



SAKARYA
ÜNİVERSİTESİ

BSM 441

Sistem Yöneticiliği

Dr. Öğr. Üyesi HÜSEYİN ESKI
heski@sakarya.edu.tr

~ Bulut Bilişim ~

Bulut Bilişime Giriş

Modern Bilişim Dünyasının Yeni Paradigması

- **Bulut bilişim nedir?:** Bulut bilişim, verilerin internet üzerinden uzaktaki sunucularda depolanması, işlenmesi ve erişilmesi anlamına gelir. Yerel donanım gerektirmez.
- **Dijital dönüşümün anahtarı:** Kuruluşların esneklik, ölçülebilirlik ve maliyet avantajları sayesinde dijitalleşmeyi hızla benimsemesini sağlar.
- **Günlük hayatımızda yeri:** Google Drive, Dropbox, Netflix gibi hizmetler, kullanıcıların bulut teknolojisini her gün farkında olmadan kullanmalarını sağlar.
- **Kurumsal kullanımın yükselişi:** KOBİ'lerden büyük işletmelere kadar pek çok organizasyon altyapısını buluta taşıyarak operasyonel verimliliklerini artırmaktadır.



Photo by Batu Gezer on Unsplash

Bulut Bilişimin Temel Kavramları

Hizmet Modelleri ve Teknolojik Yapılar

- **IaaS (Infrastructure as a Service)**: Kullanıcıların sanal sunucular, depolama alanı ve ağ kaynaklarına erişim sağladığı hizmet modelidir. Örnek: Amazon Web Services (AWS).
- **PaaS (Platform as a Service)**: Geliştiricilerin uygulama oluşturup çalıştırabildiği platformlar sunar. Örnek: Google App Engine.
- **SaaS (Software as a Service)**: Kullanıcıların yazılımlara internet üzerinden erişip kullanabildiği modeldir. Örnek: Google Docs, Microsoft 365.



Photo by Jonathan on Unsplash

Bulut Bilişimin Avantajları

Kurumsal ve Bireysel Kullanıcılar İçin Kazanımlar

- **Maliyet Tasarrufu:** Donanım, yazılım ve bakım maliyetleri ortadan kalkar. Ödemeler genellikle kullanım bazlı yapılır.
- **Esneklik ve Ölçeklenebilirlik:** İşletmeler ihtiyaç duydukça kaynaklarını artırabilir veya azaltabilir; kapasite sınırlamaları ortadan kalkar.
- **Veriye Her Yerden Erişim:** İnternet bağlantısı olan her yerden verilere erişim sağlanır, mobilite artar.
- **İş Sürekliliği ve Felaket Kurtarma:** Veriler bulutta yedeklendiği için olası felaketlerde veri kaybı riski azalır, sistemler hızla tekrar devreye alınabilir.



Photo by engin akyurt on Unsplash

Bulut Bilişimin Dezavantajları

Riskler, Sınırlamalar ve Güvenlik Endişeleri



Veri Güvenliği ve Gizlilik

Verilerin üçüncü taraf sağlayıcılar tarafından barındırılması, gizlilik ihlali ve yetkisiz erişim risklerini artırır.



Bağlantı Bağımlılığı

Bulut hizmetlerine erişim tamamen İnternet bağlantısına bağlıdır; bağlantı kesintileri hizmet aksamasına yol açabilir.



Uygunluk ve Regülasyon Sorunları

Farklı ülkelerdeki veri koruma yasaları, global bulut çözümlerinin uygulanmasını zorlaştıracaktır.



Kontrol Eksikliği

Kullanıcılar altyapı ve sistemler üzerinde tam kontrol sahibi değildir; teknik aksaklıklarda müdahale sınırlıdır.

Bulut Hizmet Modelleri Karşılaştırması

IaaS, PaaS ve SaaS Arasındaki Farklar



IaaS - Altyapı Katmanı

Donanım kaynaklarının sanallaştırılarak hizmete sunulduğu modeldir. Kullanıcılar işletim sistemi, uygulama ve veri yönetiminden sorumludur.



