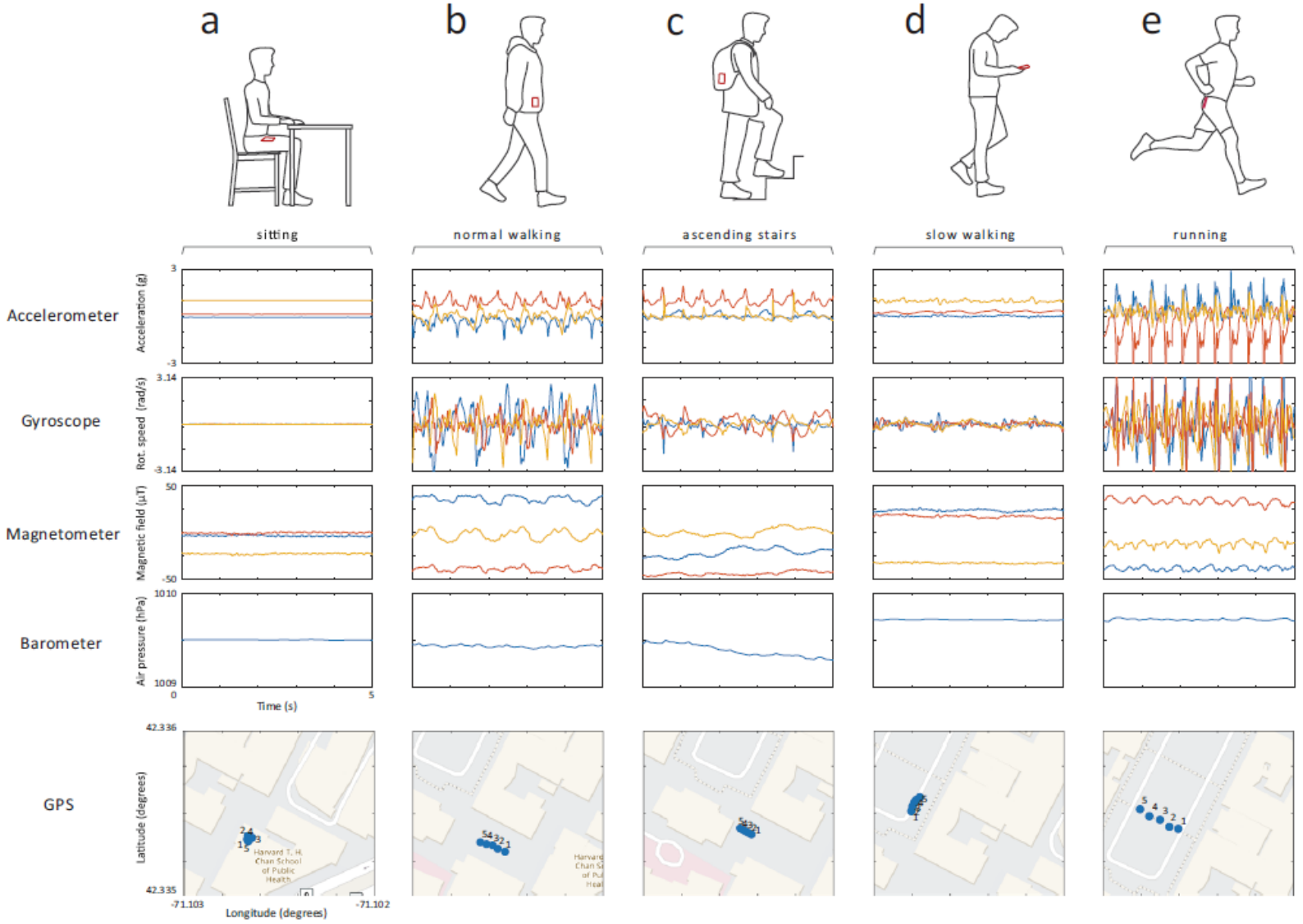






Model Bilgisi ve Tasarım

Fiziksel aktiviteler (hareket): ayakta durma, oturma, yatma, yürüme, merdiven çıkma, merdiven inme, koşma veya taşıma araçlarını kullanma (araba, otobüs, tren, gemi, bisiklet vb.).



[1] Straczkiewicz, M., James, P., & Onnela, J. P. (2021). A systematic review of smartphone-based human activity recognition methods for health research. *NPJ Digital Medicine*, *4*(1), 148.

➢ Aktivite Tespiti

Gerçek Zamanlı Aktivite Tespit Modeli

Sensörler

Accelerometer
Gyroscope
Magnetometer
GPS
Others (light, proximity, barometer, thermometer)

Ön-işleme

Standardization (Denoising, Repairing vs.)
Transformation (Normalization, Separation, etc.)

