

ÜCRETSİZ DERS NOTU ÖZETİ

Bilgi Sistemleri İşletimi

Bağımsız Denetim Lisansı

Bilgi sistemleri işletim ve operasyon yönetimi

Bu PDF'teki bölüm	6 bölüm
Modüldeki toplam bölüm	24 bölüm
Formül sayısı	0 formül
Son güncelleme	17 Eylül 2026

Bu belge **Bilgi Sistemleri İşletimi** modülünün ücretsiz bölümlerinden derlenmiştir. Tamamı ve güncel hâli:

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-isletimi>

İçindekiler

1. Bilgi Sistemleri Altyapısı ve Sunucu Teknolojileri
2. Bilgi Sistemleri Altyapısı ve Sunucu Teknolojileri • Bilgi Sistemleri Altyapısı, Sunucu Türleri ve Donanım Yönetimi
3. Bilgi Sistemleri Altyapısı, Sunucu Türleri ve Donanım Yönetimi • Donanım Bakımı, İşletim Sistemleri, Sanallaştırma ve Veri Yönetiřimi
5. Donanım Bakımı, İşletim Sistemleri, Sanallaştırma ve Veri Yönetiřimi • Veri Yönetimi, Veri Tabanı Sistemleri ve Veri Modelleme
6. Veri Yönetimi, Veri Tabanı Sistemleri ve Veri Modelleme • Sistem Arayüzleri, Bulut Biliřim ve Büyük Veri Teknolojileri

Bu PDF, **Bilgi Sistemleri İşletimi** ders notunun ücretsiz olarak yayımlanan ilk 6 bölümünü içerir. Modülün tamamı 24 bölümden oluşur; kalan 18 bölüm ile soru bankası, sesli anlatım ve deneme sınavları finlisans.com üzerinde yer alır.

Bölümler web sayfasında birbiriyle örtüşecek şekilde hazırlandığı için, bu PDF’te aynı maddenin ikinci ve sonraki tekrarları ayıklanmıştır (181 yinelenen madde). Madde sırası ve bölüm numaraları web sayfasıyla aynıdır.

1. Bilgi Sistemleri Altyapısı ve Sunucu Teknolojileri

Temel Kavramlar

- Çekirdek (Kernel): İşletim sisteminin en temel seviyesinde yer alan; kesinti işleme, işlem yönetimi ve bellek tahsisi gibi kritik görevleri yürüten, kullanıcı erişiminin kısıtlandığı ayrıcalıklı alandır.
- Aritmetik Mantık Birimi (ALU): Merkezi işlem birimi (CPU) içerisinde yer alan ve bilgisayarın gerçekleştirdiği tüm matematiksel hesaplamalar ile mantıksal karşılaştırma işlemlerinden sorumlu olan temel alt birimdir.
- Ana Bellek (RAM): Bilgisayarın çalışması için zorunlu olan, verilerin geçici olarak tutulduğu, yüksek hızlı ancak cihaz kapatıldığında içindeki bilgilerin silindiği birincil depolama ünitesidir.
- Grafik İşleme Birimi (GPU): Merkezi işlemciye göre daha fazla ALU içeren, bilgisayar grafiklerini işlemenin yanı sıra büyük veri ve yapay zeka gibi alanlarda yüksek işlem kapasitesi sunan verimli bir donanımdır.
- Ana Çatı (Mainframe) Bilgisayarlar: Günlük 1 trilyona kadar işlem yapabilen, en üst düzey güvenlik ve güvenilirlik sunan, büyük kuruluşların merkezi veri işleme ve veri ambarı ihtiyaçları için tasarlanmış yüksek performanslı sistemlerdir.
- İnce İstemci (Thin Client): Kendi yerel depolama birimi bulunmayan, işlem yapabilmek veya uygulama kullanabilmek için mutlaka bir sunucu bilgisayara erişmek zorunda olan, minimum donanımlı kişisel bilgisayar türüdür.
- Eşler Arası Model (P2P): Merkezi bir otoriteye ihtiyaç duymadan, ağdaki her kullanıcının teorik olarak ağın sahibi ve ortağı olduğu, taraflar arasında doğrudan bilgi veya varlık paylaşımı sağlayan mimaridir.
- İstemci-Sunucu Mimarisi: Verilerin merkezi bir sunucuda toplandığı, istemcilerin belirli bağlantı noktaları (port) üzerinden hizmet talep ettiği ve yönetimin merkezden sağlandığı, günümüzde en yaygın kullanılan ağ modelidir.
- Uygulama Sunucusu: Birden fazla kullanıcı tarafından paylaşılan ve genellikle yüksek kaynak gerektiren uygulamaları barındıran, istemciden gelen talepleri ilgili yazılıma ileterek sonuçları geri döndüren sunucudur.
- Web Sunucusu: İnternet sitelerinin içeriğini URL üzerinden talep eden kullanıcılara sunan, HTTP (port 80) veya HTTPS (port 443) protokollerini kullanarak GET ve POST isteklerini karşılayan sistemdir.
- Veri Tabanı Sunucusu: Yoğun miktarda verinin iş ihtiyaçlarına göre saklanmasını sağlayan DBMS yazılımlarını barındıran, performans ve güvenlik gerekçesiyle genellikle uygulama sunucusundan ayrı tutulan birimdir.
- Dosya Sunucusu: İşletme içindeki tüm dosyaların merkezi olarak saklandığı, kullanıcıların yetkileri dahilinde erişebildiği ve yedekleme işlemlerinin tek merkezden yönetilmesini sağlayan sunucu formudur.
- Donanım (Hardware): Bilgisayarın fiziksel, elle tutulur parçalarıdır.
- Yazılım (Software): Donanımın iş yapmasını sağlayan komutlar bütünüdür.
- Kernel (Çekirdek): İşletim sisteminin donanımla doğrudan etkileşime giren, bellek ve süreç yönetimi yapan en yetkili parçasıdır.
- CPU (MİB): Veri ve komutları işleyen, bilgisayarın beyni olarak nitelenen merkezi işlem birimidir.
- RAM (Ana Bellek): Bilgisayarın geçici, yüksek hızlı birincil depolama birimidir; güç kesilince veri silinir.
- Mainframe: Günlük 1 trilyona kadar işlem yapabilen, devasa işlem hacmine sahip güvenilir merkezi bilgisayar sistemidir.
- GPU: Grafik verilerini işlemek için tasarlanmış, CPU'dan daha fazla ALU içeren ve yapay zeka/blok zincirde verimli kullanılan birimdir.

