EEE374 SİBER GÜVENLİK

Prof. Dr. Hasan Hüseyin BALIK

(5. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2.Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.4 Veritabanı ve Veri Merkezi Güvenliği

2.4. İçerik

- Veritabanı Güvenliği İhtiyacı
- Veritabanı Yönetim Sistemleri
- İlişkisel veritabanları
- SQL Enjeksiyon saldırıları
- Veritabanı Erişim Kontrolü
- Çıkarım
- Veritabanı şifreleme
- Veri Merkezi Güvenliği

Veritabanı Güvenliği İhtiyacı

- Kurumsal veritabanları, hassas bilgileri tek bir mantıksal veritabanı sisteminde toplama eğilimindedir.
  - Kurumsal finansal veriler
  - Gizli telefon kayıtları
  - İsim, Sosyal Güvenlik numarası gibi müşteri ve çalışan bilgileri, banka hesap bilgileri, kredi kartı bilgileri
  - Tescilli ürün bilgileri
  - Sağlık bilgileri ve tıbbi kayıtlar
- Bu tür bilgiler, iç ve dış yanlış kullanım veya yetkisiz değişiklik tehditleri tarafından hedef alınabilir.
- Veritabanlarına özel olarak uyarlanmış güvenlik, genel bir kurumsal güvenlik stratejisinin giderek daha önemli bir bileşenidir.

Veritabanı Güvenliği

Veritabanı güvenliğinin, veritabanlarına artan güvene ayak uyduramamasının nedenleri şunlardır:

Modern veritabanı yönetim sistemlerinin (DBMS) karmaşıklığı ile bu kritik sistemleri korumak için kullanılan güvenlik tekniği arasında çarpıcı bir dengesizlik vardır.

Kurumsal veri tabanının bir kısmını veya tamamını barındırmak için bulut teknolojisine artan güven

Veritabanlarının karmaşık bir etkileşim protokolü olan Karmaşık olan Yapılandırılmış Sorgu Dili (SQL) kullanılır.

Çoğu kurumsal ortam, veri tabanı platformları, kurumsal platformlar ve işletim sistemi platformlarının heterojen bir karışımından oluşur ve güvenlik personeli için ek bir karmaşıklık engeli oluşturur.

Tipik organizasyon, tam zamanlı veritabanı güvenlik personelinden yoksundur

Etkili veritabanı güvenliği, SQL'in güvenlik açıklarının tam olarak anlaşılmasına dayalı bir strateji gerektirir

Veritabanları

- Bir veya daha fazla uygulama tarafından kullanılmak üzere depolanan verilerin yapılandırılmış koleksiyonu
- Veri öğeleri ve veri öğeleri grupları arasındaki ilişkileri içerir

- Bazen güvence altına alınması gereken hassas veriler içerir

Sorgu dili

- Kullanıcılar ve uygulamalar için veritabanına tek tip bir arayüz sağlar

Veritabanı yönetim sistemi (DBMS)

- Veritabanını oluşturmak ve sürdürmek için program paketdir
- Birden çok kullanıcıya ve uygulamaya özel sorgu olanakları sunar

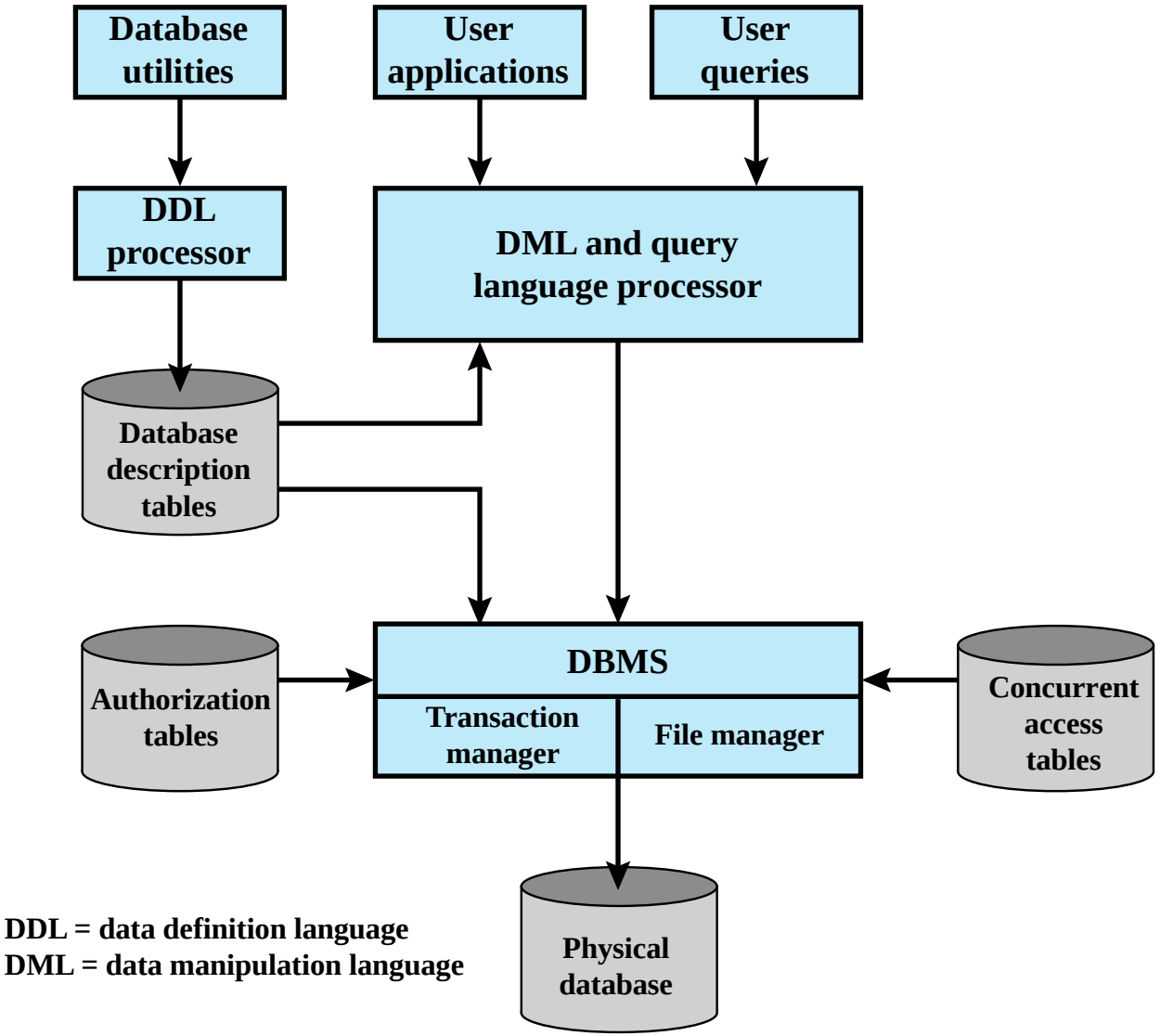


Figure 5.1 DBMS Architecture

İlişkisel Veritabanları

- İlişkisel bir veritabanının temel yapı taşı, satır ve sütunlardan oluşan bir veri tablosudur.
  - Her sütun belirli bir veri türünü tutar
  - Her satır, her sütun için belirli bir değer içerir
  - ideal olarak bir tabloda tüm değerlerin benzersiz olduğu ve o satır için bir tanımlayıcı/anahtar oluşturan bir sütunu vardır
- Bir tablo sadece iki boyutlu (satır ve sürünlar) şeklinde ise düz tablo olarak adlandırılır
  - belirli bir satır için bazı sütun konumları boş olabilir (kullanılmaz).
  - daha fazla sütun eklenmeli ve veritabanı ve beraberindeki yazılım yeniden tasarlanmalı ve yeniden oluşturulmalıdır
- Tüm tablolarda bulunan benzersiz bir tanımlayıcı ile birbirine bağlı birden çok tablonun oluşturulmasını sağlar
- Veritabanına erişmek için ilişkisel bir sorgu dili kullanılır
  - Kullanıcının belirli bir dizi kritere uyan verileri talep etmesine izin verir.