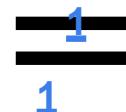
PaaS - Geliştirme Ortamı

Yazılım geliştiricilerin altyapı kurmadan uygulama geliştirmelerini sağlar. Sadece uygulama ve verilerle ilgilenirler.



SaaS - Uygulama Katmanı

Kullanıcılar, sadece uygulamayı kullanır. Tüm altyapı, platform ve yazılım servis sağlayıcı tarafından yönetilir.



Kontrol ve Sorumluluk Seviyeleri

IaaS, kullanıcıya en fazla kontrolü verirken; SaaS modeli en az kontrol ve yönetim gerektirir. PaaS bu iki modelin ortasındadır.

Bulut Bilişim Kullanım Alanları

Farklı Sektörlerde Uygulama Örnekleri



Sağlık Sektörü

Hastane sistemleri hasta bilgilerini bulutta saklayarak uzaktan erişim ve veri paylaşımını kolaylaştırır. Tele-tıp uygulamaları bu altyapıya dayanır.



Eğitim Teknolojileri

Uzaktan eğitim platformları (Zoom, Google Classroom) bulut üzerinde çalışarak esnek ve erişilebilir öğrenme ortamı sunar.



Finansal Hizmetler

Banka ve fintech uygulamaları işlem hızını artırmak, güvenlik sağlamak ve müşteri verilerini analiz etmek için bulut çözümleri kullanır.



Yapay Zeka ve Veri Analitiği

Büyük veri kümeleri bulutta işlenerek makine öğrenmesi modelleri eğitilir; bu da yapay zekanın ölçülebilirliğini artırır.

Sunucu Odalarının Yapılandırılması

Veri Merkezleri için Fiziksel Altyapı ve Güvenlik Gereksinimleri



Fiziksel Güvenlik Önlemleri

Sunucu odaları erişim kontrollü olmalı; biyometrik sistemler, kartlı geçiş ve CCTV kameralarla izlenmelidir.



İklimlendirme ve Soğutma

Yüksek performanslı cihazların aşırı ısınmasını önlemek için hassas sıcaklık ve nem kontrolü gereklidir.



Güç Yedekliliği

UPS sistemleri, jeneratörler ve çift enerji beslemeleri ile elektrik kesintilerine karşı önlem alınmalıdır.



Raf Sistemleri ve Kablolama

Standartlaştırılmış rack yapıları ve düzenli kablolama, hem havalandırma hem de bakım kolaylığı sağlar.

Yangın Güvenliği ve Afet Önlemleri

Sunucu Odaları İçin Kritik Acil Durum Tedbirleri

Yangın Algılama Sistemleri

Duman ve ısı dedektörleri sunucu odalarında erken uyarı sağlar; sistemler genellikle otomatik alarm verir.

FM200 Gazlı Söndürme

Su yerine elektronik donanıma zarar vermeyen FM200 gazı ile yanın söndürme yapılır; etkili ve cihaz dostudur.

Acil Durum Eylem Planları

Yanın, su baskını, deprem gibi durumlarda uygulanacak prosedürler önceden belirlenmiş olmalıdır.

Yedekli Sistemler ve Replikasyon

Verilerin farklı lokasyonlarda yedeklenmesi, afet durumlarda veri kaybını önler ve sistemin devamlılığını sağlar.

Veri Merkezlerinde Fiziksel Ortam Koşulları

Sıcaklık, Nem ve Temizlik Kontrolleri

- **Sıcaklık Kontrolü:** Sunucu ekipmanları belirli sıcaklık aralıklarında çalışmalıdır (genellikle 18-27°C). Aşırı ısınma sistem arızalarına yol açabilir.
- **Nem Düzeyi Yönetimi:** Nem çok düşükse statik elektrik, çok yüksek ise kondenzasyon riski oluşur. 0/040-60 arası nem idealdir.
- **Toz ve Partikül Filtreleme:** Hassas elektronik ekipmanlar için toz büyük bir tehdittir. Filtre sistemleri ve temiz odalar kullanılmalıdır.
- **HVAC Sistemleri:** Isıtma, havalandırma ve iklimlendirme (HVAC) sistemleri kesintisiz çalışmalı; otomatik izleme sistemleri ile kontrol edilmelidir.