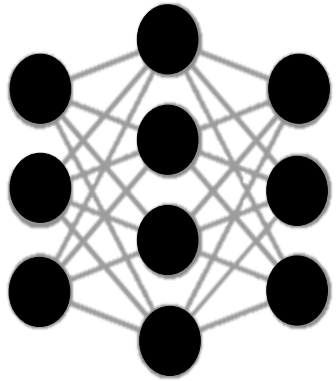
Öznitelik Çıkarımı

Segmentation
- Fixed window
- Adaptive window

Feature Type
- Time-domain
- Frequency-domain

Feature Selection
- Hand-crafted
- Deep learning

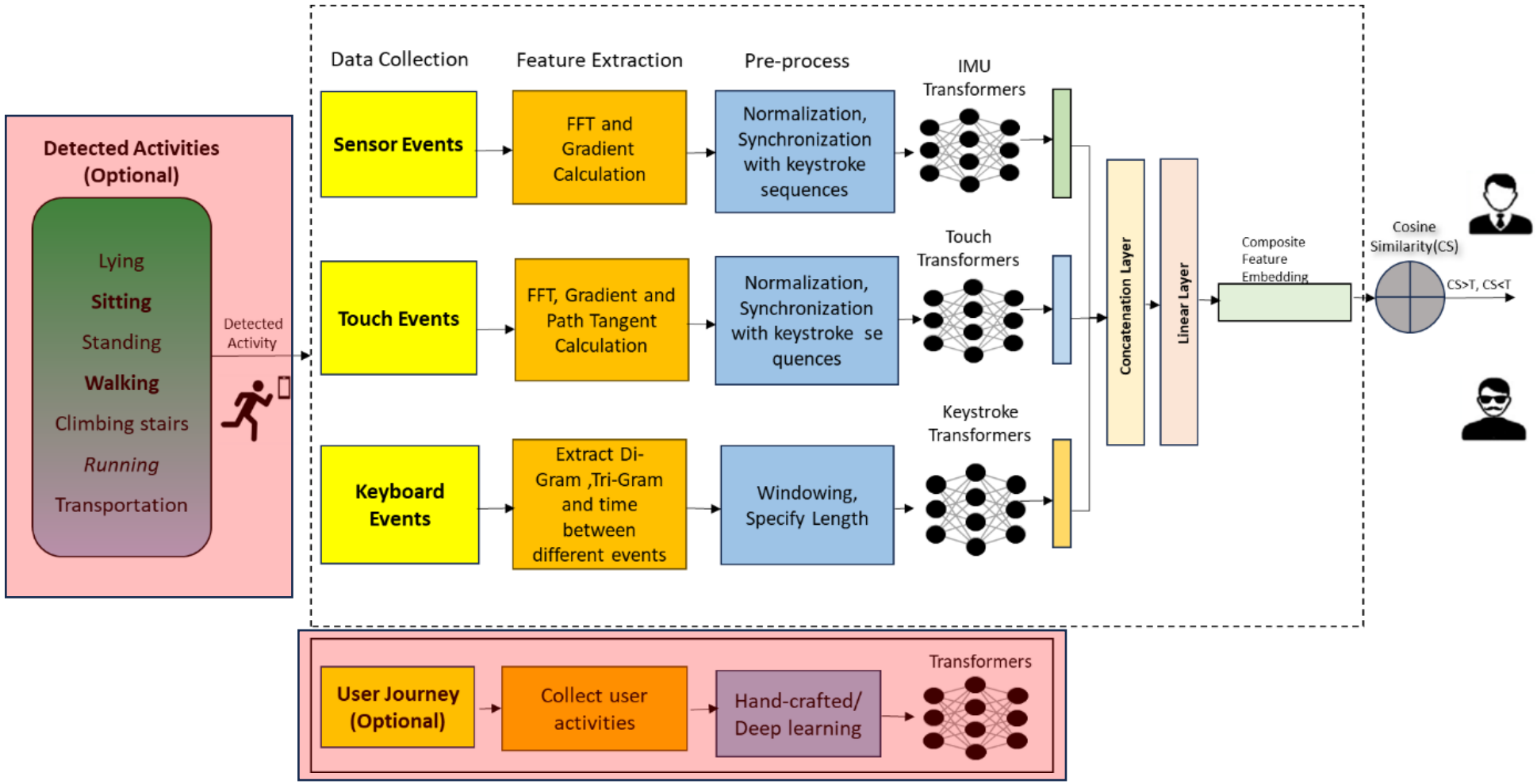
Aktivite Sınıflandırma (RNN, LSTM, Transformers, etc.)



Tespit Edilen Aktiviteler

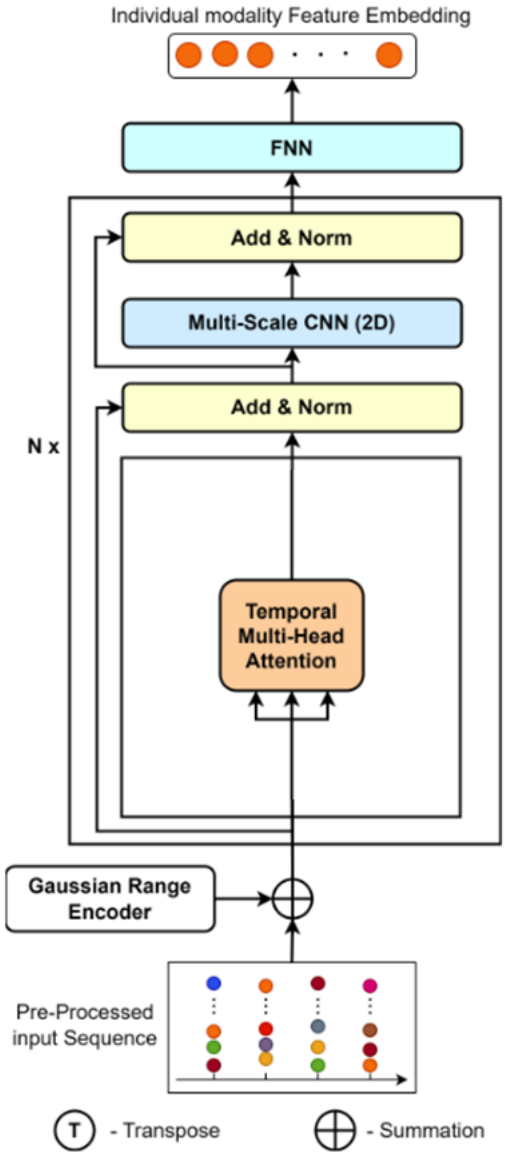
Lying
Sitting
Standing
Walking
Climbing stairs
Running
Transportation