Önemli Noktalar

- Ana bilgisayarlar (Mainframe), en yüksek düzeyde güvenlik ve güvenilirlikle günlük 1 trilyona kadar işlem yapabilecek kapasitede tasarlanmıştır.
- Dizüstü bilgisayarlar, taşınabilir olmaları için genellikle 5 kilogramın altında ağırlığa sahip olacak şekilde tasarlanır ve pil sayesinde elektrik kesintilerine dayanıklıdır.

Önemli Noktalar

- Web sunucularında standart (şifrelenmemiş) iletişim için 80 numaralı port, güvenli (şifreli) HTTPS iletişimi için ise 443 numaralı port kullanılır.
- Web sunucusu isteklerinde 'GET' sadece bilgi almak için kullanılırken, 'POST' istemcinin sunucuya veri göndermesi ve yanıt beklemesi durumunda kullanılır.
- Güvenlik, performans ve yönetim kolaylığı sağlamak amacıyla uygulama sunucusu ile veri tabanı sunucusunun farklı sunucularda işletilmesi iyi bir uygulama örneğidir.
- Bilgisayar hiyerarşisinde en temel seviyede donanım (firmware dahil) bulunur, onun üzerinde ise kernel (çekirdek) fonksiyonları yer alır.
- İkincil depolama birimleri (HDD, SSD, Optik) verinin kalıcı saklanması için şarttır ancak bilgisayarın temel çalışması için RAM gibi zorunlu birincil birim değildir.
- Bilgisayar mimarisi Firmware -> Kernel -> Sistem Yazılımı -> Uygulama katmanlarından oluşur.
- İstemci-Sunucu mimarisinde sunucu trafiği bağlantı noktaları (port) üzerinden yönetir.
- Web trafiğinde HTTP için 80, HTTPS için 443 portu standarttır.
- Dizüstü bilgisayarlar 5 kg altındaki taşınabilir sistemler olarak tanımlanır.
- İnce istemciler (Thin Client) kendi diskine sahip olmayan ve sunucuya bağımlı cihazlardır.

Sık Yapılan Hatalar

- RAM ve İkincil Depolamanın karıştırılması: RAM geçicidir, SSD/HDD kalıcıdır.
- ALU ve Kontrol Birimi görevlerinin karıştırılması: ALU hesaplar, Kontrol Birimi yönetir.
- Süper Bilgisayar ve Mainframe farkı: Süper bilgisayar karmaşık hesaplama, Mainframe yüksek işlem hacmi içindir.