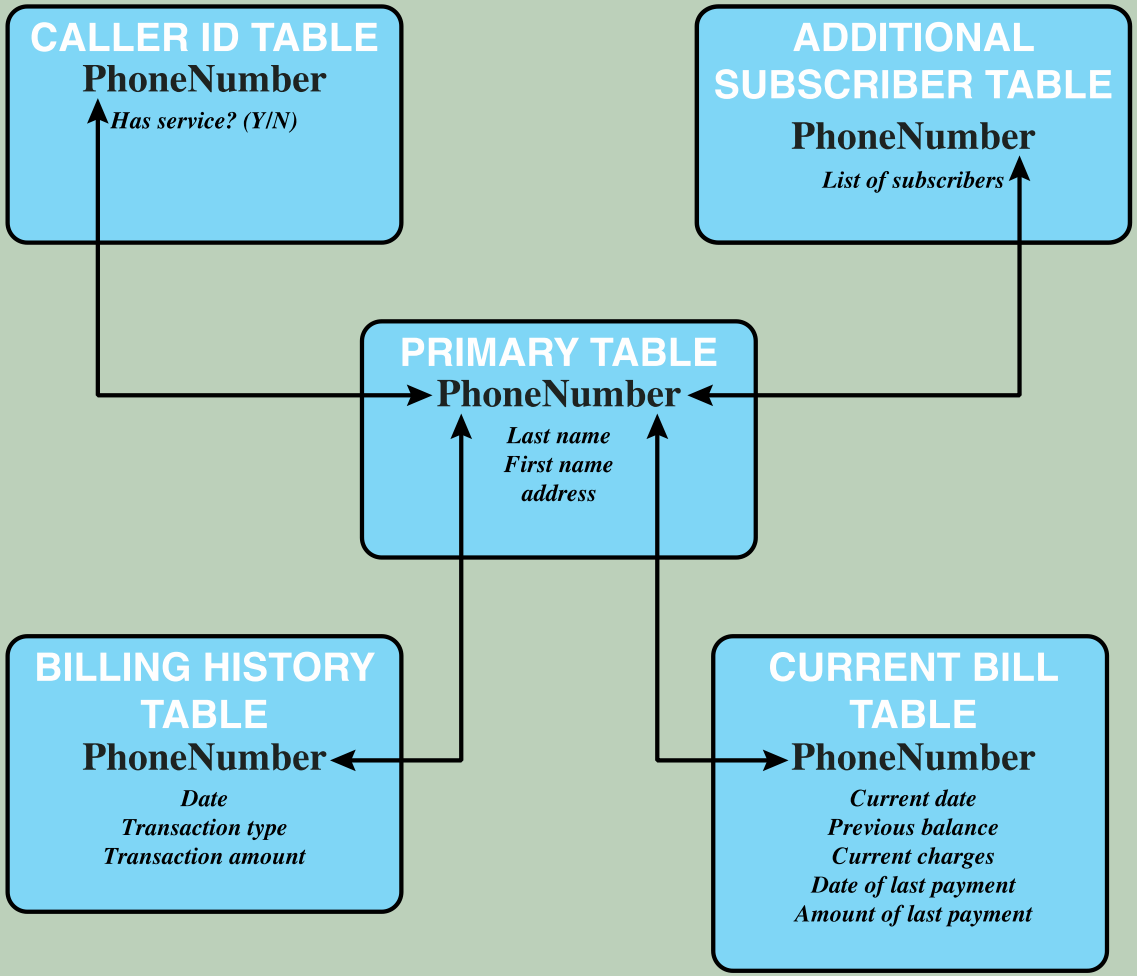


Figure 5.2 Example Relational Database Model. A relational database uses multiple tables related to one another by a designated key; in this case the key is the PhoneNumber field.

İlişkisel Veritabanı Öğeleri

- İlişki
  - tablo/dosya
- Demet (tüple)
  - Satır/kayıt
- Öznitelik (özellik)
  - sütun/alan

Birincil anahtar

- Bir satırı benzersiz olarak tanımlar
- Bir veya daha fazla sütun adından oluşur

Yabancı anahtar

- Bir tabloyu diğerindeki niteliklere bağlar

Görünüm (View)/Sanal Tablo

- Bir veya daha fazla tablodan seçilen satırları ve sütunları döndüren bir sorgunun sonucu
- Görünümler genellikle güvenlik amacıyla kullanılır

İlişkisel Veritabanları için Temel Terminoloji

Resmi Kullunım	Yaygın Kullanım	Diğer
İlişki	Tablo	Dosya
Demet (Tuple)	Satır	Kayıt
Öznitelik (özellik)	Sütün	Alan

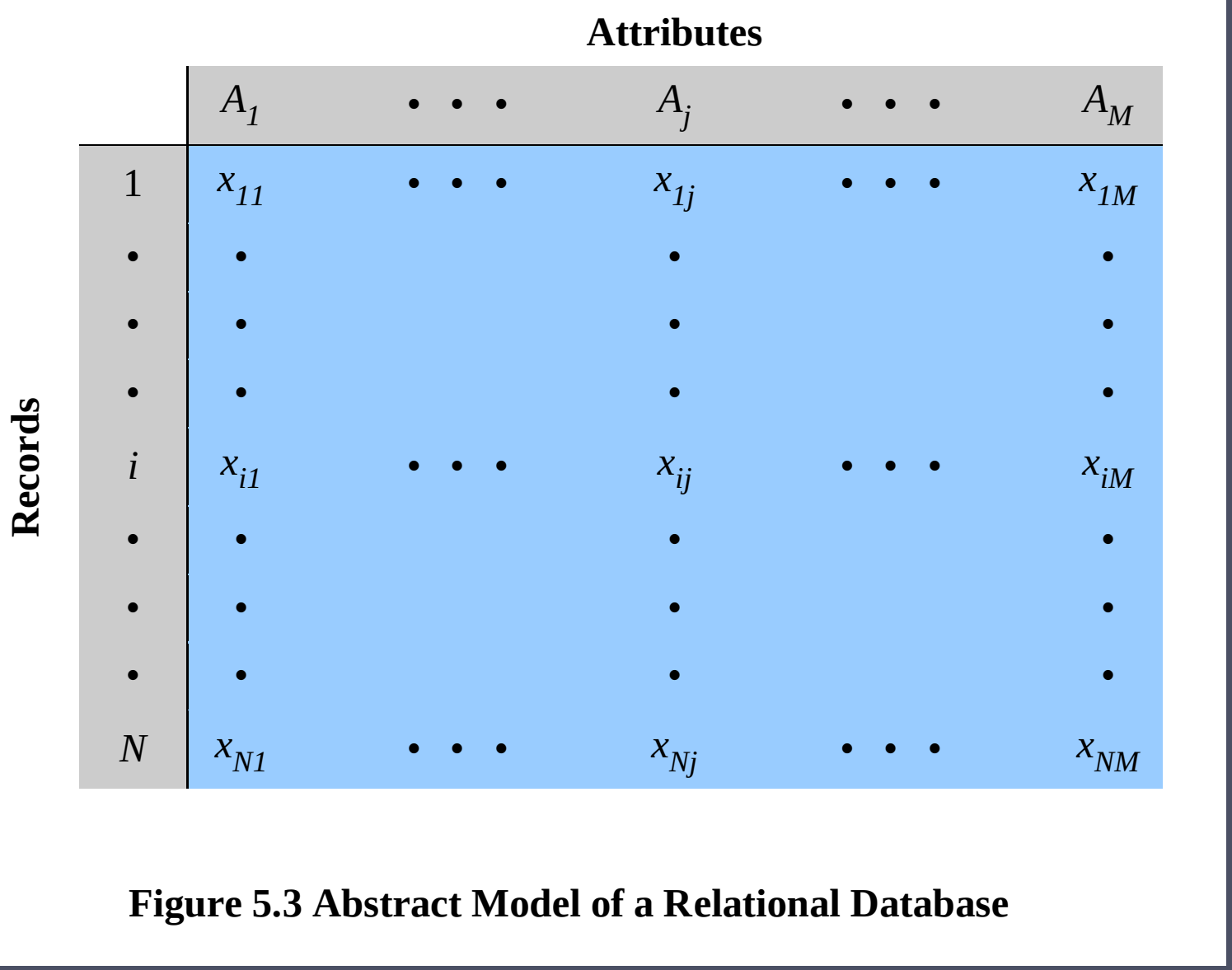


Figure 5.3 Abstract Model of a Relational Database

Her bir A_j niteliği $|A_j|$ olası değerler, x_{ij}, i varlığı için j özniteliğinin değerini belirtir.