Model Tasarım



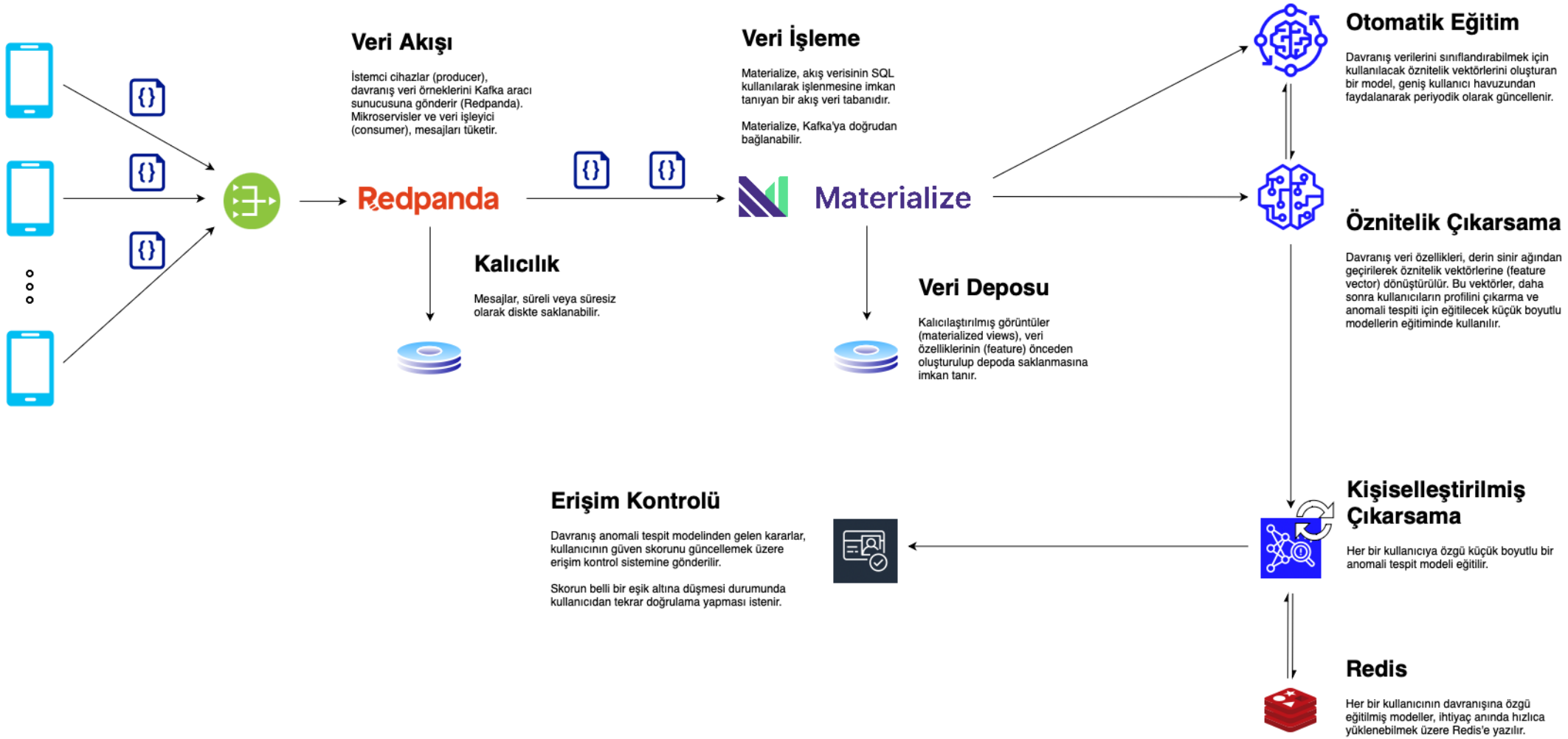
Model Mimarisi

- Oluşturulan model tuş vuruşu dinamikleri, dokunma verileri ve sensör verileri için tasarlanmış üç adet Spatio-Temporal Dual Attention Transformer (STDAT) içerir. Bu, elde edilen verilerden daha ayırt edici özellikler çıkarmak için tanıtılan yeni bir transformerdır .
- STDAT modeli, gelen veri üzerinde zamansal boyutlara odaklanan çift dikkat mekanizması kullanır. Zamansal-MHA (multi-head attention), girdi verilerini zaman içinde analiz eder ve benzersiz davranışsal kalıpların çıkarılmasına olanak tanır. Model, pozisyonel ayrıntıların örneklemler için ayrımcı bir özellik üretmede önemli olduğunu kabul ederek, girdiye Gaussian Range Encoder (GRE) kullanılarak pozisyonel kodlama ekler. GRE, pozisyonları tek bir nokta yerine pozisyon aralıkları olarak kodlayan öğrenilebilir bir aralık tabanlı pozisyonel kodlamadır. Model, ayrıca her iki dikkat modülünün çıktısını kullanarak, zamansal desenleri göz önünde bulundurularak ayrımcı özellikler içeren bir çıktı üretir .



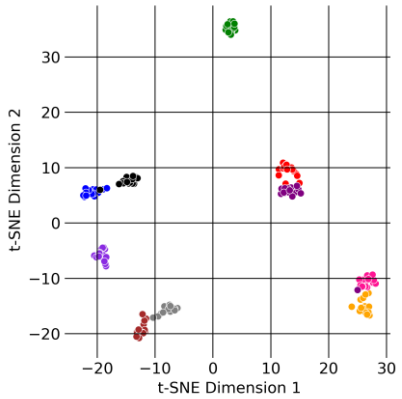
➢ Davranış Analizi Modeli Bulut Tarasımı

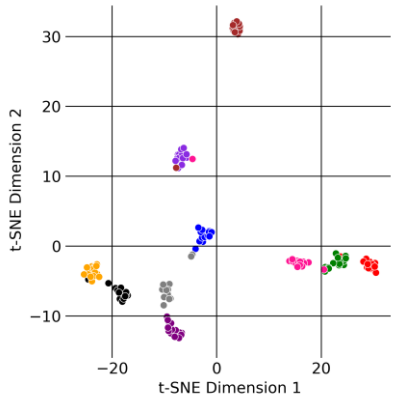
Yerinde çalıştırabilir davranış biyometriği ile sürekli doğrulama için makine öğrenmesi tasarım belgesi Şekil'de sunulmuştur.