2. Bilgi Sistemleri Altyapısı ve Sunucu Teknolojileri • Bilgi Sistemleri Altyapısı, Sunucu Türleri ve Donanım Yönetimi

Temel Kavramlar

- GET İsteği: İstemcinin sunucudan yalnızca bilgi almak istediği, sunucuya gönderecek ek verisinin bulunmadığı durumlarda kullanılan temel web protokolü isteğidir.
- POST İsteği: İstemcinin sunucuya form verisi gibi içerikler göndermek için kullandığı ve işlem sonucunda sunucudan mutlaka bir yanıt beklediği istek türüdür.
- SPF (Sender Policy Framework): Bir etki alanı adına e-posta göndermeye yetkili sunucuları DNS TXT kaydıyla listeleyen ve kimlik sahtekarlığını önleyen e-posta doğrulama protokolüdür.
- DKIM (Alan Anahtarı Tanımlı Posta): E-postanın yetkili sunucudan geldiğini ve içeriğinin yolda değiştirilmediğini kriptografik imzalar kullanarak doğrulayan SPF'den daha gelişmiş bir yöntemdir.
- DMARC: SPF ve DKIM protokolleri üzerine kurulu, alıcıya sahte e-postalarla ilgili ne yapması gerektiğini bildiren ve raporlama yeteneği sunan bir üst protokoldür.
- Vekil (Proxy) Sunucu: İstemci ile hedef sunucu arasında aracı olan, gerçek IP adresini maskeleyebilen, içerik filtreleme ve log tutma amacıyla kullanılan sunucu uygulamasıdır.
- DNS (Alan Adı Sunucusu): İnternet üzerindeki URL adreslerini hiyerarşik bir yapıda karşılık gelen sayısal IP adreslerine çeviren, 53 numaralı portu kullanan kritik bir servistir.
- DHCP Sunucusu: Ağdaki cihazlara manuel müdahale gerekmesizin dinamik olarak IP adresi ve ağ ayarları atayan, UDP 67 portu üzerinden çalışan yapılandırma protokolüdür.
- Atlama (Jump) Sunucusu: Farklı güvenlik seviyelerindeki bölgeler arasında kontrollü geçiş sağlayan, sıkılaştırılmış ve DMZ gibi kritik alanları yönetmek için kullanılan cihazdır.
- HSM (Donanım Güvenlik Modülü): Kriptografik anahtarları fiziksel olarak koruyan, FIPS 140 standartlarına uygun, yazılımsal çözümlere göre daha yüksek güvenlik sağlayan elektronik cihazdır.
- Sanallaştırma: Bir fiziksel sunucu üzerinde özel yazılımlar aracılığıyla birden fazla bağımsız sanal makine çalıştırarak donanım kaynaklarını verimli kullanma yöntemidir.
- Önleyici Bakım: Donanımlarda henüz bir arıza oluşmadan, tedarikçi önerileri doğrultusunda rutin olarak yapılan ve sistemin ömrünü uzatmayı amaçlayan bakım faaliyetidir.
- Web Sunucusu: Web sitesi uygulamalarını çalıştıran ve GET/POST isteklerine yanıt veren uygulama sunucusudur.
- SPF (Sender Policy Framework): Bir etki alanı için e-posta göndermeye yetkili sunucuları listeleyen DNS TXT kayıdır.
- DKIM: E-postaların içeriğinin değiştirilmediğini kriptografik imzalarla doğrulayan protokoldür.
- DMARC: SPF ve DKIM sonuçlarını raporlayan ve başarısızlık durumunda ne yapılacağını belirleyen politikadır.
- Jump Server (Atlama Sunucusu): Güvenli bölgeler arasındaki erişimi kontrol eden sıkılaştırılmış geçiş bilgisayarıdır.
- HSM: Kriptografik anahtarları koruyan yüksek güvenli donanım modülüdür.

Önemli Noktalar

- HTTP trafiği için şifresiz 80 portu kullanılırken, güvenli ve şifreli HTTPS trafiği için 443 portu kullanılmaktadır.
- E-posta sistemlerinde gönderim için SMTP (Port 25/587), alım için ise POP3 (Port 110) protokolleri standarttır.
- SPF protokolü, kullanıcı e-postalarını başka bir adrese yönlendirdiğinde işlevini yitirmekte; bu açık DKIM ile kapatılmaktadır.
- DNS sunucuları hem TCP hem de UDP protokolleri üzerinden 53 numaralı bağlantı noktasını kullanmaktadır.

Önemli Noktalar

- HSM cihazlarının uluslararası FIPS 140 ve Common Criteria EAL4+ güvenlik standartlarına uygun olması zorunluluktur.
- Aktif RFID etiketleri pille çalışır, pasif etiketlere göre daha uzun mesafeden iletişim kurabilir ancak daha maliyetlidir.
- Donanım bakım faaliyetleri kurum dışı personelce yapıldığında, işlem boyunca refakat edilmeli ve bitişte erişim izinleri derhal iptal edilmelidir.
- Sanallaştırma sayesinde bir fiziksel sunucudaki boş kaynaklar, ihtiyaç duyan diğer sanal sunuculara kaydırılarak maliyet avantajı sağlanır.
- HTTP 80, HTTPS 443, SMTP 25, DNS 53 ve DHCP 67 portlarını kullanır.
- Veri tabanı sunucuları yüksek kaynak tüketimi nedeniyle uygulama sunucularından ayrılmalıdır.
- Sanallaştırma, donanım kaynaklarının paylaşılmasını sağlayarak maliyet avantajı ve yönetim kolaylığı sunar.
- RFID riskleri arasında gizlilik, iş zekası sızıntısı ve süreç kesintileri yer alır.
- Donanım bakımı; önleyici (rutin) ve düzeltici (arıza sonrası) olarak ikiye ayrılır.

