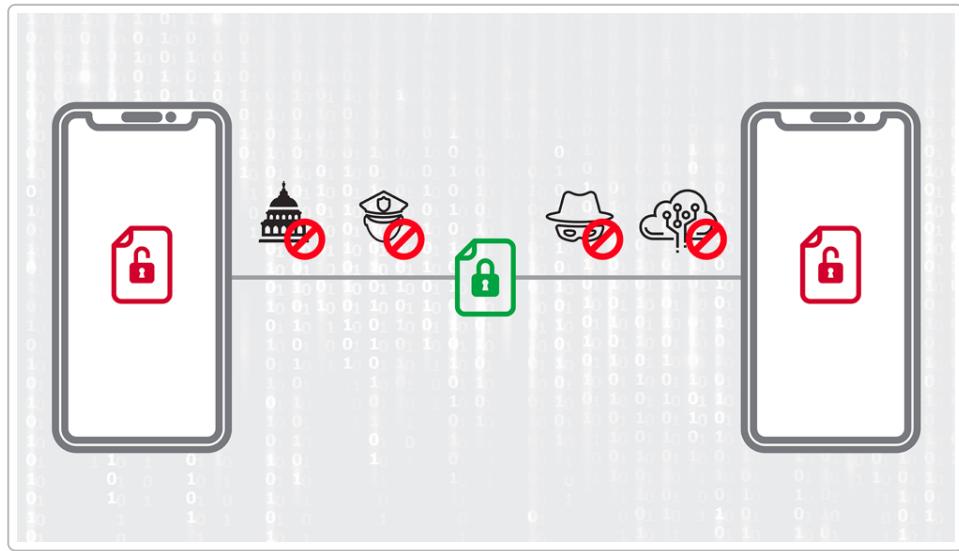


Yapay Zekâ Entegreli Yerli Mesajlaşma Uygulaması Tasarımı

Türkiye'deki kullanıcıların tercih edebileceği **yerli bir mesajlaşma uygulaması** geliştirme fikri, ulusal veri güvenliği ve egemenliği açısından önemlidir. Uluslararası platformlar (WhatsApp, Telegram vb.) milyonlarca kullanıcı verisini yurt dışındaki sunucularında saklar; ABD'nin CLOUD Act gibi yasalar, yabancı şirketlerin bu verileri istihbarat kurumlarıyla paylaşmasını zorunlu kılar ¹. Bu nedenle Türkiye'de kamu ve özel sektör yetkilileri, **yerli ve uçtan uca şifrelemeli** uygulamaları kullanmaya yönlendirilmiştir ². Örneğin Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin 2019 tarihli rehberi, kurumsal iletişimde sunucuları yurt içinde olan yerli uygulamaların kullanılmasını öngörmüştür ². Ayrıca Mobil Casus yazılımı *Pegasus* gibi araçlar, WhatsApp vb. mesajlaşma uygulamalarının hedef alabileceğini göstererek, uçtan uca şifreleme (E2EE) ve yerel sunucu kullanımının ne kadar kritik olduğunu vurgulamıştır ³ ⁴. Bu bağlamda, uçtan uca şifrelemeli, Türkiye'de barındırılan bir mesajlaşma uygulaması, hem gizliliği hem de ulusal güvenliği artıracaktır ⁴.

Uçtan Uca Şifreleme ve Protokoller

Bu tür bir uygulamanın temelinde **uçtan uca şifreleme (E2EE)** olmalıdır. E2EE'de mesajlar cihazda şifrelenir ve sadece alıcı cihazda çözülür; aradaki sunucu hiçbir zaman mesajın düz metnini göremez ⁵. Örneğin, Texas A&M Üniversitesi'nden Dr. Nitesh Saxena'ya göre WhatsApp veya iMessage kullandığınızda, "sadece siz ve alıcı cihaz bu mesajı okuyabilir; uygulama şirketi Meta veya Apple bile göremez" ⁵. Bu sayede iletiler, eğer bir saldırgan veya otorite sunucuya el koysa bile anlamlı hale gelmez.