/



Photo by m. on Unsplash

Bulut Bilişimde Güvenlik Katmanları

Veri Koruması ve Erişim Denetimi Mekanizmaları



Veri Şifreleme (Encryption)

Veriler hem aktarım sırasında hem de depolama aşamasında şifrelenerek korunur. AES-256 gibi güçlü algoritmalar kullanılır.



Çok Faktörlü Kimlik Doğrulama (MFA)

Kullanıcı girişlerinde yalnızca şifre değil, SMS, biyometrik ya da uygulama doğrulama da istenir.

:C)

Erişim Denetimi ve Yetkilendirme

Kimin, ne zaman, hangi verilere erişeceği sıkı politikalarla kontrol edilir. Role-based access control (RBAC) uygulanır.



Güvenlik Duvarları ve İzleme Sistemleri

Firewall, 10S/IPS gibi sistemler tehditleri tespit eder ve engeller. Anormallikler sürekli izlenir.

Bulut Mimarilerinde Otomasyon ve izleme

Altyapı Yönetiminde Akıllı Sistem Kullanımı

- **Otomasyon ile Kaynak Yönetimi:** Sistemler otomatik olarak kapasite artışı, yedekleme ve güncellemeleri gerçekleştirir. insan müdahalesi minimumdur.
- **İzleme ve Uyarı Sistemleri:** Gerçek zamanlı performans izleme araçları (örneğin: Prometheus, Grafana) sistem sağlığını takip eder.
- **Log Yönetimi ve Analizi:** Sistem günlükleri analiz edilerek anormallikler tespit edilir. Güvenlik tehditleri ve performans düşüşleri erkenden fark edilir.
- **Olay Müdahale Otomasyonu:** Olaylara otomatik yanıt veren sistemler, kesintileri en aza indirir ve müdahale süresini kısaltır.