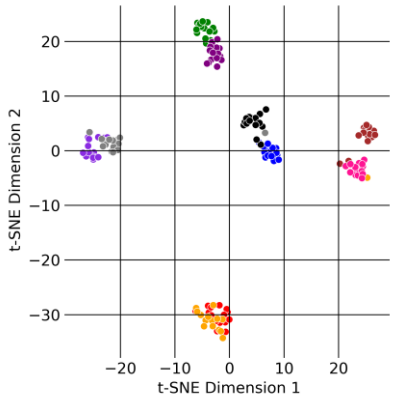


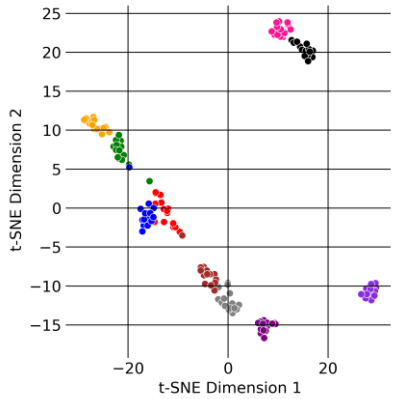
t-SNE plotları

t-SNE plotlarında farklı kullanıcılara ait özniteliklerin kümenlendiğini gözlemleyebiliyoruz.









Başarı Ölçütleri

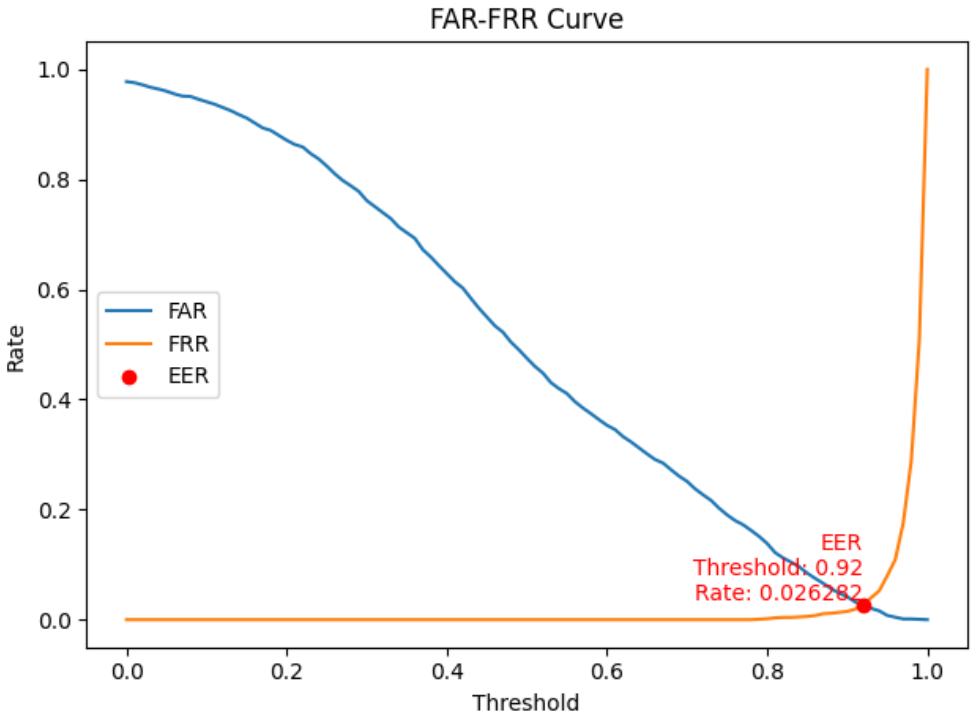
Proje başvuru aşamasında yapılan kapsamlı değerlendirmeler sonucu, belirlenen başarı ölçütleri projenin hedeflerine ulaşma kapasitesini ve amacının gerçekleşme derecesini ölçmek için hayati önem taşımaktadır. Bu ölçütler, projenin genel performansının objektif bir şekilde değerlendirilmesini, ilerlemenin sürekli olarak izlenmesini ve elde edilen sonuçların kapsamlı bir şekilde analiz edilmesini sağlar. Model seçim sürecinde, bu başarı ölçütleri temel alınarak yapılan değerlendirmeler, projenin sonuçlarının güvenilirliğini ve uygulamadaki etkinliğini artırma yolunda kritik bir role sahiptir. Bu çerçevede, modellerin seçimi ve değerlendirilmesi sürecinde başarı ölçütleri, modelin performansını maksimize etme ve projenin genel başarısını optimize etme amacıyla kullanılmıştır.

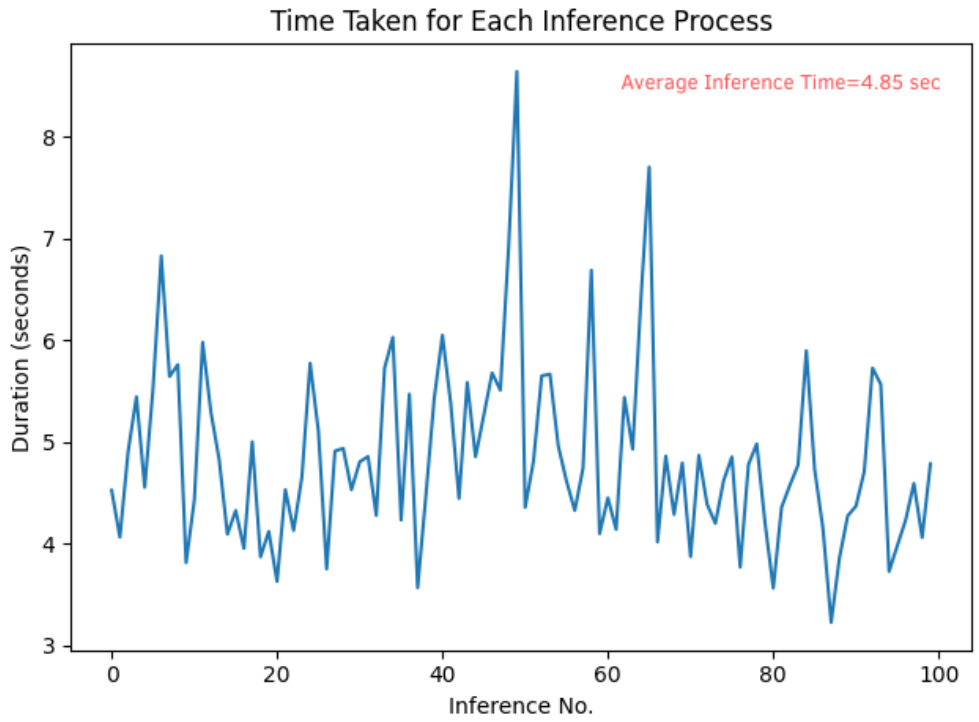
Teknik Özellikler

Teknik Özellik	Proje Çıktısı (Planlanan)	Proje Çıktısı (Tamamlanan)
Jiroskop	Var	Mevcut
Sekans (bigram, trigram)	Var	Mevcut
İvmeölçer	Var	Mevcut
Manyetometre	Yok	Mevcut
Sürükleme yönü	Var	Mevcut
Sürükleme süresi	Var	Mevcut
Parmak basıncı	Var	Mevcut
Parmak hızı	Var	Mevcut