Şekil: Mesajlar uçtan uca şifreleme ile korunduğunda yalnızca gönderen ve alıcı cihazlar veriyi çözer; ara sunucular veya kötü niyetliler içeriği göremez ⁵.

Uçtan uca şifreleme için **Signal Protokolü** gibi kanıtlanmış yöntemler kullanılabilir. Bu protokolün kalbinde Trevor Perrin ve Moxie Marlinspike tarafından geliştirilen **Çift Tekerlekli (Double Ratchet)** algoritması bulunur ⁶. Double Ratchet, her mesaj için yeni anahtarlar türeterek geçmiş ve gelecekteki mesajların güvenliğini sağlar (ileri gizlilik). 2025 itibarıyla Signal protokolü post-kuantum güvenliği için

Sparse Post-Quantum Ratchet (SPQR) ile güncellenmiştir; böylece gelecekte kuantum saldırılara karşı dayanıklı olacak şekilde CRYSTALS-Kyber şifrelemesi katmanı eklenmiştir⁷.

Yerelde geliştirilen uygulamalarda da benzer teknolojiler uygulanmıştır. Örneğin HAVELSAN'ın **İLETİ** uygulaması, beyaz kutu kriptografisiyle anahtarları yazılım içinde korur ve kurumlara kendi sunucularında kurulum imkânı sunar⁴. Turkcell'in BiP ve Türk Telekom'un Yaay uygulamaları ise tüm veriyi Türkiye'deki veri merkezlerinde tutarak üçüncü taraf erişimini engeller⁸. Bu yaklaşım, mesajların hem iletim hem de depolama aşamasında şifreli kalmasını sağlar. Grup sohbetlerinde ise cihazlar arası anahtar paylaşımını güvenli yapan ek doğrulama adımları (örneğin QR kod veya PIN) gerekebilir. Bu doğrulama süreçleri genellikle kullanıcı hatasına açıktır, bu yüzden otomatik kontroller geliştirilmeli; araştırmacılar "idealde tek bir tuşla işlem onayı" gibi çözümler üzerinde çalışmaktadır⁹.

Yapay Zekâ Entegrasyonu ve Gizlilik

Mesajlaşma uygulamasına entegre edilecek yapay zekâ (LLM) özellikleri (mesaj özeti, otomatik yanıt önerisi vb.) kullanıcı deneyimini zenginleştirebilir. Ancak mevcut pratikte; Google Gemini veya Apple Siri/Intelligence ile mesaj yazmak, o mesajın (geçici de olsa) şirket sunucularına gönderilmesini ve metnin Google/Apple tarafından görülmesini beraberinde getiriyor¹⁰. Örneğin Android'de WhatsApp ile Gemini entegrasyonu kurulduğunda, yazılan mesajlar Google'ın "Gemini Uygulama Etkinliği"ne kopyalanıyor ve varsayılan ayarla kalıcı depolanabiliyor¹⁰. Bu durum, uctan uca şifreleme vaadini bozmaktadır. Birçok kullanıcı, bu araçlar sayesinde "herşeyi yazdıktan sonra" Google veya Apple'ın metni görmediğini varsaya da, gerçekle metin içerikleri bulut sunucularına ulaşıyor¹⁰¹¹.