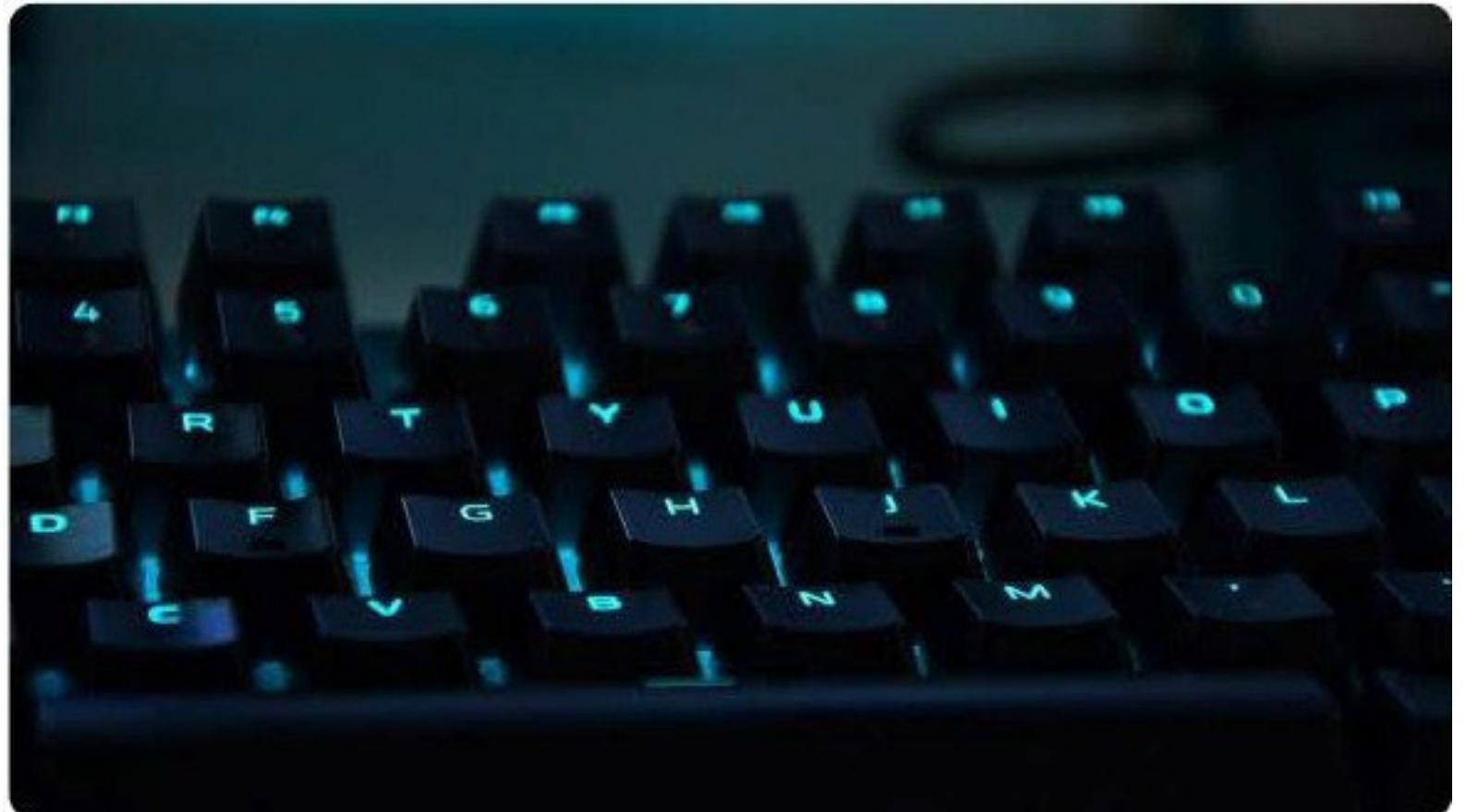


Photo by Anas Alshanti on Unsplash

Yedekleme ve Geri Yükleme Stratejileri

Bulutta Veri Güvenliği ve Süreklik Planlaması



Yedekleme Türleri

Tam yedekleme, artımlı yedekleme ve farklı yedekleme gibi yöntemler, veri koruma stratejilerinin temelini oluşturur.



3-2-1 Kuralı

3 kopya veri, 2 farklı ortam, 1 tanesi farklı fiziksel lokasyonda olacak şekilde yedekleme yapılmalıdır.



Otomatik Yedekleme Sistemleri

Zamanlanmış ve düzenli olarak otomatik çalışan yedekleme sistemleri insan hatasını en aza indirir.



Geri Yükleme Planları ve Testleri

Veri kaybı durumunda geri dönüş süreçleri önceden planlanmalı ve belirli aralıklarla test edilmelidir.

Bulut Bilişimde Mevzuat ve Yasal Düzenlemeler

Veri Gizliliği ve Uyumluluk Gereklilikleri

- **KVKK {Türkiye}:** Kişisel Verilerin Korunması Kanunu, bireylerin kişisel verilerinin işlenmesini ve saklanması düzenler. Bulut sistemlerine özel yükümlülükler getirir.
- **GDPR (AB):** Avrupa Birliği'nin Genel Veri Koruma Tüzüğü, veri işleme süreçlerinde kullanıcı rızası, unutulma hakkı ve veri taşınabilirliğini zorunlu kılar.
- **Veri Lokalizasyonu Gereklilikleri:** Bazı ülkeler verilerin yerel sunucularda saklanması şart koşar. Bulut sağlayıcılarının bu kurallara uyum sağlaması gereklidir.
- **Uyumluluk Denetimleri ve Sertifikalar:** ISO 27001, SOC 2 gibi standartlarla uyumluluk sağlanmalı ve denetim raporları düzenli olarak hazırlanmalıdır.