Department Table

Did	Dname	Dacctno
4	human resources	528221
8	education	202035
9	accounts	709257
13	public relations	755827
15	services	223945

primary key

Employee Table

Ename	Did	Salarycode	Eid	Ephone
Robin	15	23	2345	6127092485
Neil	13	12	5088	6127092246
Jasmine	4	26	7712	6127099348
Cody	15	22	9664	6127093148
Holly	8	23	3054	6127092729
Robin	8	24	2976	6127091945
Smith	9	21	4490	6127099380

foreign key

primary key

(a) Two tables in a relational database

Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(b) A view derived from the database

Figure 5.4 Relational Database Example

Yapılandırılmış sorgu dili (SQL)

- İlişkisel bir veritabanında şema tanımlamak, verileri işlemek ve sorgulamak için standartlaştırılmış dildir
- ANSI/ISO standardının birkaç benzer versiyonu vardır
- Hepsi aynı temel sözdizimini ve semantiği takip eder

SQL ifadeleri şu amaçlarla kullanılabilir:

- Tablolar oluşturmak
- Tablolara veri eklemek ve silmek
- Görünümler oluşturmak
- Sorgu ifadeleriyle verileri çekmek

SQL Enjeksiyon Saldırıları (SQLi)

- En yaygın ve tehlikeli ağ tabanlı güvenlik tehditlerinden biridir
- Web uygulaması sayfalarının doğasından yararlanmak için tasarlanmıştır
- Veritabanı sunucusuna kötü amaçlı SQL komutları gönderir
- En yaygın saldırı hedefi, verilerin toplu olarak çekilmesidir
- Ortama bağlı olarak SQL enjeksiyonu aşağıdaki amaçlarla da kullanılabilir:
  - Verileri değiştirmek veya silmek
  - İsteğe bağlı işletim sistemi komutlarını yürütmek
  - Hizmet reddi saldırısı başlatmak (DoS)

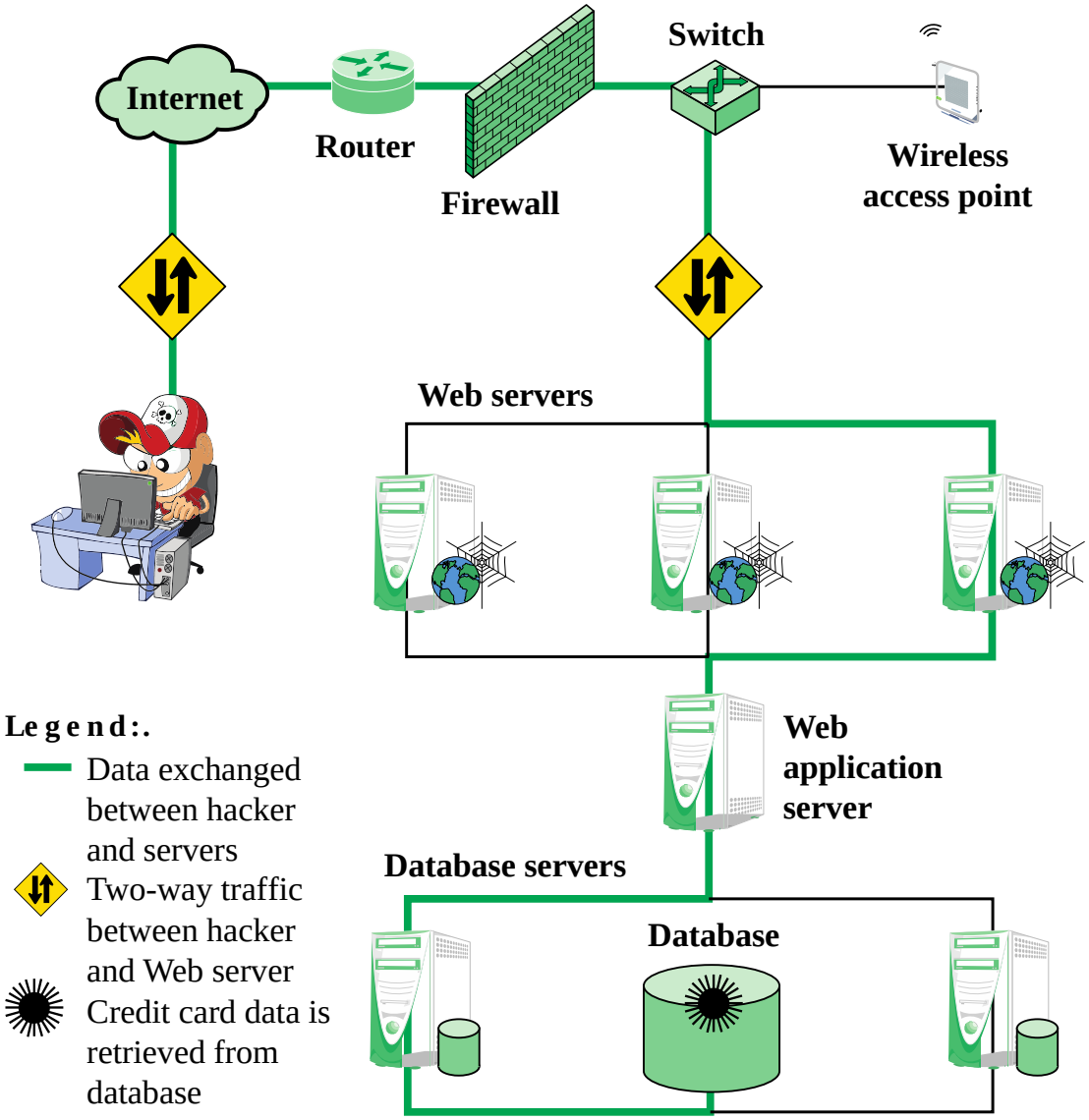
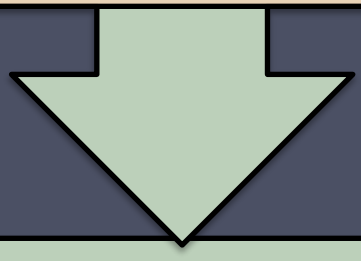


Figure 5.5 Typical SQL Injection Attack

Enjeksiyon Tekniği

SQLi saldırısı genellikle bir metin dizesini zamanından önce sonlandırarak ve yeni bir komut ekleyerek çalışır

Eklenen komut çalıştırılmadan önce ek dizelere sahip olabileceğinden, saldırgan enjekte edilen dizeyi "- -" yorum işaretiyle sonlandırır



Sonraki metin yürütme zamanında yoksayılır

SQLi Saldırı Alanları

Kullanıcı girişi

- Saldırganlar, uygun hazırlanmış kullanıcı girişi sağlayarak SQL komutları enjekte eder

Sunucu değişkenleri

- Saldırganlar, HTTP ve ağ üstbilgilerine yerleştirilen değerleri taklit edebilir ve verileri doğrudan üstbilgilere yerleştirerek bu güvenlik açığından yararlanabilir.

İkinci dereceden enjeksiyon

- İkinci dereceden enjeksiyon, SQL enjeksiyon saldırılarına karşı eksik önleme mekanizmaları mevcut olduğunda gerçekleşir.
- Kötü niyetli bir kullanıcı, bir SQL enjeksiyon saldırısını tetiklemek için sistemde veya veritabanında zaten mevcut olan verilere güvenebilir, bu nedenle saldırı gerçekleştiğinde, sorguyu bir saldırıya neden olacak şekilde değiştiren girdi kullanıcıdan değil, sistemin kendisinden gelir.

