İşaret Dili Tanıma Sistemi

İşlevsel Olmayan Gereksinimler

NFR-01 – Gerçek Zamanlı Yanıt Süresi Performansı

Sistem, işaret tanıma işlemlerini gerçek zamanlı olarak gerçekleştirmeli ve kullanıcı deneyimini olumsuz etkilememek için maksimum 200 milisaniye içerisinde yanıt vermelidir. Bu süre, insan algısının gecikmeyi fark etmediği Weber-Fechner yasası temelinde belirlenmiştir; 250ms üzerindeki gecikmeler kullanıcı deneyiminde belirgin olumsuzluk yaratmaktadır.

Video akışı işleme gecikme süresi 50ms'yi aşmamalıdır. Bu değer, 30 FPS video akışında frame-to-frame tutarlılığı sağlamak için kritiktir. Alternatif olarak 60 FPS kullanılması durumunda bu süre 33ms'ye düşürülmelidir.

İşaret tanıma algoritması çalışma süresi 100ms ile sınırlı tutulmalıdır. Bu süre, CNN (Convolutional Neural Network) tabanlı modeller için optimize edilmiştir; RNN (Recurrent Neural Network) kullanılması durumunda performans %20-30 düşebilir, ancak sekans tanıma doğruluğu artabilir.

Sistem, eş zamanlı 100 kullanıcı tarafından kullanıldığında bile bu performans kriterlerini koruyabilmelidir. Load balancing ve mikroservis mimarisi ile ölçeklenebilirlik sağlanmalı; monolitik mimari kullanılması durumunda performans degradasyonu kaçınılmazdır.

NFR-02 – Veri Güvenliği ve Kriptografik Koruma

Sistem, kullanıcı verilerinin güvenliğini SSL/TLS 1.3 protokolü ile sağlamalıdır. TLS 1.3, önceki sürümlere göre yaklaşık %40 daha hızlı el sıkışma süresi (handshake) ve gelişmiş forward secrecy sağladığı için tercih edilmektedir. Alternatif olarak TLS 1.2 uygulanabilir; ancak bu durumda performans kaybı yaşanabilir.

Kişisel veriler, AES-256 algoritması ile şifrelenmelidir. AES-256, AES-128'e kıyasla daha yüksek güvenlik düzeyi sunmakta ve kuantum hesaplamaya karşı daha dirençli bir yapıya sahiptir. RSA ve 3DES gibi algoritmalar hem güvenlik hem de verimlilik açısından günümüz ihtiyaçlarını karşılamamaktadır.

Video kayıtları ve profil verileri, uçtan uca şifreleme (end-to-end encryption) ile korunmalıdır. Hassas veriler için, k-anonymity, l-diversity ve differential privacy gibi anonimleştirme teknikleri uygulanmalıdır.

Kullanıcı kimlik bilgileri, güvenli bir şekilde SHA-256 algoritması ile hash edilerek saklanmalıdır. SHA-1 ve MD5 gibi eski algoritmaların güvenlik açıkları nedeniyle tercih

edilmemekte; daha yüksek güvenlik gerektiren durumlarda bcrypt veya Argon2 gibi salt-based hash fonksiyonları önerilmektedir.

Son olarak, sistemin tüm veri işleme süreçleri, GDPR ve KVKK gibi yasal düzenlemelere tam uyum içinde tasarlanmalı ve yürütülmelidir.

NFR-03 – Erişilebilirlik ve Evrensel Tasarım Uyumluluğu

Sistem, WCAG 2.1 AA seviyesi erişilebilirlik standartlarına tam uyumlu olmalıdır. Bu standart, ISO 14289 ve Section 508 gereksinimlerini de karşıladığı için uluslararası uyumluluk açısından tercih edilmektedir. WCAG 2.2 veya AAA seviyesi daha kapsamlı erişilebilirlik sunar; ancak implementasyon maliyeti %40-60 artabilir.

Ekran okuyucu yazılımları ile tam uyumluluk sağlanmalıdır. JAWS (en yaygın kullanılan), NVDA (açık kaynak) ve VoiceOver (macOS/iOS) ile test edilmeli; ARIA (Accessible Rich Internet Applications) etiketleri doğru şekilde uygulanmalıdır.

Klavye navigasyonu %100 desteklenmeli ve Tab order mantıklı sıralamaya sahip olmalıdır. Mouse-only kullanıcı arayüzleri motor engelli kullanıcıları dışarıda bıraktığı için tercih edilmemelidir.

Yüksek kontrast modu bulunmalı ve minimum 4.5:1 kontrast oranı sağlanmalıdır. Deuteranopi, Protanopi ve Tritanopi renk körlüğü türleri için ColorBrewer paleti kullanılması önerilmektedir.