Bu nedenle bizim uygulamada **LLM tarafının kullanıcı verisi görmemesi** gerekmektedir. Bunun için birkaç yaklaşım vardır:

- **Cihaz içi (on-device) AI:** Kullanıcının cihazında çalışan küçük ölçekli bir model veya embedding sistemi, gelen ve giden mesajlar üzerinde çalışabilir. Böylece veri hiç sunucuya gönderilmez. Ancak mobil donanımlar hâlen büyük dil modellerini çalıştırmaya kâfi gelmemektedir. Bu nedenle büyük özetleme veya analiz işlevleri halen bulut gücüne ihtiyaç duyabilir.
- **Güvenilir Donanım Ortamları (TEE):** Veriyi şifreli olarak sunucuya göndermek ancak verinin yalnızca güvenli bir donanım yongasında çözüldüğü bir ortamda yapay zekâ işlemlerini gerçekleştirmek mümkündür. Stanford Üniversitesi'nden Hazy Research ekibi, **güvenli hesaplama ortam (confidential computing)** kullanarak bir protokol tasarlampostur¹². Bu protokolde, istemci ile sunucu arasında geçici anahtar değiş tokusu ve attestasyon (donanımın doğrulanması) yapılır; mesajlar ancak "enclave" olarak adlandırılan donanım izolasyonu içinde çözülür ve LLM orada çalışır¹². Araştırmacılar, Azure bulutunda NVIDIA H100 veya AMD SEV-SNP gibi teknolojilerle şifre çözme ve model çıkışını yalnızca donanım içindeki bölmede gerçekleştirerek, "gizli sohbetin artık bir fantezi olmadığını" göstermiştir¹². Bu yolla metinler, hem iletişim esnasında hem de işlem sırasında saldırganların veya sunucu operatörlerinin erişemeyeceği hâle gelir.
- **Çok Taraflı Hesaplama (SMPC):** Bir diğer yaklaşım, şifreli veriler üzerinde *Multi-Party Computation* (SMPC) teknikleri kullanmaktadır¹¹¹³. SMPC'de birden fazla taraf verilerini ifşa etmeden ortak bir hesaplama gerçekleştirir. Örneğin hesaplamlar, istemcilerdeki şifreli parçalardan oluştuktan sonra sunucuya gönderilir; sunucu bu parçalar üzerinde işlem yapar ama hiçbir zaman ham veriyi görmez¹¹¹³. Texas A&M Üniversitesi'nden araştırmacılar, "şifrelenmiş veriler üzerinde hiçbir şey açığa çıkarmadan" yapay zekâ özellikleri eklemeye yönelik teknikler üzerinde çalışıklarını belirtmektedir¹¹. Büyük ölçekli LLM'ler için SMPC ve **Homomorfik**

Şifreleme (HE) hâlen performans sınırlamaları nedeniyle tam olarak uygulanabilir olmasa da (özellikle çok büyük modellerde), bu teknolojiler gelişmeye devam etmektedir ¹⁴ ¹⁵.

Bu yaklaşımalar bir arada ele alınabilir. Örneğin kullanıcının gizliliği tehlikeye girmeden sunucu tarafı yapay zekâ işlevi için Apple'ın benimsediği **“Özel Bulut Hesaplama”** (Private Cloud Compute) modeli akla getirilebilir ¹⁶. Apple bu yöntemde, veriyi ancak Apple'ın kontrolündeki özel bir donanım yongasında (teknik olarak güvenli bir ortamda) çözmekte ve işleme almayı hedeflemektedir ¹⁶. Bu durum, teorik olarak OpenAI gibi standart sunucu ortamlarında olduğundan çok daha güçlü bir gizlilik sunar, fakat tamamen şifreleme temelli değildir ve hâlâ merkezi bir sunucuya güven gerektirir ¹⁷. Ayrıca ileriye dönük hazırlık olarak **post-kuantum kriptografi** kullanımı planlanmalıdır. Sinyal protokolündeki SPQR örneğinde olduğu gibi, kuantuma dayanıklı anahtar değişim algoritmaları (örn. CRYSTALS-Kyber) eklenebilir ⁷.

Kısacası, yapay zekâyı entegre ederken kullanıcı verisi **asla düz metin olarak sunucuya gönderilmemeli**; işlem ya tamamen istemci tarafında veya donanım içinde, şifre çözme hakkı kısıtlı bir alanda yapılmalıdır ¹² ¹¹. Elde edilen modeller de kullanıcı verileriyle eğitilmekten ziyade, federatif ya da diferansiyel gizlilik gibi yöntemlerle geliştirilebilir.