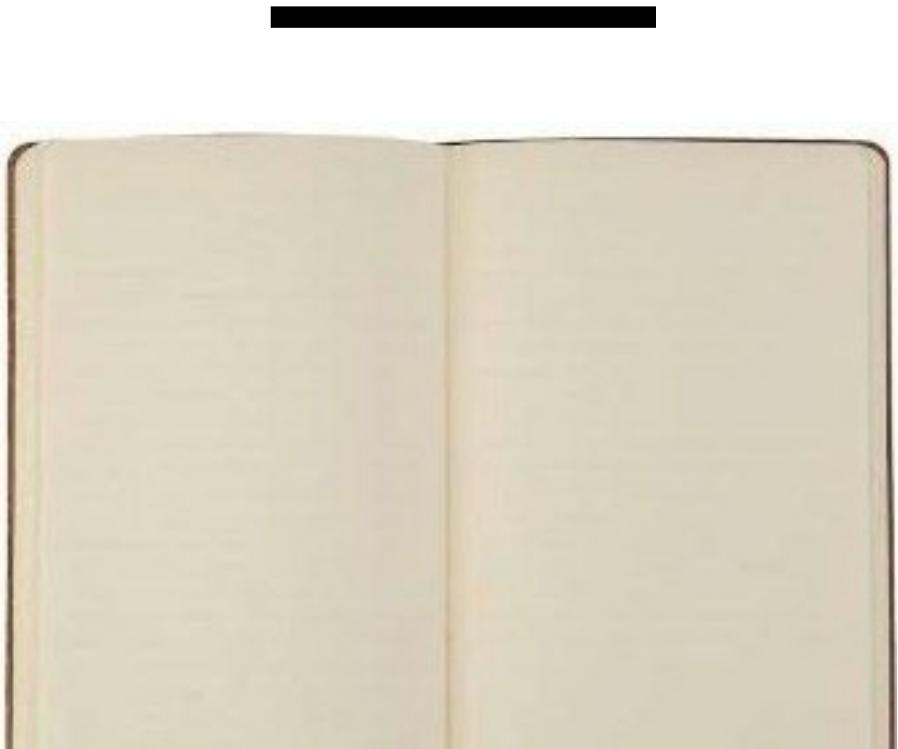


Photo by engin akyurt onUnsplash

Bulut Tabanlı Eğitim Platformları

E-Öğrenmenin Altyapısında Bulut Bilişim



Öğrenme Yönetim Sistemleri (LMS)

Moodle, Google Classroom, Canvas gibi platformlar bulut altyapısı üzerinden çalışarak uzaktan eğitimi mümkün kılar.



Erişilebilirlik ve Süreklilik

Internet bağlantısı olan her yerden, her cihazla eğitime erişim sağlanabilir. Ders materyalleri her zaman güncellenebilir.



Kişiselleştirilmiş Öğrenme

Bulut destekli analitik araçlar sayesinde her öğrencinin öğrenme süreci izlenebilir ve ihtiyaçlara göre şekillendirilebilir.



Veri Saklama ve Paylaşım Kolaylığı

Ders notları, videolar ve sınavlar merkezi bir sistemde saklanarak kolayca paylaşılabilir ve yedeklenebilir.

Bulut Bilişim ve Yapay Zeka Entegrasyonu

AI/ML Modelleri için Güçlü ve Ölçeklenebilir Altyapı



Veri Yoğunluğu ve İşleme Gücü

Yapay zeka sistemleri büyük veri setleriyle çalışır. Bulut, bu verilerin işlenmesi için gerekli kaynakları esnek biçimde sunar.



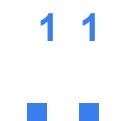
Makine Öğrenmesi Servisleri

AWS SageMaker, Azure ML, Google AI Platform gibi servisler model eğitimi, test ve dağıtım süreçlerini kolaylaştırır.