Kukiler

- Saldırgan, uygulama sunucusu tanımlama bilgisinin içeriğine dayalı olarak bir SQL sorgusu oluşturduğunda, sorgunun yapısı ve işlevi değiştirilecek şekilde tanımlama bilgilerini değiştirebilir.

Fiziksel kullanıcı girişi

- Web istekleri alanının dışında bir saldırı oluşturan kullanıcı girdisi uygulamak

Bant içi (inband) Saldırılar

- SQL kodunu enjekte etmek ve sonuçları almak için aynı iletişim kanalını kullanır
- Alınan veriler doğrudan uygulama Web sayfasında sunulur
- Bunlar;

Totoloji

Bu saldırı biçimi, her zaman doğru olarak değerlendirilmeleri için bir veya daha fazla koşullu ifadeye kod enjekte eder

Satır sonu yorumu

Belirli bir alana kod enjekte edildikten sonra, satır sonu yorumları kullanılarak takip eden meşru kod geçersiz kılınır

Bindirilmiş Sorgular

Saldırgan, amaçlanan sorgunun ötesinde ek sorgular ekleyerek saldırıyı meşru bir isteğin üzerine bindirir

Çıkarımsal saldırılar

- Gerçek bir veri aktarımı yoktur, ancak saldırgan, belirli istekler göndererek ve Web Sitesi/veritabanı sunucusunun ortaya çıkan davranışını gözlemleyerek bilgileri yeniden yapılandırabilir.
- Bunlar:
  - Kuraldışı/mantıksal olarak yanlış sorgular
    - Bu saldırı, bir saldırganın bir Web uygulamasının arka uç veritabanının türü ve yapısı hakkında önemli bilgiler toplamasını sağlar.
    - Saldırı, diğer saldırılar için bir ön bilgi toplama adımı olarak kabul edilir.
  - Kör SQL enjeksiyonu
    - Sistem, saldırgana herhangi bir hatalı bilgi göstermeyecek kadar güvenli olsa bile, saldırganların bir veritabanı sisteminde bulunan verileri çıkarmasına izin verir.

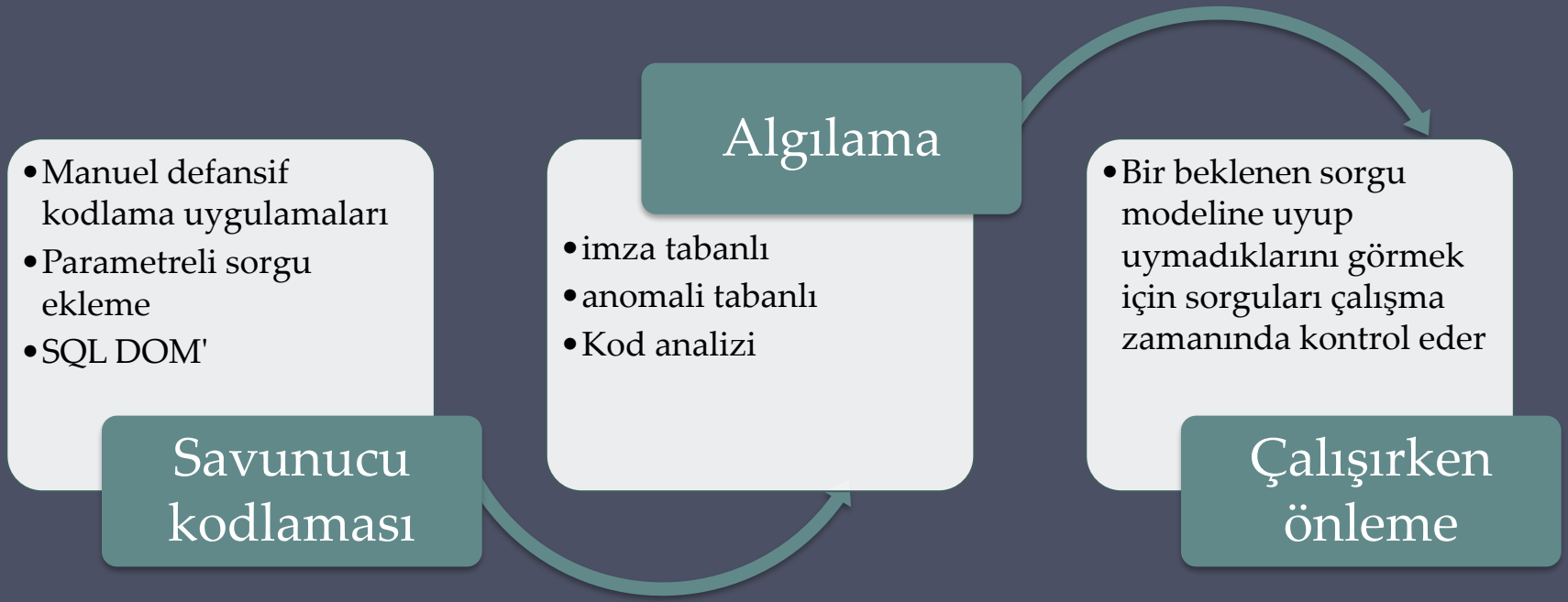
Bant Dışı (out-of-Band) Saldırılar

- Veriler farklı bir kanal kullanılarak alınır (örneğin, bir sorgunun sonuçlarını içeren e-posta oluşturulur ve test cihazına gönderilir)

- Bu, bilgi alımında sınırlamalar olduğunda kullanılabilir, ancak veritabanı sunucusundan giden bağlantı gevşek olduğunda

SQLi karşı önlemler

- Üç tip:



Veritabanı Erişim Kontrolü

Veritabanı erişim kontrol sistemi şunları belirler:

Kullanıcının veritabanının tamamına veya yalnızca bir kısmına erişimini

Kullanıcının sahip olduğu erişim haklarını (oluşturma, ekleme, silme, güncelleme, okuma, yazma)

Bir dizi yönetim politikasını destekler

Merkezi yönetim

- Az sayıda ayrıcalıklı kullanıcı erişim haklarını verebilir ve iptal edebilir

Mülkiyet tabanlı yönetim

- Bir tablonun yaratıcısı, tabloya erişim haklarını verebilir veya iptal edebilir

Merkezi olmayan yönetim

- Tablonun sahibi, diğer kullanıcılara yetkilendirme haklarını verebilir ve iptal edebilir, bu da onların tabloya erişim haklarını vermelerine ve iptal etmelerine izin verir.

SQL Erişim Kontrolleri

- Erişim haklarını yönetmek için iki komut kullanılır:
  - Grant (bağışlamak)
    - Bir veya daha fazla erişim hakkı vermek için kullanılır veya bir kullanıcıya bir role atamak için kullanılabilir
  - Revoke (Geri çekmek)
    - Erişim haklarını iptal eder
- Tipik erişim hakları şunlardır:
  - Seçme
  - Ekleme
  - Güncelleme
  - Silme
  - Referanslar

Rol Tabanlı Erişim Kontrolü (RBAC)

- Rol tabanlı erişim denetimi, yönetim yükünü hafifletir ve güvenliği artırır
- Bir veritabanı RBAC'ının aşağıdaki yetenekleri sağlaması gerekir:
  - Rolleri oluştur ve sil
  - Bir rol için izinleri tanımlayın
  - Kullanıcıları rollere atama ve atamayı iptal etme
- Veritabanı kullanıcılarının kategorileri:

Uygulama Sahibi	Son kullanıcı	Yönetici
• Bir uygulamanın parçası olarak veritabanı nesnelerine sahip olan bir son kullanıcı	• Belirli bir uygulama aracılığıyla veritabanı nesneleri üzerinde çalışan ancak veritabanı nesnelerinin hiçbirine sahip olmayan bir son kullanıcı	• Veritabanının bir kısmı veya tamamı için idari sorumluluğu olan kullanıcı