Başarı Ölçütü	Hedeflenen Değer	Gerçekleşen Değer
Davranış biyometriği- sınıflama başarım metriği olarak- FRR (False Rejection Rate)	<= %5	**%2,8**
Davranış biyometriği- sınıflama başarım metriği olarak- FAR (False Acceptance Rate)	<= %3	**%2,6**
Kullanıcı için özgünlük denetimi için denetim aralığı (saniye olarak)	<= 10 sn	**4,85 sn**

Model Performansı





Grafiğe ilişkin olarak farklı eşik seviyeleri için FRR ve FAR değerleri verilmiştir.

- ✓ 0,89 eşik => FRR = %1.3, FAR = %4.8
- ✓ 0,9 eşik=> FRR = %1,5, FAR = %4,1
- ✓ 0,91 eşik => FRR = %1,9, FAR = %3,2
- ✓ **0,92 eşik => FRR = %2,8, FAR = %2,6**
- ✓ 0,93 eşik => FRR = %4, FAR = %2

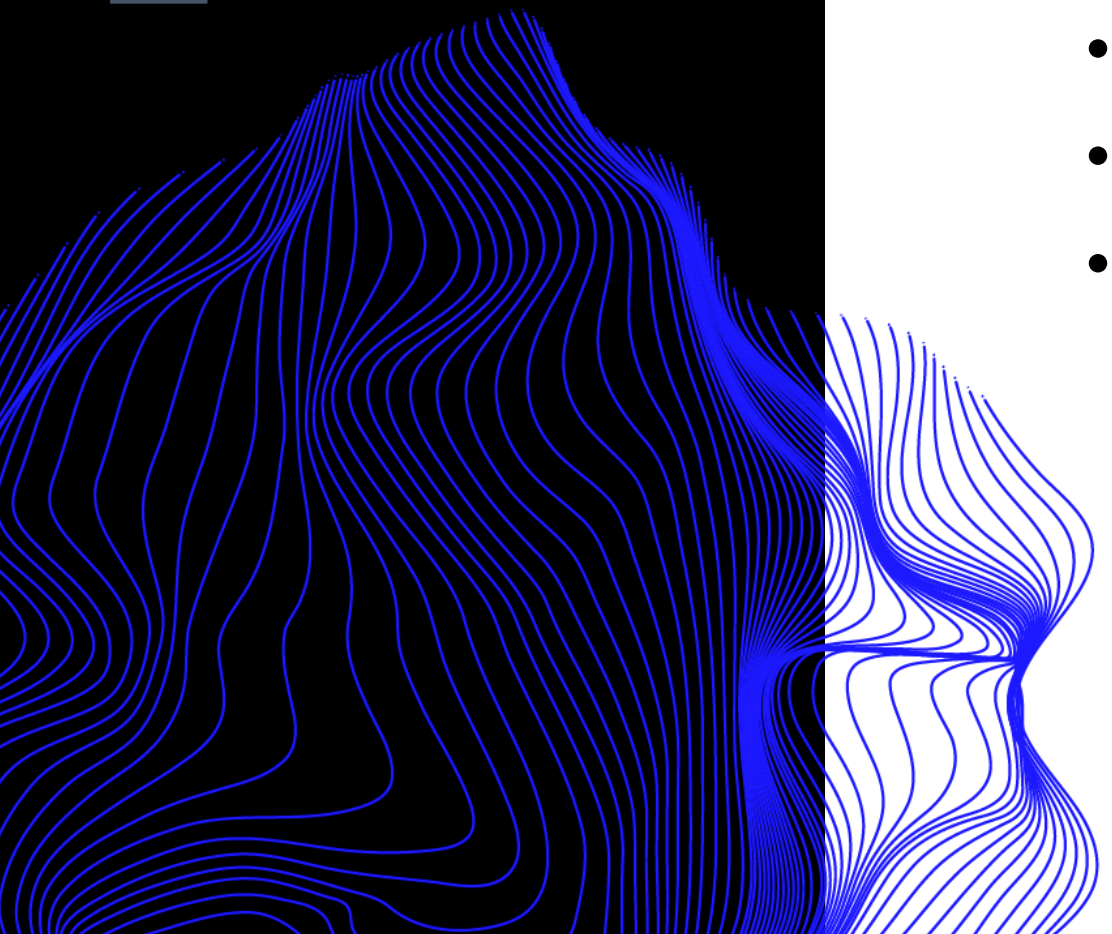
KOBIL

Risk Verilerinin Analizi

Yapay Zeka Arf Ödülleri

KOBİL Teknoloji A.Ş.

İçindekiler



- Risk Verilerinin Analizi
- İş Planı
- Veri İşleme
- Model Bilgisi ve Tasarım
- Gerçekleştirilen Başarı Ölçütleri

Risk Verilerinin Analizi

Mobil cihazlardan gelen risk verilerini toplayarak, cihazlara **düşük, orta ve yüksek** olmak üzere **üç seviyeli bir risk** atayan bir değerlendirme sistemi geliştirdik. Bu sistem, kullanıcıların mobil cihazlarını güvenli bir şekilde kullanmalarını sağlamak amacıyla potansiyel tehditleri gerçek zamanlı olarak analiz ederek sınıflandırır. Risk değerlendirmesi, cihazın güvenlik durumu ve olası tehditlerin etkileri üzerine odaklanır. Kullanılan risk değerlendirme kriterleri aşağıda verilmiştir fakat model gelecekte olabilecek farklı kriterlere uyum sağlama özerlliğine sahiptir.