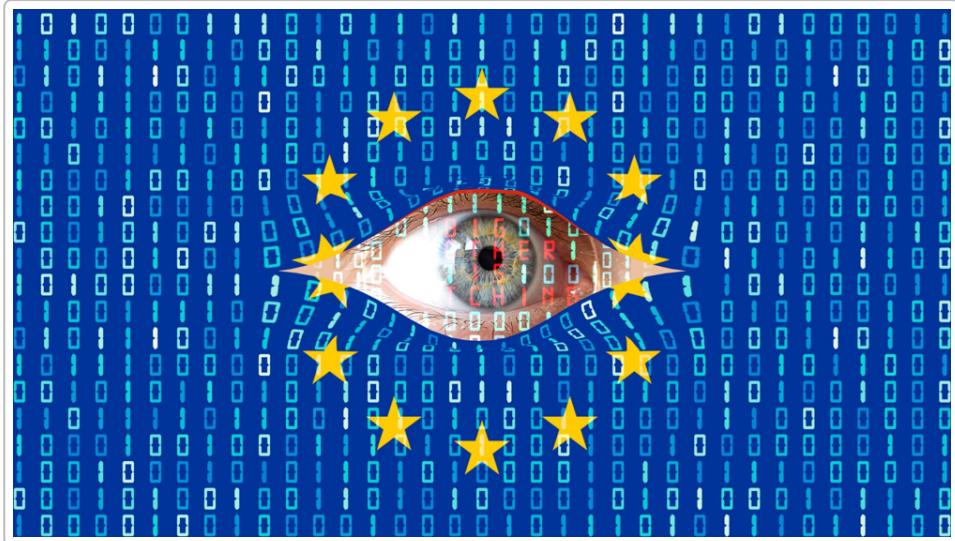
Gizlilik Teknolojileri ve Çok Taraflı Hesaplama

Yukarıda dejindigimiz gibi, **Şifreli Çok Taraflı Hesaplama (SMPC)** ve Homomorfik Şifreleme (HE) gibi ileri kriptografik yöntemler, veri güvenliğini artırmak için etüt edilmelidir. SMPC, birden fazla tarafın özel verilerini paylaşmadan ortak bir hesaplama yapabilmesini sağlar ¹³ ¹⁸. Örneğin hastaneler hastalık tahmini modellerini birbirlerinin verilerini görmeden birlikte eğitebilir veya bankalar müşterilerin gizliliğini ihlal etmeden kara para aklama örüntülerini karşılaştırabilir ¹³.

Bu yaklaşım henüz hesaplama yoğun olsa da, Avrupa veri koruma kuruluşları SMPC'yi “bir sonraki nesil gizlilik teknolojileri”nin merkezi bileşeni olarak görüyor ¹⁹. EDPS'e göre SMPC ile veriler, yalnızca saklanırken değil, hesaplama sırasında da gizli tutulur; geleneksel şifrelemenin ötesinde “işlem sürecinde veri sizmasını” öner ¹³. SMPC'yi güvenilir donanım ve homomorfik şifreleme ile birleştirerek veri güvenliği daha da güçlenebilir ²⁰. Örneğin Microsoft, **Özel Küme Kesişim (Private Set Intersection)** adında, iki tarafın kendi verileriyle kesişimi şifreli biçimde hesaplayıp yalnızca ortak öğeleri öğrenmesini sağlayan protokoller geliştirmiştir ²¹. Bu tür teknikler, kullanıcıların mesaj geçmişi şifreli kalsa bile belirli analizlerin (mesela spam tespiti) yapılmasına izin verebilir.