Sık Yapılan Hatalar

- Hata: GET ve POST isteklerinin aynı amaçla kullanıldığının sanılması. Doğrusu: GET veri çekmek, POST veri göndermek için kullanılır.
- Hata: SPF'nin tüm e-posta sahteciliğini tek başına önlediği düşüncesi. Doğrusu: SPF yönlendirmelerde çalışmaz, DKIM ve DMARC ile desteklenmelidir.
- Hata: Sanal sunucuların fiziksel sunucudan tamamen bağımsız kaynaklara sahip olduğunun sanılması. Doğrusu: Sanal sunucular fiziksel sunucunun CPU ve RAM'ini paylaşır.
- Hata: Donanım bakımının sadece arıza anında yapılacağı düşünülmesi. Doğrusu: Arıza öncesi yapılan önleyici bakım, sistem sürekliliği için kritiktir.
- Hata: HSM'nin sadece bir yazılım olduğunun sanılması. Doğrusu: HSM fiziksel bir donanımdır ve yazılım tabanlı modüllerden daha yüksek güvenlik sunar.
- SPF ve DKIM'in mesajı şifrelediğini sanmak (Sadece kimlik doğrularlar).
- Düzeltici bakımı rutin bir faaliyet olarak karıştırmak (Arıza durumunda yapılır).
- SMTP'nin doğuştan güvenli bir protokol olduğunu düşünmek (Güvenlik sonradan eklenmiştir).

3. Bilgi Sistemleri Altyapısı, Sunucu Türleri ve Donanım Yönetimi • Donanım Bakımı, İşletim Sistemleri, Sanallaştırma ve Veri Yönetimi

Temel Kavramlar

- **Düzeltilici Bakım:** Bir sorun ortaya çıktığında, hizmet masası seviyesinde veya üretici desteğiyle çözülmek üzere yapılan ve donanım çeşitlendikçe karmaşıklığı artan bakım türüdür.
- **Erişilebilirlik Raporları:** Donanımların kullanıcılar tarafından kullanılabilirliği süreleri gösteren, yetersiz kapasite veya eğitim eksikliği gibi kesinti nedenlerini belirleyen raporlardır.
- **Varlık Yönetimi Raporları:** İşletmedeki bilgisayar, sunucu, ağ cihazı ve mobil cihaz gibi tüm donanımların güncel envanterini sağlayan, varlık yönetimi uygulamaları için kritik raporlardır.
- **API (Application Programming Interface):** Uygulamaların donanıma doğrudan erişimi olmadığından, işletim sisteminin sunduğu ve donanımla etkileşimi sağlayan küçük programcıklardır.
- **Kernel (Çekirdek):** İşletim sisteminin en temel bileşeni olup ana bellek, işlemci ve aygıtlar üzerinde doğrudan kontrole sahip olan, donanım ile yazılım arasındaki arayüzdür.
- **Sanal Bellek (Paging):** İşlerin ihtiyaç duyduklarından daha az fiziksel bellek ile çalışabilmelerini sağlayan, bellek yönetiminin bir parçası olan iyileştirme tekniğidir.
- **En Az Ayrıcalık İlkesi:** Süreçlerin işlevlerini yerine getirmek için sadece gereken yetkiye, sadece yeterli süre boyunca sahip olması gerektiğini savunan temel güvenlik ilkesidir.
- **Kayıt Defteri (Registry):** Windows işletim sistemlerinde önemli sistem seçeneklerinin ve parametrelerinin ayarlandığı, denetçiler için kritik öneme sahip özel yapılandırma dosyalarıdır.
- **CIS (The Center for Internet Security):** Sistemler için aktif izin parametreleri ve port ayarları gibi sıkılaştırılmış baz konfigürasyon önerileri yayınlayan bağımsız ve küresel bir organizasyondur.
- **Hipervizör (Sanallaştırma Yazılımı):** Doğrudan donanıma veya işletim sistemi üzerine kurularak fiziksel kaynakları sanal ortamlara bölen ve kaynak dağıtımını yöneten yazılım katmanıdır.
- **NFV (Ağ Fonksiyonlarını Sanallaştırma):** Dizin hizmetleri ve IP yapılandırması gibi ağ işlevlerini fiziksel cihazlardan ayırarak farklı ortamlar arasında dağıtılmasına olanak sağlayan teknolojidir.
- **Veri Yönetimi:** Kurumsal verinin güvenliği, kalitesi ve yaşam döngüsünün iş hedefleriyle uyumlu şekilde yönetilmesi için oluşturulan stratejik ve operasyonel çerçevedir.
- **Düzeltilici Bakım:** Bir sorun ortaya çıktığında onu düzeltmek amacıyla yapılan müdahale.
- **Kernel (Çekirdek):** İşletim sisteminin donanım ve yazılım arasındaki iletişimi yöneten en temel bileşeni.
- **Hipervizör:** Fiziksel kaynakları sanal makinelere bölen sanallaştırma yazılımı.
- **API:** Uygulamaların işletim sistemi hizmetlerine (donanım erişimi vb.) ulaşmasını sağlayan arayüz programcıkları.
- **Veri Sözlüğü:** Meta verilerin (veri tanımları ve ilişkileri) tutulduğu merkezi yapı.
- **CIS Benchmarks:** Sistemleri güvenli hale getirmek için kullanılan bağımsız baz konfigürasyon önerileri.