Değerlendirilen Risk Kriterleri:

1. Jailbreak/Kök Erişimi (Risk-ID [1])

2. Manipülasyon (Risk-ID [2])

3. Zararlı Uygulama (MaliciousApp) (Risk-ID [4])

4. Kod Enjeksiyonu (CodeInjection) (Risk-ID [6])

5. Emülatör Algılama (Emulator Detection) (Risk-ID [0x47])

6. Bellek Koruma (Memory Protection) (Risk-ID [8])

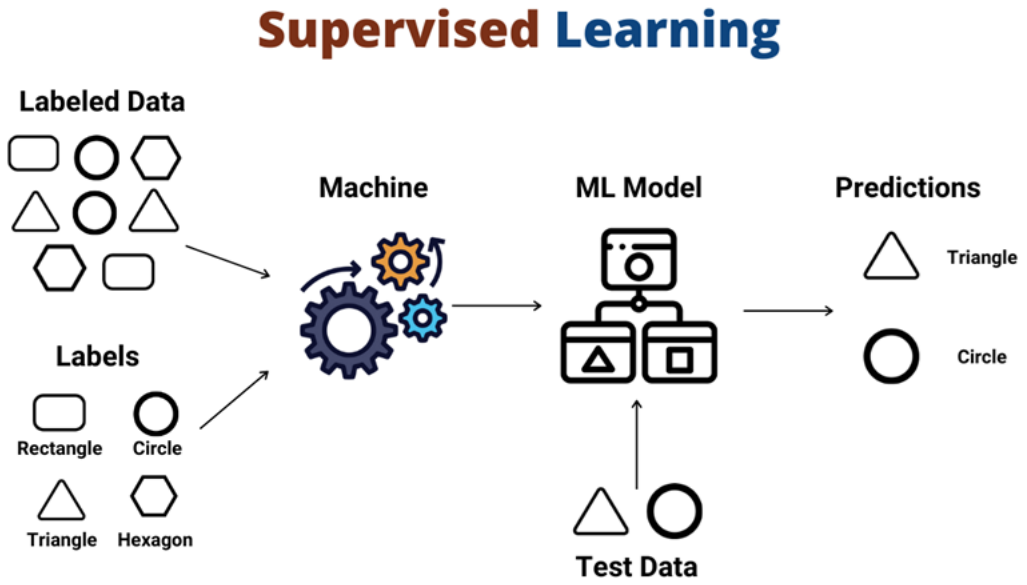
İş Planı

No.	FAALİYETLER	2023-1						2023-2						2024-1					
		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6
1	**Proje Hazırlık ve Risk Analizi**																		
1.1.	Güncel kullanılan metotların dezavantajları ve mevcut sunulan en iyi çözümün saptanması																		
1.2.	Kullanılmak istenilen modelin detaylı araştırılması ve mevcut probleme uygunluğunun incelenmesi																		
2	**Veri Toplama**																		
2.1.	Kullanıma açık risk puanlama üzerine oluşturulan veri setlerinin tespit edilmesi																		
2.2.	Firmamız bünyesinde bulunan verilerin risk puanlama için değerlendirilmesi																		
2.3.	Uygun veri kaynaklarının belirlenerek veri toplama işleminin başlatılması																		
2.4.	Anlamsız veya eksik olan verilerin çıkarılarak uygun şekilde temizlenmesi																		
2.5.	Güvenlik uzmanları tarafından elde edilen verinin risk değerlendirmesinin yapılarak etiketlenmesi																		
2.6.	Veriyi eğitim, doğrulama ve test kümelerine ayırma																		
2.7.	Veriyi büyütme yöntemlerinin araştırılması																		
2.8.	Normalizasyon ihtiyaçlarının belirlenmesi																		
3	**Model Geliştirme ve Model Başarım Stratejilerinin Geliştirilmesi**																		
3.1.	Risk puanlama için literatür incelemesi sonucunda çıkan uygun modelin tanımlanması																		
3.2.	Model eğitimi için yazılım ihtiyaçlarının belirlenmesi (kütüphaneler, çerçeveler, vs.)																		
3.3.	Ayırt edici özniteliklerin belirlenmesi ve risk puanlama üzerinde etkili olacak ağırlıklarına karar verilmesi																		
3.4.	Özniteliklerin en etkili şekilde modele nasıl beslenebileceğinin analizinin yapılması																		
3.5.	Risk puanlama için karar verilen modelin toplanmış ve etiketlenmiş veri üzerinde eğitiminin yapılması																		
3.6.	Sürekli model değerlendirmesi ve iyileştirme için pekiştirmeli öğrenme tekniğinin modele eklenmesi																		
3.7.	Modeli güvenlik uzmanlarından alınacak destek ile ödül-ceza yöntemi kurularak optimum sonucu elde edilmesi																		
3.8.	Geç füzyon için bir mimari tasarımına ihtiyaç olup olmadığının belirlenmesi																		
3.9.	Erken füzyon için bir mimari tasarımına ihtiyaç olup olmadığının belirlenmesi																		
3.10.	Geç füzyon ve erken füzyon için elde edilen sonuçların değerlendirilerek hangisinin yapılacağına karar verilmesi																		
4	**Model Değerlendirmesi ve Optimizasyonu**																		
4.1.	Model performansının değerlendirilmesi için metriklerin belirlenmesi																		
4.2.	Belirlenen metriklere göre model performansının ölçülmesi																		
4.3.	Değerlendirme kriterlerine ve performans metriklerine göre modele ince ayar yapılması																		
4.4.	Risk puanlama için uluslararası model performans değerlendirmesi yapan bağımsız merkezlerin araştırılması																		
4.5.	Muhtemel çevrimdışı çalışma seçenekleri için modelin optimize edilmesi																		
4.6.	Hızlandırıcılar kullanılarak model çıkarım hızının arttırılması																		
4.7.	Optimize edilmiş modelin farklı cihaz ve Android/IOS sürümlerinde test edilmesi																		
5	**Sunucu/Uç Nokta Kurulumu ve Arayüz Tasarımı**																		
5.1.	Sorunsuz bir deneyim sağlamak için veri akışı mimarisini tasarlanması																		
5.2.	Risk puanlama modeli için bir sunucunun belirlenmesi																		
5.3.	Risk puanlama modeli için API uç noktalarının gelişirilmesi																		
5.4.	Kullanıcı arayüz düzeninin ve arayüz öğelerinin tasarlanması																		
5.5.	Risk bitlerinin elde edilmesi sürecinin uygulanması																		
5.6.	Risk bitlerinin gönderilmesi ve sonucun döndürülme süreçlerinin tamamlanması																		
5.7.	Risk bitlerinin güvenli bir şekilde depolanması																		
5.8.	Risk bitlerinin güvenli bir kanal üzerinden sunucuya gönderilmesi																		
5.9.	Kullanıcı isteklerini yönetecek bir sistem tasarımı																		
6	**Entegrasyon/Test Süreçleri ve Dokümantasyon**																		
6.1.	Entegrasyon testlerinin yapılması																		
6.2.	Bir test uygulaması üzerinden entegre sistemin gerçek Kullanıcı Kabul Testini gerçekleştirilmesi.																		
6.3.	Otomatik derlemeler ve CI/CD süreçlerinin tamamlanması.																		
6.4.	Sistem ve model dökümantasyonun oluşturulması.																		
6.5.	Karşılaşılan güçlükleri ve uygulanan çözümleri içeren dökümantasyon.																		
6.6.	Entegrasyon ve üretim süreçlerini açıklayan dökümantasyon.																		