Microsoft SQL Sunucuda bulunan Sabit Roller

rol	izinler
Sabit Sunucu Rolleri	
sysadmin	SQL Server'da herhangi bir aktivite gerçekleştirebilir ve tüm veritabanı fonksiyonları üzerinde tam kontrole sahip olabilir
serveradmin	Sunucu genelinde yapılandırma seçeneklerini ayarlayabilir, sunucuyu kapatabilir
setupadmin	Bağlantılı sunucuları ve başlatma prosedürlerini yönetebilir
securityadmin	Oturum açmaları ve CREATE DATABASE izinlerini yönetebilir, ayrıca hata günlüklerini okuyabilir ve şifreleri değiştirebilir
processadmin	SQL Server'da çalışan süreçleri yönetebilir
dbcreator	Veritabanları oluşturabilir, değiştirebilir ve bırakabilir
diskadmin	Disk dosyalarını yönetebilir
bulkadmin	BULK INSERT deyimlerini çalıştırabilir
Sabit Veritabanı Rolleri	
db_owner	Veritabanındaki tüm izinlere sahip
db_accessadmin	Kullanıcı kimlikleri ekleyebilir veya kaldırabilir
db_datareader	Veritabanındaki herhangi bir kullanıcı tablosundan tüm verileri seçebilir
db_datawriter	Veritabanındaki herhangi bir kullanıcı tablosundaki herhangi bir veriyi değiştirebilir
db_ddladmin	Tüm Veri Tanımlama Dili (DDL) ifadelerini yayınlayabilir
db_securityadmin	Tüm izinleri, nesne sahipliklerini, rolleri ve rol üyeliklerini yönetebilir
db_backupoperator	DBCC, CHECKPOINT ve BACKUP deyimleri yayınlayabilir
db_denydatareader	Veritabanındaki verileri seçme iznini reddedebilir
db_denydatawriter	Veritabanındaki verileri değiştirme iznini reddedebilir

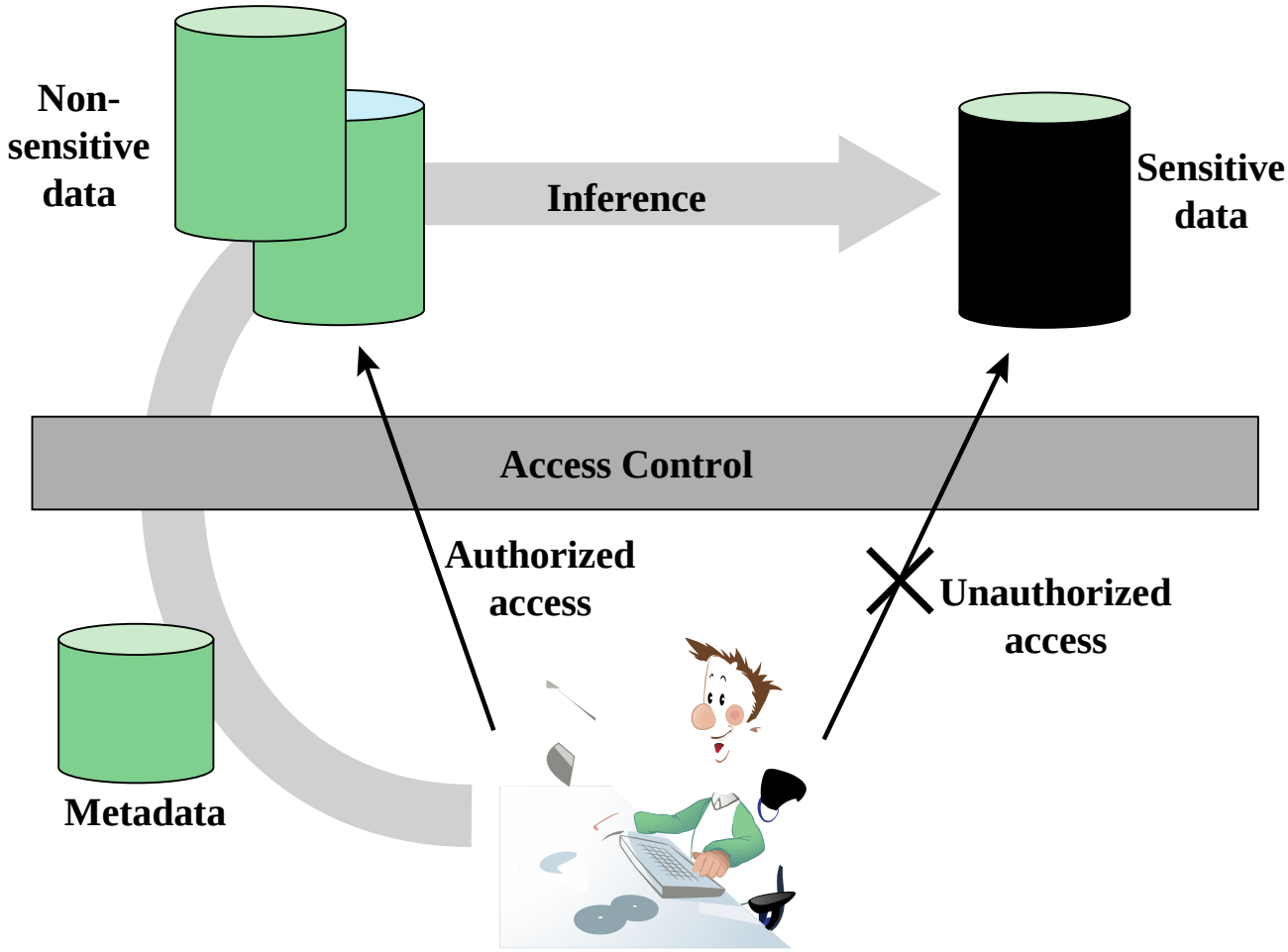


Figure 5.7 Indirect Information Access Via Inference Channel

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost ($)
in-store/online	7.99
online only	5.49
in-store/online	104.99

Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

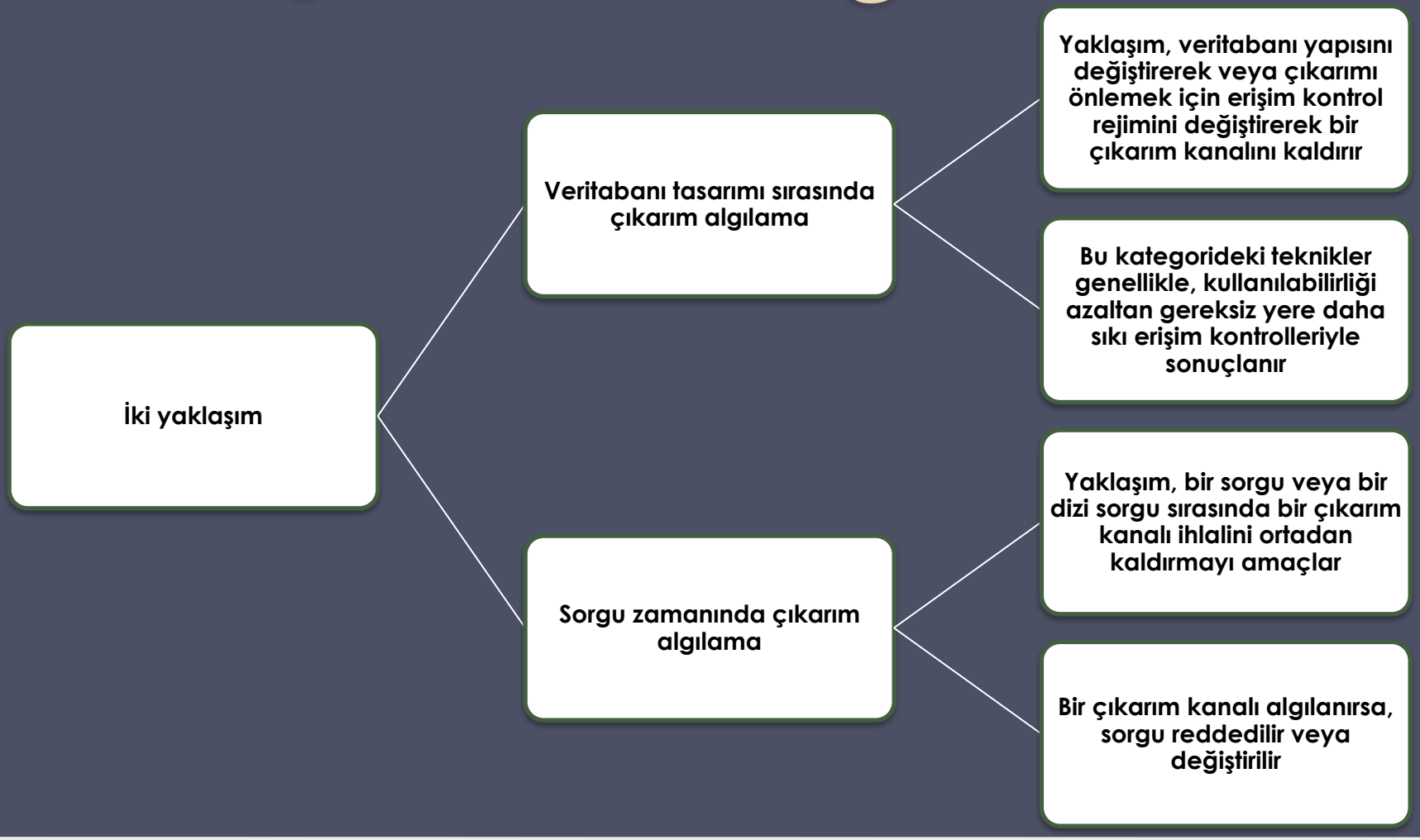
(b) Two views

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Figure 5.8 Inference Example

Çıkarım Algılama



- Bu yaklaşımlardan herhangi biri için bazı çıkarım algılama algoritması gereklidir
- Çok seviyeli güvenli veri tabanları ve istatistiksel veri tabanları için özel çıkarım algılama tekniklerinin geliştirilmesinde ilerleme kaydedilmiştir.

Veritabanı Şifreleme

- Veritabanı, herhangi bir kuruluş için tipik olarak en değerli bilgi kaynağıdır.
  - Çoklu güvenlik katmanları tarafından korunuyor
    - Güvenlik duvarları, kimlik doğrulama,genelerişim kontrol sistemleri, DB erişim kontrol sistemleri, veritabanı şifreleme
    - Şifreleme, veritabanı güvenliğinde son savunma hattı haline gelir
  - Tüm veritabanına, kayıt düzeyinde, öznitelik düzeyinde veya bireysel alan düzeyinde uygulanabilir
- Şifrelemenin dezavantajları:
  - Anahtar yönetimi
    - Yetkili kullanıcılar, erişim sahibi oldukları veriler için şifre çözme anahtarına erişebilmelidir.
  - Esneklik
    - Veritabanının bir kısmı veya tamamı şifrelendiğinde, kayıt araması yapmak daha zor hale gelir.

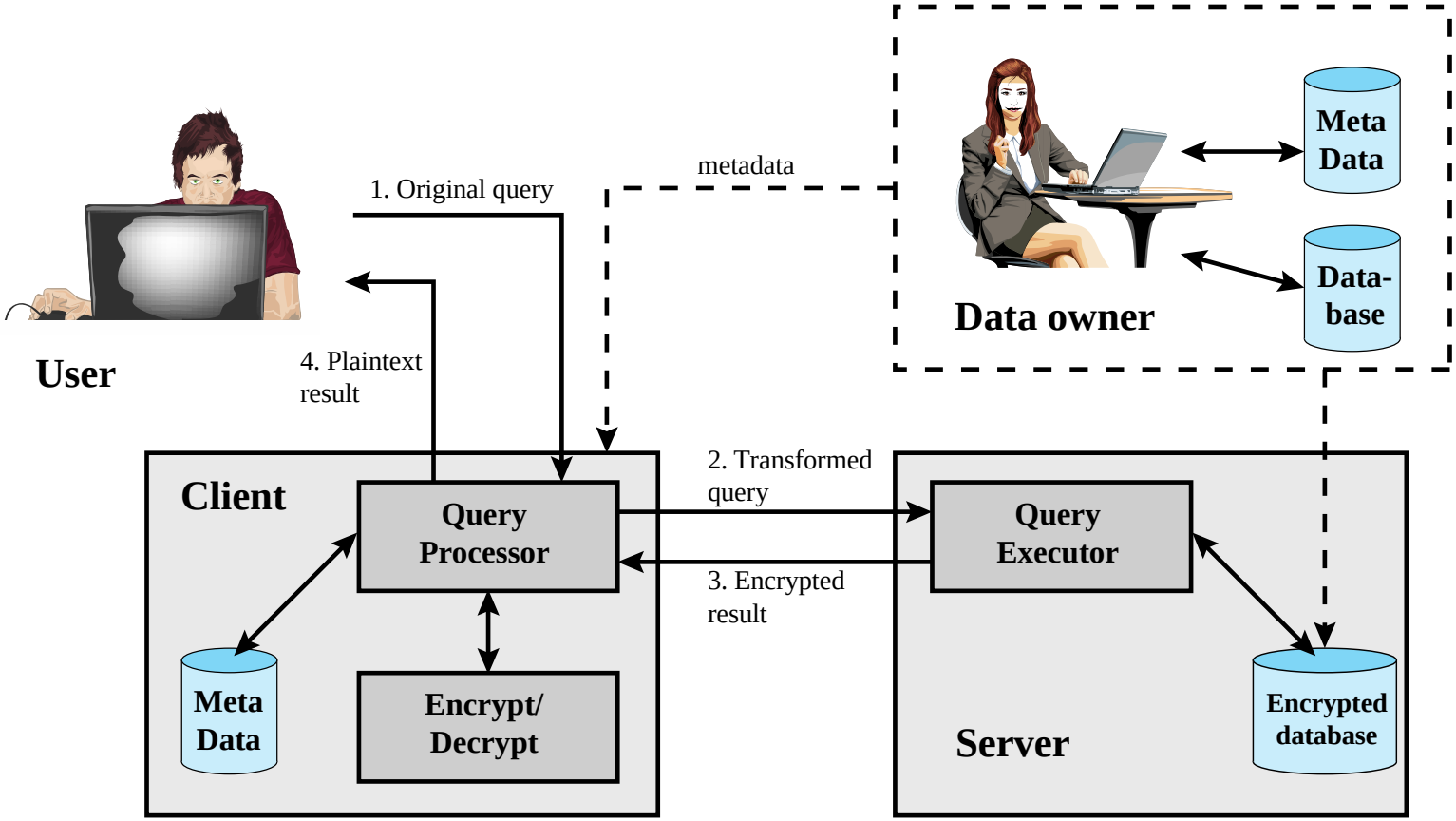
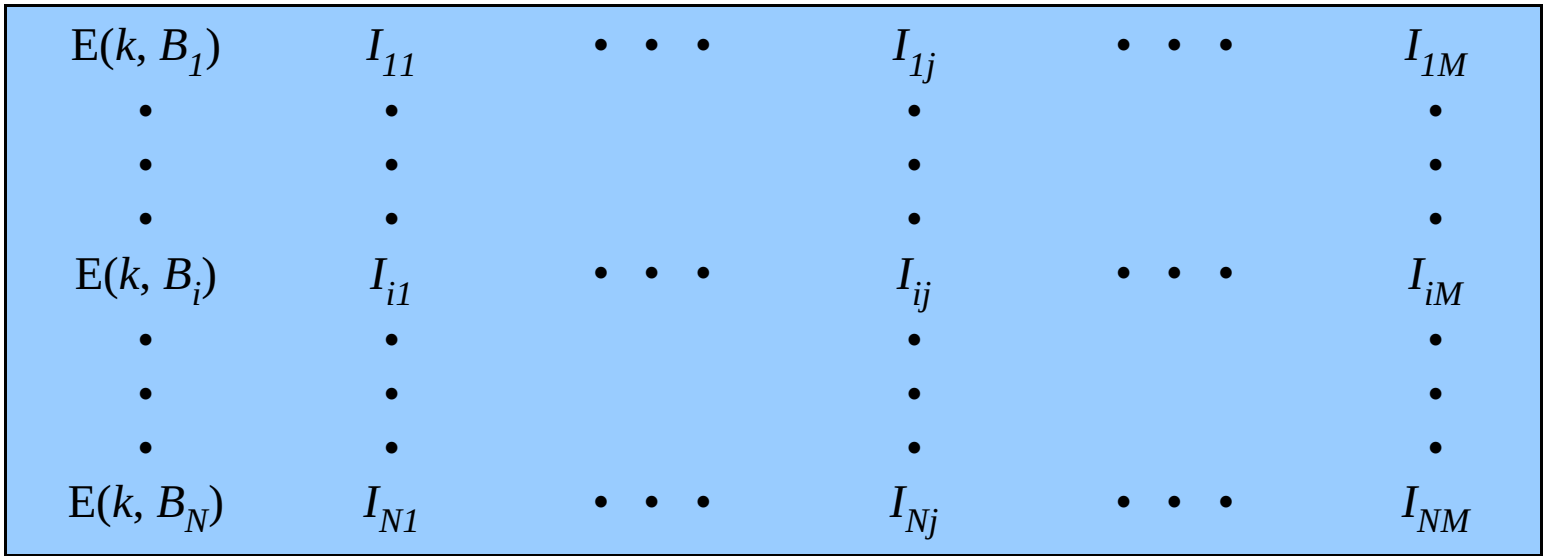