Önemli Noktalar

- Kurum dışı bakım personeli, uzaktan erişim dahil tüm faaliyetlerde kurum çalışanlarının refakatinde olmalı ve iş bitiminde erişim izinleri derhal geri alınmalıdır.
- Resmi bakım planları için yönetim onayı alınmalı, bütçeyi aşan bakım maliyetlerinin sebepleri denetçi tarafından mutlaka sorgulanmalıdır.
- Performans raporlarının anlamlı olması için kabul edilebilir kesinti süresi ve eşik değerler gibi hedeflerin (SLA) önceden belirlenmiş olması şarttır.
- Donanım tedarik süreci 'gerektiği zaman' yaklaşımı yerine yazılı bir planla, merkezi bir birim tarafından ve fayda/maliyet analizi yapılarak yönetilmelidir.
- Linux tabanlı sunucular, lisans ücreti gerektirmediği için Windows tabanlı sunuculara göre kurulum ve bakım maliyeti açısından daha avantajlıdır.
- Sanallaştırmada, hassas verilerin ve kritik uygulamaların yer aldığı sanal sunucuların diğer kuruluşlarla aynı fiziksel sunucuda (paylaşımlı) bulunmaması önerilir.

Önemli Noktalar

- İşletim sistemi denetiminde sunucular üzerindeki açık portlar, gereksiz servisler ve yetkili kullanıcıların işlem iz kayıtları (logs) mutlaka incelenmelidir.
- Veri kalitesi COBIT 2019'a göre İçsel (kesinlik, nesnellik vb.) ve Bağlamsal (ilgililik, tamlık vb.) olmak üzere iki ana kategoride değerlendirilir.
- Bakım faaliyetleri kritik iş saatleri dışında planlanmalı ve mutlaka yönetim onaylı bir plan dahilinde yürütülmelidir.
- Uzaktan bakım erişimlerinde izinler işlem bazlı verilmeli, loglanmalı ve iş bitince derhal geri alınmalıdır.
- Performans izleme proaktif bir süreçtir; sadece raporlama yetmez, eşik değerlere göre aksiyon alınmalıdır.
- Donanım tedariki 'gerektiği zaman' değil, kurumsal mimari ve iş planlarıyla uyumlu bir yazılı planla yapılmalıdır.
- İşletim sistemi bütünlüğü için 'en az ayrıcalık' ilkesi uygulanmalı ve süreç izolasyonu sağlanmalıdır.
- Hassas veriler, paylaşımlı bulut ortamlarında diğer kuruluşlarla aynı fiziksel sunucuda barındırılmamalıdır (izolasyon riski).

Sık Yapılan Hatalar

- Rutin bakımı plansız veya en yoğun saatte yapmak.
- Sadece rapor almayı performans yönetimi sanmak (analiz ve aksiyon eksikliği).
- Dış personelin sisteme refakatsiz veya süresiz yetkiyle erişmesine izin vermek.
- İşletim sistemi denetiminde sadece yüzeysel ayarlara bakıp yapılandırma dosyalarını (Registry vb.) atlamak.

5. Donanım Bakımı, İşletim Sistemleri, Sanallaştırma ve Veri Yönetimi • Veri Yönetimi, Veri Tabanı Sistemleri ve Veri Modelleme