Yasal Düzenlemeler ve Geleceğe Bakış

Uygulamanın başarısı, teknik güvenliğin yanı sıra yasal uygunluğa da bağlıdır. Avrupa Birliği'nin **“ProtectEU”** stratejisi (Nisan 2025) ile, kolluk kuvvetlerinin şifreli verilere *2030 yılına kadar* etkili biçimde erişebilmesi hedefleniyor ²². Haziran 2025'te açıklanan Yol Haritası'nda E2EE, kolluk birimlerinin “en büyük teknik zorluğu” olarak nitelendirilmiş ²³. Örneğin çıkartılması planlanan kriptografik yol haritası ile 2030'dan itibaren Europol'ün daha ileri deşifre yetenekleri kazanması öngörlüyor ²⁴. Bu durum, uygulamanın tamamen “kapanı kırılmaz” bir şifreleme kullanması durumunda bile devletlerin baskılıarı artabileceği anlamına geliyor.



Şekil: AB Komisyonu'nun "ProtectEU" stratejisinde 2030'a kadar şifreli verilere erişim sağlanması hedefleniyor; rapor, uçtan uca şifrelemenin kolluk için "en büyük teknik zorluk" olduğunu belirtiyor ²² ²³. Bu siyasi ortamda, uygulamada yasa dışı içerikle mücadele ihtiyaçları gözetilerek kullanıcı gizliliğine saygı duyan çözümler geliştirmek gerekecektir.

Türkiye açısından da kamuda yerli uygulama kullanımı teşvik edilmektedir. Örneğin, çeşitli kurumlar WhatsApp vb. yabancı uygulamaları güvenlik zayıflıkları nedeniyle yasaklama eğilimindedir. Fransa ve Rusya gibi ülkeler de benzer şekilde kendi yerel platformlarını zorunlu kılmıştır ²⁵. Uygulama, GDPR benzeri veri koruma mevzuatlarına ve ilerde gelebilecek şifreleme düzenlemelerine uyumlu olmalı; kullanıcı onayı ile sınırlı içerik tarama çözümleri eklemek de bir seçenek olabilir. Ancak genel ilke, verinin şifresiz hiçbir zaman çözülmemesi ve kullanıcının kontrolünde kalmasıdır.

Önerilen Yaklaşımlar ve Yol Haritası

Özetle, planlanan Türkçe mesajlaşma uygulamasında aşağıdaki tedbirlere öncelik verilmelidir:

- **Uçtan uca şifreleme:** Tüm mesaj trafiği şifrelenmeli, anahtarlar sadece kullanıcı cihazlarında tutulmalıdır ⁵ ⁴. Sunucu tarafı hiçbir düz metni veya şifresi çözülebilir veriyi görmemelidir.
- **Güvenli anahtar yönetimi:** Kullanıcı kimlik doğrulaması (örneğin QR kod veya PIN) kolaylaştırılmalı; kullanıcıların doğrulama işlemlerini atlaması engellenmelidir ⁹. Anahtar değişimi güvenilir protokollerle yapılmalıdır.
- **Yerel veri saklama:** Mesaj yedekleri ve kullanıcı verileri Türkiye'deki sunucularda tutulmalı, şifreli biçimde depolanmalıdır ⁸. Böylece üçüncü ülke erişimi ve yasalarından korunma sağlanır.
- **Yapay zekâ entegrasyonu:** AI özellikleri için mümkünse model veya ozet çıkarma istemci tarafından gerçekleştirilmeli; sunucuya gönderilen veriler ancak güvenilir bir donanım ortamında çözülmelidir ¹² ¹¹. Hesaplama sırasında da **şifreli veri işlemeye** yönelik teknolojiler (TEE, SMPC, HE) araştırılmalıdır. Örneğin veriyi şifreli tutup sadece özetini çıkarmaya odaklanan yaklaşımlar üzerinde çalışılabilir.