NFR-04 – Sistem Ölçeklenebilirlik ve Kapasitesi

Sistem, horizontal ve vertical scaling destekleyerek minimum 10,000 eş zamanlı aktif kullanıcıya hizmet verebilmelidir. Cloud-based mikroservis mimarisi kullanılarak otomatik scaling mekanizmaları devreye alınmalıdır. Veri tabanı sharding ve load balancing teknikleri ile sistem yükü dağıtılmalı, peak usage zamanlarında %99.9 uptime garanti edilmelidir.

NFR-05 – Platform Bağımsızlığı ve Çapraz Uyumluluk

Sistem, Windows, macOS, Linux, iOS ve Android işletim sistemlerinde yüksek performanslı ve tutarlı kullanıcı deneyimi sunmalıdır. Mobil ve masaüstü uygulamalar, hedef platformların doğal performans kapasitelerine uygun biçimde optimize edilmelidir.

Web tabanlı sürüm, Chrome, Firefox, Safari ve Edge tarayıcılarının son üç ana sürümüyle tam uyumlu olmalıdır. Responsive tasarım ilkeleri doğrultusunda sistem, tablet, akıllı telefon ve masaüstü cihazlarda optimum kullanılabilirlik sağlamalıdır.

Sistem, PWA (Progressive Web App) standartlarını desteklemeli ve internet bağlantısı olmayan ortamlarda offline çalışma yeteneğine sahip olmalıdır.

NFR-06 – Donanım Kaynak Optimizasyonu

Sistem, minimum donanım gereksinimlerinde etkin çalışabilmelidir: 4GB RAM, dual-core processor ve 720p webcam yeterli olmalıdır. CPU kullanımı %70'i, RAM kullanımı %2GB'ı aşmamalıdır. GPU acceleration desteği ile performans artırılmalı, ancak GPU olmayan sistemlerde de çalışabilir durumda olmalıdır. Pil ömrünü korumak için enerji verimli algoritmalar kullanılmalıdır.

NFR-07 – Veri Bütünlüğü ve Yedekleme Sistemi

Kullanıcı verileri günlük otomatik yedekleme ile korunmalı, kritik veriler için real-time replication sağlanmalıdır. Database integrity check mekanizmaları günlük olarak çalışmalı, corruption durumunda otomatik recovery prosedürleri devreye alınmalıdır. Point-in-time recovery özelliği ile 30 gün geriye dönük veri kurtarma imkânı sunulmalıdır. Yedek veriler farklı coğrafi lokasyonlarda saklanmalıdır.

NFR-08 – Kullanıcı Deneyimi ve Arayüz Standartları

Sistem arayüzü, kullanıcı deneyimi prensipleri doğrultusunda sezgisel ve öğrenmesi kolay olmalıdır. Ortalama öğrenme süresi yeni kullanıcılar için 15 dakikayı aşmamalıdır. Erişilebilirlik rehberi doğrultusunda color-blind friendly renk paleti kullanılmalı, font büyüklükleri dinamik olarak ayarlanabilir olmalıdır.

NFR-09 – Hata Toleransı ve Sistem Güvenilirliği

Sistem, %99.5 erişilebilirlik (uptime) garantisi ile 7/24 kesintisiz hizmet sunmalıdır. Kritik hizmetlerin sürekliliği, failover mekanizmaları ile sağlanmalı; cascading failure senaryolarına karşı ise circuit breaker tasarım deseni uygulanmalıdır.

Sistem, arıza durumlarında kademeli bozulma (graceful degradation) prensibi doğrultusunda, temel işlevlerin çalışmaya devam etmesini sağlamalıdır.

Ayrıca, kapsamlı izleme (monitoring) ve uyarı sistemleri (alerting) ile proaktif hata tespiti gerçekleştirilebilmelidir.

NFR-10 – Veri Gizliliği ve Anonimleştirme

Sistem, kullanıcı mahremiyetini korumak amacıyla diferansiyel gizlilik (differential privacy) tekniklerini uygulamalıdır. Biyometrik veriler, yerel cihazda işlenmeli ve ham veri olarak buluta gönderilmemelidir.

Kullanıcıların rıza yönetimi (consent management) mekanizması ile, GDPR kapsamında tanımlanan unutulma hakkı (right to be forgotten) desteklenmeli; veri saklama politikaları (data retention policies) otomatik olarak uygulanmalıdır.

Ayrıca, kullanıcı kimlik bilgilerinin korunması için takma adlandırma (pseudonymization) ve k-anonymity gibi anonimleştirme yöntemleri kullanılmalıdır.