Temel Kavramlar

- Veri Yönetimi: Verilerin güvenli, verimli ve uygun maliyetli şekilde toplanması, saklanması ve politika/düzenlemeler dâhilinde kullanımının optimize edilmesini sağlayan süreçlerin bütünüdür.
- İçsel Veri Kalitesi: COBIT 2019 çerçevesinde verinin gerçek değerlerle uyumunu ifade eden; kesinlik, nesnellik, inanılabilirlik ve itibar kriterlerini kapsayan kalite alt başlığıdır.
- Bağlamsal Veri Kalitesi: Verinin kullanıcının görevine uygunluğunu, ilgililik, tamlık, geçerlilik ve yeterlilik gibi kriterlerle ölçen ve kalitenin kullanım amacına bağlı olduğunu kabul eden boyuttur.
- Veri Yaşam Döngüsü: Verinin planlama ve tasarım aşamalarıyla başlayıp, geliştirme, kullanım (saklama, paylaşma, izleme) ve nihayetinde elden çıkarma/imha süreçlerini kapsayan varlık süresidir.
- Veri Akış Şeması (DFD): Verilerin sistemdeki girdi, çıktı, kaynak ve depolama noktalarını grafiksel olarak gösteren, ancak süreçlerin zamanlaması veya sırası hakkında bilgi içermeyen modelleme aracıdır.
- İlişkisel Veri Tabanı: Verilerin yapılandırılmış tablolar halinde tutulduğu, SQL diliyle yönetilen ve çok yönlü ilişkileri yönetebilen ancak yapılandırılmamış veriler için uygun olmayan altın standart modeldir.
- NoSQL Veri Tabanı: İlişkisel modelin aksine yapılandırılmamış büyük miktardaki veriyi tablo formatına dönüştürmeden hızlıca işleyebilen ve dağıtık yapıda çalışabilen veri tabanı sistemidir.
- Veri Ambarı (Data Warehouse): Anlamlı iş iç görüleri elde etmek için heterojen kaynaklardan gelen verileri birleştiren, operasyonel veri tabanından ayrı tutulan ve iş zekâsı sistemlerinin çekirdeğini oluşturan ortamdır.
- Kavramsal Veri Modeli: Sistemin neyi içereceğini, varlık sınıflarını ve iş kurallarını en yüksek soyutlama düzeyinde sunan, genellikle proje gereksinimleri toplama aşamasında oluşturulan büyük resimdir.
- Mantıksal Veri Modeli: Veri türleri ve uzunlukları gibi öznitelikleri belirten, varlık ilişkilerini gösteren ancak herhangi bir teknik sistem gereksinimi içermeyen, orta seviye soyutlamaya sahip modeldir.
- Fiziksel Veri Modeli: Verilerin veri tabanında nasıl depolanacağını gösteren, ilişkisel tabloları ve anahtarları içeren, en az soyut ve performansa yönelik teknik özellikleri barındıran nihai tasarımıdır.
- Normalleştirme: Veri tekrarını önlemek için tanımlayıcı anahtarlar kullanarak verileri gruplandıran, depolama alanını azaltan ancak sorgu performansı maliyeti yaratabilen bir düzenleme tekniğidir.
- Ara Katman Yazılımı (Middleware): Uygulama katmanı ile işletim sistemi arasında yer alan, iki ayrı uygulamayı birbirine bağlayarak veri akışını ve iletişim kanalını sağlayan otomatikleştirilmiş arayüz çözümüdür.
- Sistem Arayüzü: İki veya daha fazla donanım, yazılım veya uygulama programının insan müdahalesi olmaksızın otomatik veri aktarımı ve etkileşim sağladığı fonksiyonel ve fiziksel bağlantı noktalarıdır.
- Veri Kalitesi: COBIT 2019'a göre İçsel (Kesinlik, Nesnellik vb.) ve Bağlamsal (İlgililik, Tamlık vb.) olarak iki ana kategoride değerlendirilir.
- Veri Yaşam Döngüsü: Planlama, Tasarım, Geliştirme, Kullanım/İşletim ve Elden Çıkarma aşamalarından oluşan süreç.
- NoSQL: Yapılandırılmamış veriler için esnek; Key-Value, Document, Column Store ve Graph türleri bulunan veri tabanı modeli.
- Veri Ambarı (DW): Heterojen kaynaklardan gelen verilerin iş zekâsı ve analiz için toplandığı stratejik ortam.
- Ara Katman (Middleware): Farklı uygulama veya sistemler arasında veri akışını sağlayan yapıştırıcı yazılım.

Önemli Noktalar

- Veri Akış Şemaları (DFD), süreçlerin zamanlaması veya paralel/seri çalışma sırası hakkında kesinlikle bilgi içermez.
- Veri ambarı bir ürün değil, operasyonel veri tabanından ayrı tutulan mimari bir ortamdır.

Önemli Noktalar

- Yedekleme politikası oluşturulurken iş etki analizi yapılmalı ve iş birimlerinin kesinti/kayıp tahammül süreleri (yasal zorunluluklar dahil) esas alınmalıdır.
- Şifrelenmiş verilere erişim için kullanılan şifreleme anahtarları (verisi) sınırlı erişime sahip olmalı ve belirli zamanlarda mutlaka değiştirilmelidir.
- Kişiden kişiye veri iletimi (e-posta eki vb.), izlenmesi ve güvenliğinin sağlanması en zor olan veri akış türüdür.
- Veri modelleme süreci hiyerarşik olarak Kavramsal Model ile başlar, Mantıksal Model ile detaylanır ve Fiziksel Model ile sonuçlanır.
- Normalleştirme işlemi depolama alanını optimize ederken, karmaşık sorguların çalışma performansını olumsuz etkileyebilir.
- Veri tabanı denetiminde sadece sunucu erişimi değil, aynı zamanda log kayıtlarına erişim ve yapılandırma ayarlarının değişimi de kontrol edilmelidir.
- Veri Akış Şemaları (DFD) süreçlerin zamanlaması veya sırası hakkında bilgi içermez.
- Veri tabanı yedekleme politikası 'İş Etki Analizi' sonuçlarına göre rasyonelleştirilmelidir.
- Şifrelenmiş yedeklerde anahtar (key) yönetimi, verinin kendisi kadar kritiktir.
- Normalleştirme veri tekrarını azaltır ancak sorgu maliyetini (performansı) etkileyebilir.
- Kişiden kişiye veri aktarımı (e-posta vb.) izlenmesi en zor akış türüdür.