Tahminleme ve Otomasyon

Müşteri davranış tahmininden ekipman arızası ön görüşüne kadar birçok işlem bulut tabanlı AI sistemleriyle otomatikleştirilebilir.



API ve Entegrasyon Kolaylığı

Hazır AI API'leri (yüz tanıma, konuşma, metin analizleri) bulut sağlayıcıları üzerinden hızlıca entegre edilebilir.

Siber Tehditler ve Savunma Yöntemleri

Bulut Bilişimde Güvenliği Tehdit Eden Unsurlar



DDoS ve Hizmet Kesintisi Saldırıları

Dağıtık hizmet reddi saldırıları sistemleri aşırı yükleyerek erişilemez hale getirir. Bulut platformlarında trafik filtreleme yapılmalıdır.



Ransomware (Fidye Yazılımı)

Verileri şifreleyip karşılığında fidye talep eden kötü amaçlı yazılımlar, bulut sistemleri de hedef alabilir.



Veri İhlalleri ve Yetkisiz Erişim

Kötü yapılandırılmış güvenlik politikaları, hassas bilgilerin sızmasına yol açar. Erişim kontrolü kritik önemdedir.



Siber Savunma Stratejileri

WAF, 10S/IPS sistemleri, güvenlik duvarları ve çok faktörlü kimlik doğrulama gibi önlemlerle sistemler korunur.

Hizmet Seviyesi Anlaşmaları (SLA)

Bulut Sağlayıcıları ile Müşteriler Arasındaki Güvence Mekanizması

- **Uptime Garantisi:** SLA'lar genellikle %99.9 veya üzeri hizmet sürekliliği taahhüdü içerir. Sürekli hizmetin sınırları net olarak belirlenir.
- **Performans ve Yanıt Süresi:** Sistem yanıt süreleri, bant genişliği ve işlem hızları gibi metrikler SLA kapsamında takip edilir.
- **Veri Güvenliği ve Yedeklilik:** SLA'lar veri bütünlüğü, yedekleme sıklığı ve güvenlik protokollerine dair standartları da kapsayabilir.
- **İhlal Durumunda Yaptırımlar:** SLA ihlalleri durumunda hizmet kredileri, para iadesi veya sözleşme feshi gibi yaptırımlar uygulanabilir.



Photo by ThisisEngineering RAEng on Unsplash

Maliyet Yönetimi ve Optimizasyon

Bulut Kullanımında Verimli Kaynak Dağılımı

0

Kaynak Kullanımı İzleme

Kullandığın kadar öde (pay-as-you-go) modeli, kaynak kullanımının sürekli takip edilmesini zorunlu kılar.



Gereksiz Servisleri Tespit Etme

Atıl durumda kalan sanal makineler, kullanılmayan depolama birimleri tespit edilip devre dışı bırakılmalıdır.

X

Rezervasyon ve Taahhüt İndirimleri

Uzun süreli taahhütlerle veya rezerve örneklerle %40'a varan indirimler elde edilebilir.



Maliyet Analitik Araçları

AWS Cost Explorer, Azure Cost Management gibi araçlarla raporlama, trend takibi ve bütçe kontrolü yapılabilir.

Genel Değerlendirme ve Kapanış

Bulut Bilişim Yolculuğuna Veda

- **Kavramları Pekiştirdik:** Temel bulut hizmet modellerinden dağıtık mimariye, güvenlikten felaket kurtarmaya kadar geniş bir yelpazeyi inceledik.
- **Avantaj ve Riskleri Tarttık:** Bulutun sunduğu esneklik, maliyet avantajı ve erişilebilirlik kadar, güvenlik ve gizlilik konularındaki dikkat edilmesi gerekenleri de değerlendirdik.
- **Güncel Uygulamalara Odaklandık:** Yapay zeka entegrasyonundan CI/CD süreçlerine kadar bulutun endüstrilere nasıl entegre olduğunu gördük.
- **Birlikte Öğrendik:** Bu sunum sadece bilgi aktarmak değil; tartışmak, keşfetmek ve birlikte öğrenmek amacı taşıyordu.