Veri İşleme

- 5 milyon civarında bir veriyi KOBIL veri tabanından elde etmeyi hedefliyoruz. Burada bir düzenleme ve normalizasyon adımı yapacağız.
- Risk puanlama modelimizin temelinde denetimli öğrenme kullanacağız.

Denetimli öğrenme, bir modelin eğitim sürecinin, önceden etiketlenmiş veya doğru cevapları içeren verilere dayandığı bir öğrenme türüdür. Özetle, bu yaklaşım, bir modelin belirli bir görevi öğrenmesi ve daha sonra yeni verileri analiz etmek, tahmin etmek veya sınıflandırmak için kullanması amacıyla kullanılır. Örneğin, geometrik şekilleri üçgen, daire diktörtgen v.s. olarak sınıflandırmak veya görüntülerdeki nesneleri tanımak gibi birçok uygulama alanında denetimli öğrenme kullanılır. Bu süreç, veri toplama, model eğitimi ve performans değerlendirmesi adımlarını içerir ve makine öğrenme alanının temel taşlarından birini oluşturur.



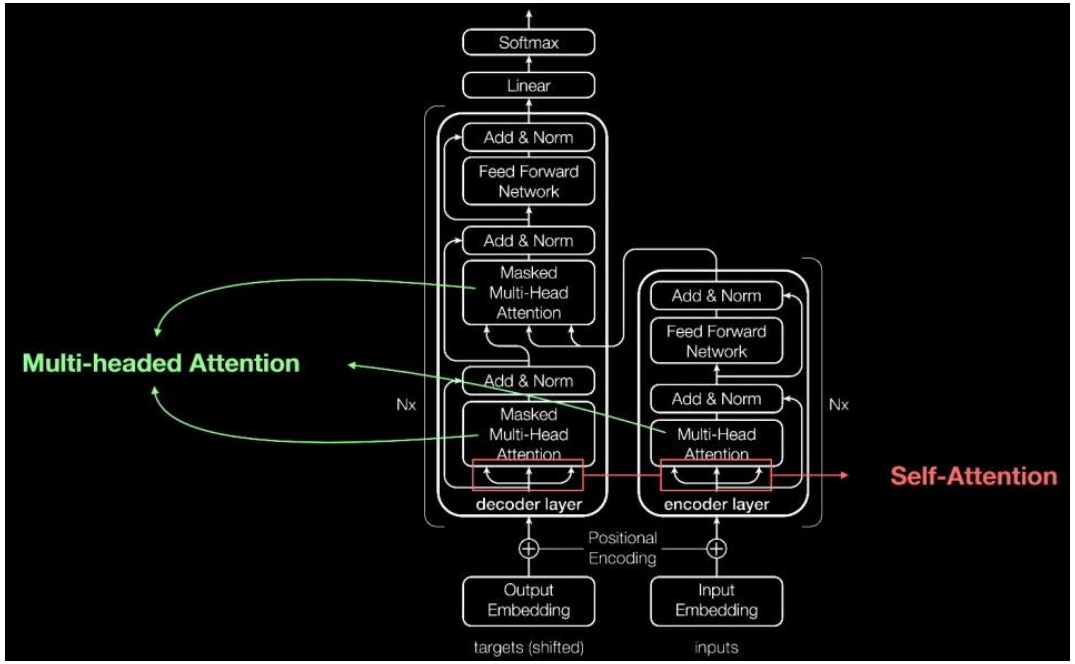
Model Bilgisi ve Tasarım

Transformers mimarisi temelinde inşa edilmiş bir yapay zeka modelidir. Örneğin GPT, genellikle birçok tekrarlanan bloktan oluşur ve her blok, dikkat (attention) mekanizması ve besleme ileri (feedforward) katmanları içerir. GPT'nin temel bileşenlerine bakacak olursak:

Dikkat Mekanizması (Attention Mechanism): Her GPT bloğu, dikkat mekanizması içerir. Bu mekanizma, modelin giriş verilerinin farklı kısımlarına odaklanmasına olanak tanır. Dikkat mekanizması, metin verilerinin içindeki ilişkileri daha iyi anlamak için kullanılır.

Özyinelemesiz Dikkat (Self-Attention): GPT'deki dikkat mekanizması, özyinelemesizdir, yani veri sırasıyla işlenmez. Bu, paralel hesaplamaların yapılmasına ve eğitim sürecinin hızlanmasına olanak tanır.

Besleme İleri Katmanı (Feedforward Layer): Dikkat mekanizması sonuçları, besleme ileri katmanlarına iletilir. Bu katmanlar, özellikleri işler ve daha sonra sonuçları çıkarır.



Layer Normalizasyon: Her GPT bloğunda, katman normalizasyonu adı verilen bir teknik kullanılır. Bu, eğitim sürecini stabilize etmeye ve modelin daha hızlı yakınsamasına yardımcı olur.