Figure 5.9 A Database Encryption Scheme



$B_i = (x_{i1} \| x_{i2} \| \ldots \| x_{iM})$

Figure 5.10 Encryption Scheme for Database of Figure 5.3

Table 5.3 Encrypted Database Example

(a) Employee Table

eid	ename	salary	addr	did
23	Tom	70K	Maple	45
860	Mary	60K	Main	83
320	John	50K	River	50
875	Jerry	55K	Hopewell	92

(b) Encrypted Employee Table with Indexes

E(*k*, *B*)	I(eid)	I(ename)	I(salary)	I(addr)	I(did)
1100110011001011…	1	10	3	7	4
0111000111001010…	5	7	2	7	8
1100010010001101…	2	5	1	9	5
0011010011111101…	5	5	2	4	9

Veri Merkezi Güvenliği

- Veri merkezi:
  - Çok sayıda sunucu, depolama aygıtı ve ağ anahtarı ve ekipmanı barındıran kurumsal tesistir.
  - Sunucuların ve depolama cihazlarının sayısı tek bir tesiste onbinleri bulabilir
  - Genellikle yedekli veya yedek güç kaynakları, yedekli ağ bağlantıları, çevresel kontroller ve çeşitli güvenlik cihazlarını içerir.
  - Bir binanın bir odasını, bir veya daha fazla katı veya bütün bir binayı işgal edebilir
- Kullanım örnekleri şunları içerir:
  - Bulut hizmeti sağlayıcıları
  - Arama motorları
  - Büyük bilimsel araştırma tesisleri
  - Büyük işletmeler için BT tesisleri

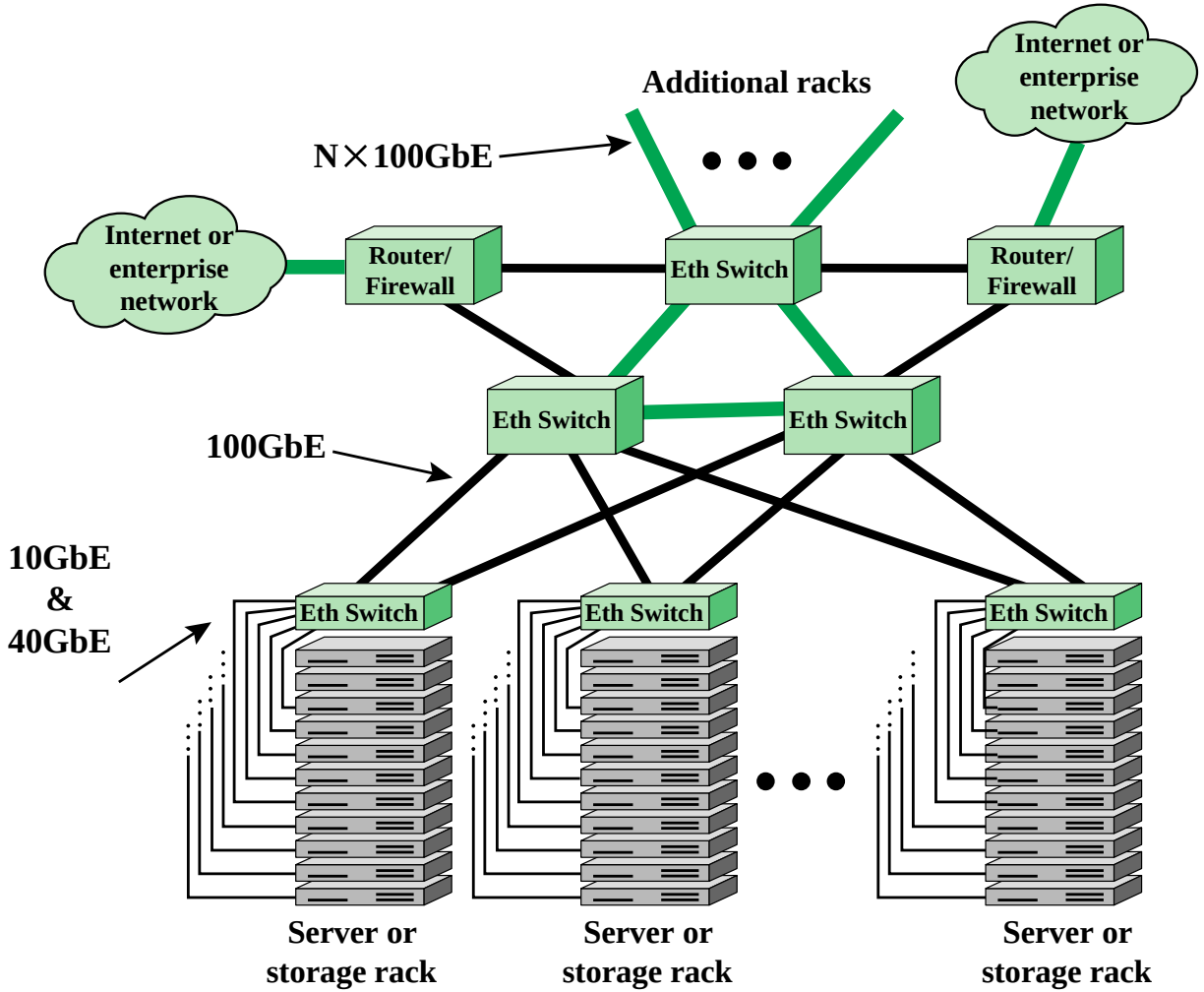


Figure 5.11 Key Data Center Elements

Kablolama ve Çapraz Bağlantılar

- Çapraz bağlantı:
  - Kabloların sonlandırılmasını ve diğer kablolama veya ekipmanla ara bağlantılarını sağlayan bir tesis
- Yatay kablolama:
  - Sunucuları ve diğer dijital ekipmanları ağa bağlamak için yerel alan ağı (LAN) sağlamak amacıyla bir katın kablo dolabını çalışma alanlarındaki duvar plakalarına bağlamak için kullanılan herhangi bir kablolama
  - Yatay terimi, bu tür kabloların tipik olarak tavan veya zemin boyunca döşenmesi nedeniyle kullanılır
- Omurga kablolama:
  - Veri merkezi odaları veya muhafazaları ile bir binanın ana çapraz bağlantı noktası arasında çalıştırır