Sık Yapılan Hatalar

- DFD'lerin süreç sırasını gösterdiğini düşünmek (Sadece akışı gösterirler).
- İçsel ve Bağlamsal veri kalitesi kriterlerini birbirine karıştırmak.
- Yedekleme yapmanın tek başına yeterli olduğunu sanmak (Geri dönüş testleri şarttır).
- NoSQL veri tabanlarının sadece yapılandırılmamış veri için olduğunu sanmak (Her ikisini de işleyebilirler).

6. Veri Yönetimi, Veri Tabanı Sistemleri ve Veri Modelleme • Sistem Arayüzleri, Bulut Bilişim ve Büyük Veri Teknolojileri

Temel Kavramlar

- Ara Katman Yazılımı (Middleware): Sistemler arası veri akışını ve entegrasyonu sağlayan, kurum içinde geliştirilebileceği gibi piyasadan hazır olarak da temin edilebilen altyapı yazılım çözümüdür.
- İnkâr Edilemezlik Kontrolleri: Verinin asıl alıcısının amaçlanan alıcı olmasını ve işlemin taraflarca reddedilememesini sağlayan, sistem arayüzlerinde veri güvenliğini artıran kritik bir güvenlik mekanizmasıdır.
- Son Kullanıcı Bilgi İşlemi (EUC): Teknik bilgisi olmayan kullanıcıların kendi uygulamalarını tasarlamasıdır; esneklik sağlasa da değişiklik yönetimi ve yedekleme eksikliği gibi ciddi operasyonel riskler barındırır.
- Beyaz Liste (White List): EUC modelinde güvenliği sağlamak amacıyla bilgisayar ve sunucularda yalnızca önceden tanımlanmış ve izin verilmiş uygulama ve servislerin çalıştırılmasına izin veren kısıtlama yöntemidir.
- Kontrollerde Kullanılan Bilgiler (IUC): İşletmenin kendi iç kontrollerini yürütürken kullandığı rapor veya verilerdir; denetçi bu verilerin çekildiği kaynak ve parametrelerin doğruluğunu mutlaka teyit etmelidir.
- İşletme Tarafından Üretilen Bilgiler (IPE): Risk değerlendirme veya doğrulama prosedürlerinde denetim kanıtı olarak kullanılan personel listesi gibi bilgilerdir; işletmenin kendi kontrol süreçlerinde doğrudan kullanılmazlar.
- Hizmet Olarak Yazılım (SaaS): Tüketicinin uygulamaları web üzerinden kullandığı, altyapı veya işletim sistemi üzerinde hiçbir kontrolünün olmadığı, sadece sınırlı uygulama yapılandırma yetkisine sahip olduğu bulut modelidir.
- Hizmet Olarak Altyapı (IaaS): Tüketicinin işletim sistemi, depolama ve uygulamalar üzerinde kontrol sahibi olduğu, ancak temel fiziksel bulut altyapısını yönetemediği en geniş kapsamlı kaynak sağlama modelidir.
- Melez (Hibrit) Bulut: Veri ve uygulama taşınabilirliği sağlayan standart teknolojilerle birbirine bağlanan, özel ve halka açık gibi iki veya daha fazla farklı bulut altyapısının birleşiminden oluşan modeldir.
- Büyük Veri (Big Data): Geleneksel veri yönetimi araçlarıyla işlenemeyecek kadar hacimli, hızlı üretilen ve yapılandırılmamış çeşitlilikteki verilerin özel teknolojilerle analiz edilmesini ifade eden kavramdır.
- Yapılandırılmamış Veri: E-posta, video veya sosyal medya içeriği gibi önceden tanımlanmış bir formatı veya veri kümesi olmayan, günümüzdeki toplam veri büyüklüğünün yaklaşık %95'ini oluşturan verilerdir.
- Hadoop: Büyük verinin birden fazla makine üzerinde paralel olarak saklanmasını ve analiz edilmesini sağlayarak kurumlara hız ve verimlilik artışı getiren açık kaynaklı bir yazılım çerçevesidir.
- Sistem Arayüzü: Sistemler arası veri aktarımını sağlayan fiziksel veya fonksiyonel bağlantı noktaları.
- EUC (Son Kullanıcı Bilgi İşlemi): Teknik uzman olmayan kullanıcıların kendi iş uygulamalarını geliştirmesi.
- IUC / IPE: Denetimde kullanılan; işletmenin kontrolde kullandığı (IUC) veya denetçinin kanıt olarak ürettiği (IPE) bilgiler.
- Bulut Bilişim: Paylaşılan kaynak havuzuna her yerden ve isteğe bağlı erişim sağlayan model.
- Büyük Veri (3V): Hacim (Volume), Hız (Velocity) ve Çeşitlilik (Variety) ile karakterize edilen devasa veri kümeleri.