Staked Blocks (Üst Üste Bloklar): GPT, genellikle birçok bloğun üst üste eklenmesiyle oluşturulur. Bu, modelin derinliğini artırır ve daha karmaşık görevleri çözmeye olanak tanır.

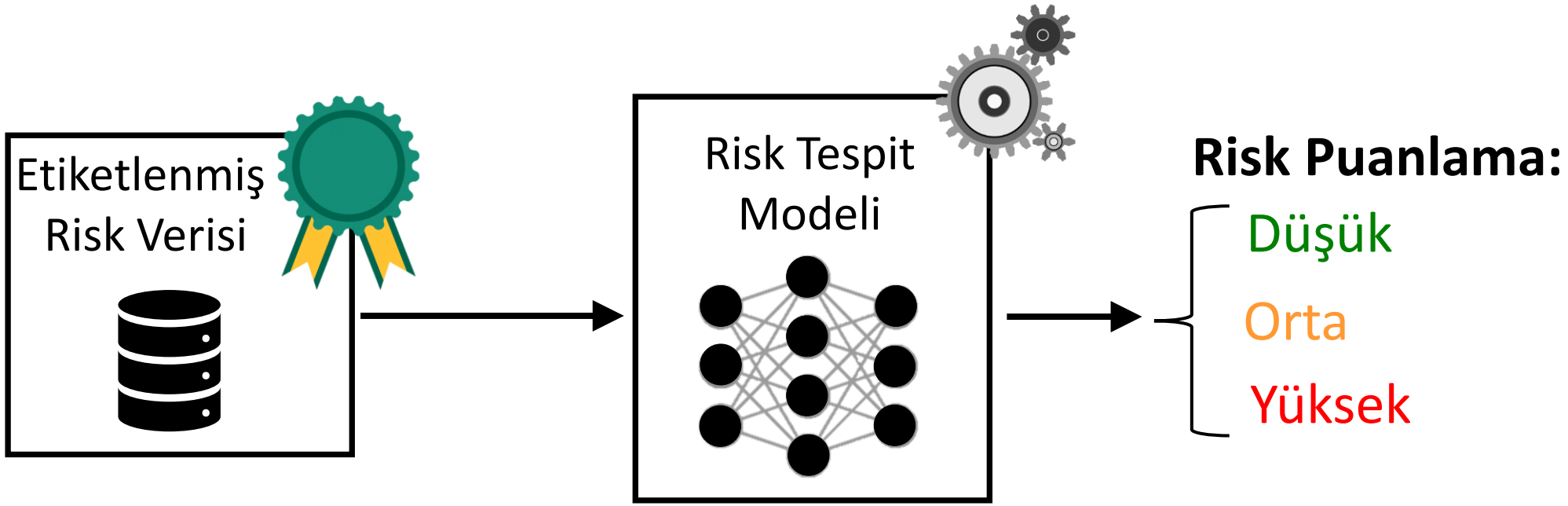
Kelime Gömme (Word Embeddings): GPT, kelime gömme katmanları ile başlar. Bu katmanlar, kelime dağarcığını vektörlerle temsil ederler ve metin verilerini işlemeye başlamak için kullanılır.

Lineer Dönüşüm Katmanı (Linear Transformation Layer): GPT'nin çıkışı, genellikle bir lineer dönüşüm katmanı ile sonuçlanır. Bu katman, modelin sonuçlarını istenen çıktı biçimine dönüştürür.

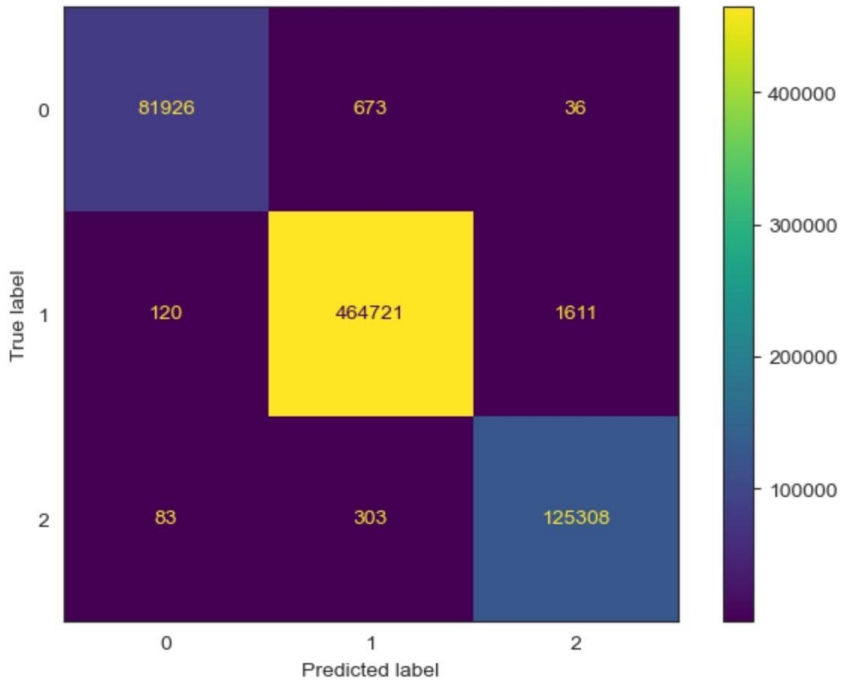
- ✓ **GPT modelleri, genellikle büyük veri setleri üzerinde ön eğitim ile başlatılır ve ardından belirli görevlere özelleştirilir. Bu yapının, doğal dil işleme görevleri gibi çeşitli uygulamalarda başarılı olduğu kanıtlanmıştır.**

Risk Değerlendirme Sistemi

Model Mimarisi



Gerçekleştirilen Başarı Ölçütleri



	precision	recall	f1-score	support
0	1.00	0.99	0.99	82635
1	1.00	1.00	1.00	466452
2	0.99	1.00	0.99	125694
accuracy			1.00	674781
macro avg	0.99	0.99	0.99	674781
weighted avg	1.00	1.00	1.00	674781