• **Gizlilik teknolojileri:** Çok taraflı hesaplama ve homomorfik şifreleme gibi yeni şifreleme yöntemleri yakın takip edilmeli, pratik uygulamaları denenmelidir ¹³ ¹⁵. Kuantum bilgisayar tehdidine karşı post-kuantum kriptografi (ör. CRYSTALS-Kyber) kullanılmalı ⁷.

• **Düzenleyici uyum:** Avrupa'nın ve Türkiye'nin veri koruma ve kolluk gereksinimleri izlenmeli, gereklikçe izinli içerik tarama veya yasal zorunluluklar gözetilerek sistem tasarlanmalıdır. Ancak olası düzenlemeler, kullanıcı gizliliğini mümkün olduğunda koruyacak biçimde uygulanmalıdır.

Bu adımlar izlenerek geliştirilecek bir sistem, hem kullanıcıların gizliliğini en üst düzeyde koruyabilir hem de gelecek düzenlemelere uyumlu esneklik sunar. Sonuçta esas amaç, **verilerin şifreli tutulduğu, anlamlı hale getirilmediği ve LLM dahil hiçbir tarafın içeriğe doğrudan erişemediği** bir iletişim platformu kurmaktadır ⁵ ¹¹.

Kaynaklar: Yukarıdaki öneri ve açıklamalar, endüstri araştırmaları ve uzman analizleri (EFF, ACLU, Texas A&M, Stanford Hazy Research, EDPS vb.) ışığında derlenmiştir ¹⁰ ⁵ ²² ¹² ¹³. Bu kaynaklar, güvenli mesajlaşma protokollerini, yapay zekâ entegrasyonu ve gizlilik teknolojileri konularındaki güncel literatürden almıştır.

¹ ² ³ ⁴ ⁸ ²⁵ YERLİ MESAJLAŞMA UYGULAMALARI NEDEN ÖNEMLİ? NEXT ÖRNEĞİYLE DETAYLI BİR İNCELEME

<https://ictmedia.com.tr/yazar/icerik/1190>

⁵ ⁹ ¹¹ Spy Vs. Spy: Texas A&M Researchers Work To Secure Messaging | Texas A&M University Engineering

<https://engineering.tamu.edu/news/2025/05/spy-vs-spy-texas-am-researchers-work-to-secure-messaging.html>

⁶ ⁷ Double Ratchet Algorithm - Wikipedia

https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm

¹⁰ When AI and Secure Chat Meet, Users Deserve Strong Controls Over How They Interact | Electronic Frontier Foundation

<https://www.eff.org/deeplinks/2025/10/when-ai-and-secure-chat-meet-users-deserve-strong-controls-over-how-they-interact>

¹² Mind the Trust Gap: Fast, Private Local-to-Cloud LLM Chat · Hazy Research

<https://hazyresearch.stanford.edu/blog/2025-05-12-security>

¹³ ¹⁹ ²⁰ Secure multi-party computation: powering privacy through collaboration | European Data Protection Supervisor

https://www.edps.europa.eu/press-publications/press-news/blog/secure-multi-party-computation-powering-privacy-through-collaboration_en

¹⁴ ¹⁶ ¹⁷ Let's talk about AI and end-to-end encryption – A Few Thoughts on Cryptographic Engineering

<https://blog.cryptographyengineering.com/2025/01/17/lets-talk-about-ai-and-end-to-end-encryption/>

¹⁵ ²¹ Applications of Homomorphic Encryption and Secure Multi-Party Computation

<https://www.cyberark.com/resources/blog/applications-of-homomorphic-encryption-and-secure-multi-party-computation>

¹⁸ Secure multi-party computation - Wikipedia

https://en.wikipedia.org/wiki/Secure_multi-party_computation

²² ²³ ²⁴ The EU wants to decrypt your private data by 2030 | TechRadar

<https://www.techradar.com/vpn/vpn-privacy-security/the-eu-wants-to-decrypt-your-private-data-by-2030>