Önemli Noktalar

- Sistem arayüzlerindeki hatalar, kurumsal itibar kaybının ötesinde idari ve yasal yaptırımlara yol açabilecek finansal raporlama riskleri taşır.
- Bir hizmetin 'Bulut Bilişim' sayılması için; isteğe bağlı self-servis, geniş ağ erişimi, kaynak havuzu, hızlı esneklik ve ölçülü hizmet özelliklerinin tamamını taşıması gerekir.

Önemli Noktalar

- EUC modelinde kullanıcıların yerel yönetici haklarının engellenmesi ve şahsi cihazlardan erişimin sıkı kontrol edilmesi asgari güvenlik gereksinimidir.
- Bulut bilişimde veri güvenliği 'dinlenmede' (at rest) ve 'dolaşımda' (in motion) olmak üzere iki aşamalıdır ve her ikisi için de en iyi koruma yöntemi şifrelemedir.
- Bulut hizmeti alımlarında 'denetim hakkı' (right to audit) sözleşmeye eklenmelidir; bu hak alınamıyorsa CSA'nın CAIQ gibi bağımsız denetim raporları talep edilmelidir.
- Büyük verinin analizinde 3V kriteri (Hacim/Volume, Hız/Velocity, Çeşitlilik/Variety) verinin niteliğini belirleyen temel unsurlardır.
- Spark teknolojisi, büyük veriyi ana bellek (RAM) üzerinde analiz ederek Hadoop gibi geleneksel disk tabanlı sistemlere göre çok daha yüksek hız artışı sağlar.
- Arayüz hataları finansal raporlamada kritik yanlışlıklara yol açabilir.
- EUC (Gölge IT) esneklik sağlasa da değişiklik yönetimi ve güvenlik riskleri taşır.
- Bulut güvenliği, hizmet veren ve alan arasında paylaşılan bir sorumluluktur.
- Bulut modelleri: SaaS (Yazılım), PaaS (Platform), IaaS (Altyapı).
- Yapılandırılmış veri toplam verinin sadece %5'ini oluşturur.

Sık Yapılan Hatalar

- Hata: Bulut bilişimin her türlü dış kaynak kullanımı ile aynı olduğu sanılır. Doğrusu: Bulut bilişim, dış kaynak kullanımının 5 temel karakteristik özelliğe sahip özel bir alt türüdür.
- Hata: IUC ve IPE kavramları birbirinin yerine kullanılır. Doğrusu: IUC işletmenin kontrolü yürütürken kullandığı veridir, IPE ise denetçinin kanıt toplarken kullandığı işletme üretimi bilgisidir.
- Hata: Buluta geçildiğinde veri güvenliği sorumluluğunun tamamen sağlayıcıya geçtiği düşünülür. Doğrusu: Güvenlik, seçilen hizmet (SaaS, PaaS, IaaS) ve dağıtım modeline göre paylaşımlı bir sorumluluktur.
- Hata: Yapılandırılmış verinin toplam verinin büyük kısmını oluşturduğu varsayılır. Doğrusu: Yapılandırılmış veri toplam verinin sadece %5'ini oluştururken, %95'i yapılandırılmamış veridir.
- Hata: Manuel mutabakatların her zaman otomatik kontrollerden üstün olduğu sanılır. Doğrusu: Otomatik kontroller denetim açısından öncelikli tercih edilir; manuel kontrollerde ise yapan kişinin yetkinliği kritiktir.
- Bulut bilişim ile dış kaynak kullanımını tamamen aynı sanmak (Bulutun karakteristik 5 özelliği vardır).
- IUC ve IPE terimlerini birbirine karıştırmak (Kontrolde kullanılan vs. işletme tarafından üretilen).
- Büyük veriyi sadece 'çok veri' olarak düşünmek (Hız ve çeşitlilik de zorunlu kriterlerdir).

Devamı ücretsiz kayıtle

Bilgi Sistemleri İşletimi modülünün **24 bölümünün 6 tanesi** bu PDF'te. Kalan 18 bölüm, konu anlatımı ve çıkmış soru tarzındaki soru bankası FinLisans'ta.

- ✓ Ücretsiz üyelikle soru çözmeye hemen başla — kredi kartı istemiyoruz.
- ✓ Tüm SPK/SPL dersleri için ders notu, özet ve formül kartları.
- ✓ Konu bazlı soru bankası, deneme sınavı ve yanlış analizi.
- ✓ Sesli ders anlatımı ile yolda/işte tekrar imkânı.
- ✓ İlerlemeni takip eden panel ve sınav geri sayımı.

Bu modülün güncel ve tam sayfası

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-isletimi>

Ücretsiz kayıt ol → <https://www.finlisans.com/auth/signup>

Son güncelleme: **17 Eylül 2026** · Kaynak: finlisans.com ders notları

Bu doküman sınavlara hazırlık amaçlı bir özettir; resmî kaynak yerine geçmez. SPL'nin yayımladığı güncel çalışma notlarını da takip ediniz.