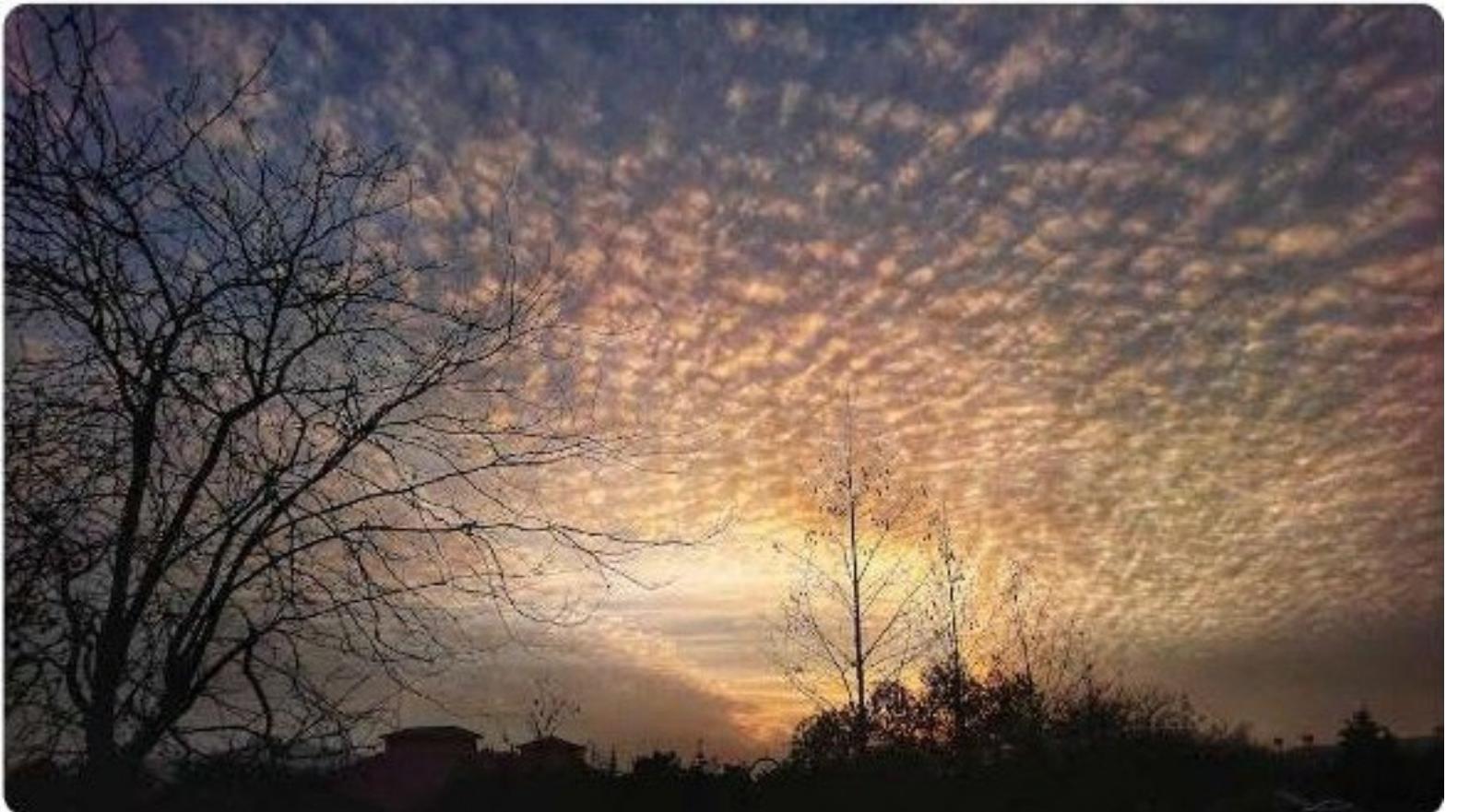


Photo by Atilla Bingöl on Unsplash