Güvenlik tehditleri

- Veri merkezi, büyük miktarda veri barındırır. Bu veriler;
  - sınırlı bir fiziksel alanda bulunur
  - birbirine bağlı ile birlikte doğrudan içerir
  - harici ağ bağlantıları aracılığıyla erişilebilir
  - işletmenin en büyük tek varlığıdır
- Önemli tehditlerden bazıları:
  - hizmet redi
  - Hedefli saldırılardan gelişmiş ıslartı tehditler
  - Gizlilik ihlalleri
  - SQL enjeksiyonu gibi uygulama açıkları
  - Kötü amaçlı yazılım
  - Fiziksel güvenlik tehditleri

Data Security	**Encryption, Password policiy, secure IDs, Data Protection (ISO 27002), Data masking, Data retention, etc.**
Network Security	**Firewalls, Anti-virus, Intrusion detection/ prevention, authentication, etc.**
Physical Security	**Surveillance, Mantraps, Two/ three factor authentication, Security zones, ISO 27001/ 27002, etc.**
Site Security	**Setbacks, Redundant utilities Landscaping, Buffer zones, Crash barriers, Entry points, etc.**

Figure 5.12 Data Center Security Model

TIA-492

- Telekomünikasyon Endüstrisi Derneği (TIA)
- TIA-492 (*Veri Merkezleri için Telekomünikasyon Altyapı Standardı*) veri merkezlerinin telekomünikasyon altyapısı için minimum gereksinimleri belirtir
- Aşağıdaki gibi konuları içerir:
  - Ağ mimarisi
  - Elektriksel tasarım
  - Dosya depolama, yedekleme ve arşivleme
  - Sistem yedekliliği
  - Ağ erişim kontrolü ve güvenliği
  - Veritabanı Yönetimi
  - ağ sağlayıcısı
  - Uygulama barındırma
  - İçerik dağıtımı
  - Çevresel kontrol
  - Fiziksel tehlikelere karşı koruma
  - Güç yönetimi

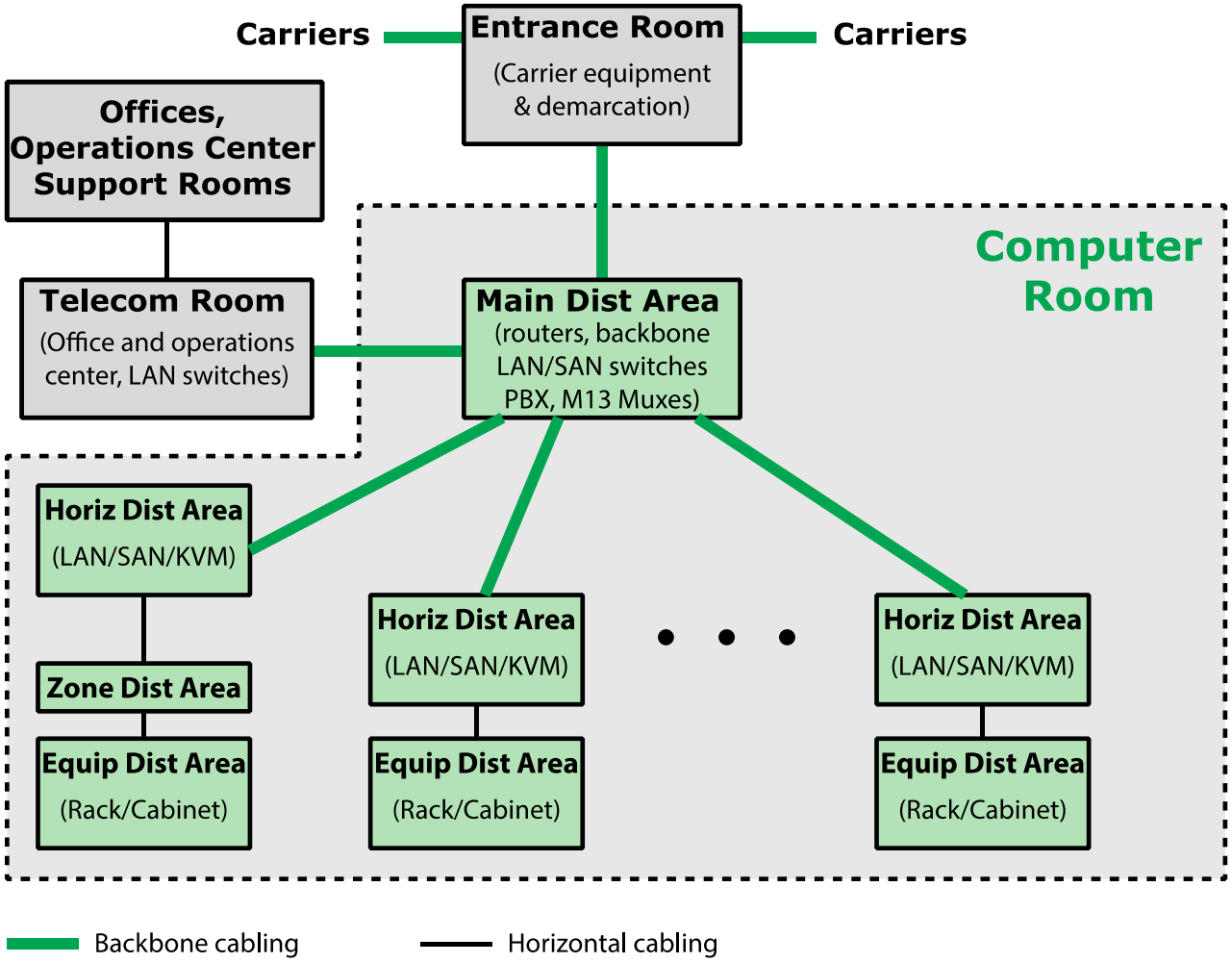


Figure 5.13 TIA-942 Compliant Data Center Showing Key Functional Areas

Aşama (Tier)	Sistem tasarımı	Kullanılabilirlik /Yıllık Kesinti Süresi
1	• Hem planlanmış hem de planlanmamış faaliyetlerden kaynaklanan kesintilere karşı hassas •Güç ve soğutma dağıtımı için tek yol, yedek bileşen yok •Yükseltilmiş zemin, UPS veya jeneratör olabilir veya olmayabilir •Uygulaması 3 ay sürer •Önleyici bakım yapmak için tamamen kapatılmalıdır	%99.671/ 28.8 saat
2	• Hem planlanmış hem de planlanmamış faaliyetlerden kaynaklanan kesintilere daha az duyarlı •Güç ve soğutma dağıtımı için tek yol, yedekli bileşenler içerir •Yükseltilmiş zemin, UPS ve jeneratör içerir •Uygulaması 3 ila 6 ay sürer •Güç yolunun ve altyapının diğer bölümlerinin bakımı, bir işlemin kapatılmasını gerektirir	%99.741/ 22.0 saat
3	•Bilgisayar donanımının çalışmasını kesintiye uğratmadan planlı aktiviteyi etkinleştirir ancak planlanmamış olaylar yine de aksamalara neden olur •Birden fazla güç ve soğutma dağıtım yolu, ancak yalnızca bir yol etkin, yedekli bileşenler içerir •Uygulaması 15 ila 20 ay sürer •Yükseltilmiş zemin ve bir yolda yük taşımak için diğer yolda bakım yapmak için yeterli kapasite ve dağıtım içerir	%99.982/ 1,6 saat
4	•Planlı etkinlik kritik yükü kesintiye uğratmaz ve veri merkezi, kritik yük etkisi olmadan en az bir en kötü planlanmamış olayı sürdürebilir • Çoklu aktif güç ve soğutma dağıtım yolları, yedekli bileşenler içerir •Uygulaması 15 ila 20 ay sürer	%99,995/ 0,4 saat

TIA-942'de Tanımlanan Veri Merkezi Katmanları