NETWORK AND SYSTEM SECURITY (CORE ELECTIVE - 5) CS424

Unit 3 : SYSTEM SECURITY

Unit 3 Overview

- User Authentication
- Access Control
- **Database and Cloud security**
- Malicious Software
- Denial of Service Attack
- Intrusion Detection
- Intrusion Prevention

Database and Cloud security

The need for Database Security

- Corporate financial data
- Confidential phone records
- Customer and employee information, such as name, Social Security number, bank account information, and credit card information
- Proprietary product information
- Health care information and medical records

Reasons why database security has not kept pace

- There is a dramatic imbalance between the complexity of modern database management systems (DBMS) and the security techniques used to protect these critical systems
- Databases have a sophisticated interaction protocol called the Structured Query Language (SQL), which is far more complex, for example, than the Hypertext Transfer Protocol (HTTP) used to interact with a Web service.

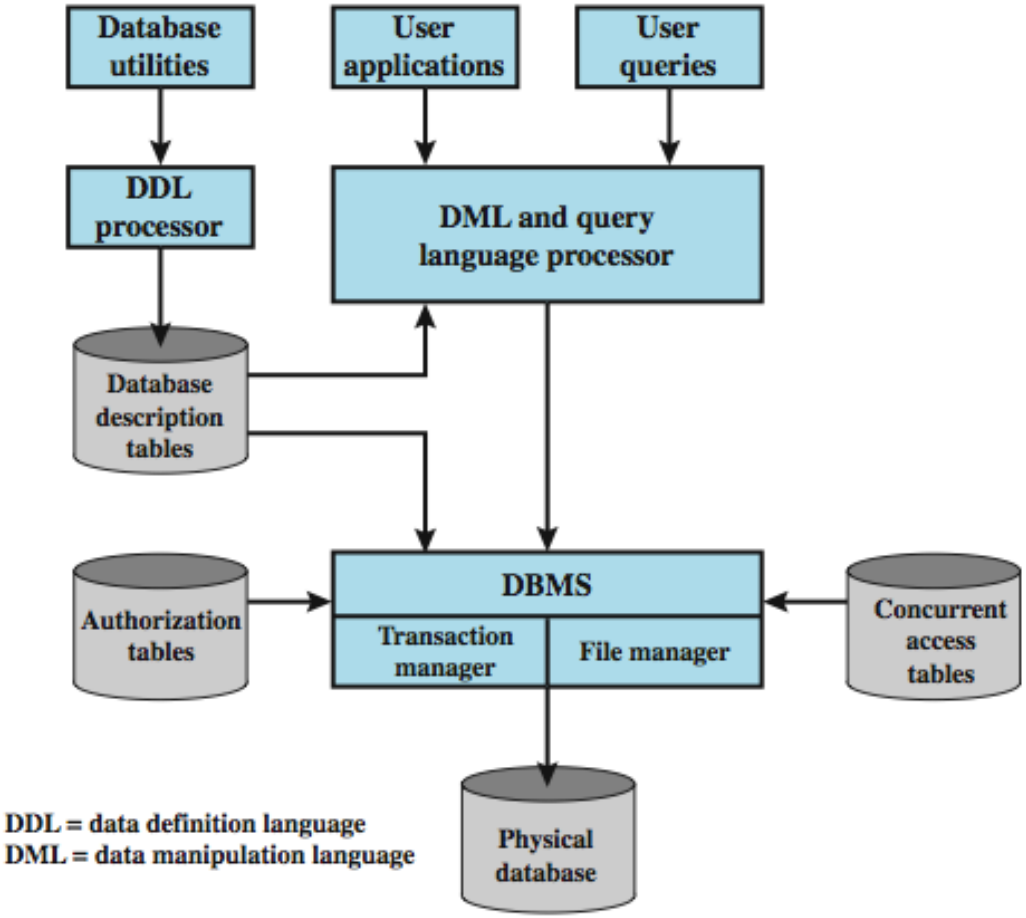
Reasons why database security has not kept pace ..

- The typical organization lacks full-time data base security personnel.
- Most enterprise environments consist of a heterogeneous mixture of database platforms (Oracle, IBM DB1 and Informix, Microsoft, Sybase, etc.), enterprise platforms (Oracle E-Business Suite, PeopleSoft, SAP, Siebel, etc.), and OS platforms (UNIX, Linux, z/OS, and Windows, etc.). This creates an additional complexity hurdle for security personnel.

Database systems

- Structured collection of data stored for use by one or more applications
- Contains the relationships between data items and groups of data items
- Can sometimes contain sensitive data that needs to be secured
- Query language: Provides a uniform interface to the database

Database Security



Database Access Control

- DBMS provide access control for database
- assume have authenticated user
- DBMS provides specific access rights to portions of the database
  - e.g. create, insert, delete, update, read, write
  - to entire database, tables, selected rows or columns
  - possibly dependent on contents of a table entry
- can support a range of policies:
  - **centralized administration** – A small number of privileged users may grant and revoke access rights.
  - **ownership-based administration** - The owner (creator) of a table may grant and revoke access rights to the table.
  - **decentralized administration** – In addition to granting and revoking access rights to a table, the owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table.

SQL-Based Access Definition

```
GRANT          { privileges | role }
[ON            table]
TO             { user | role | PUBLIC }
[IDENTIFIED BY password]
[WITH          GRANT OPTION]
```

- The GRANT OPTION indicates that the grantee can grant this access right to other users, with or without the grant option.
- GRANT SELECT ON ANY TABLE TO ricflair
- This statement enables user ricflair to query any table in the database.

SQL-Based Access Definition…

- Select: Grantee may read entire database; individual tables; or specific columns in a table.
- Insert: Grantee may insert rows in a table; or insert rows with values for specific columns in a table.
- Update: Semantics is similar to INSERT.
- Delete: Grantee may delete rows from a table.
- References: Grantee is allowed to define foreign keys in another table that refer to the specified columns.

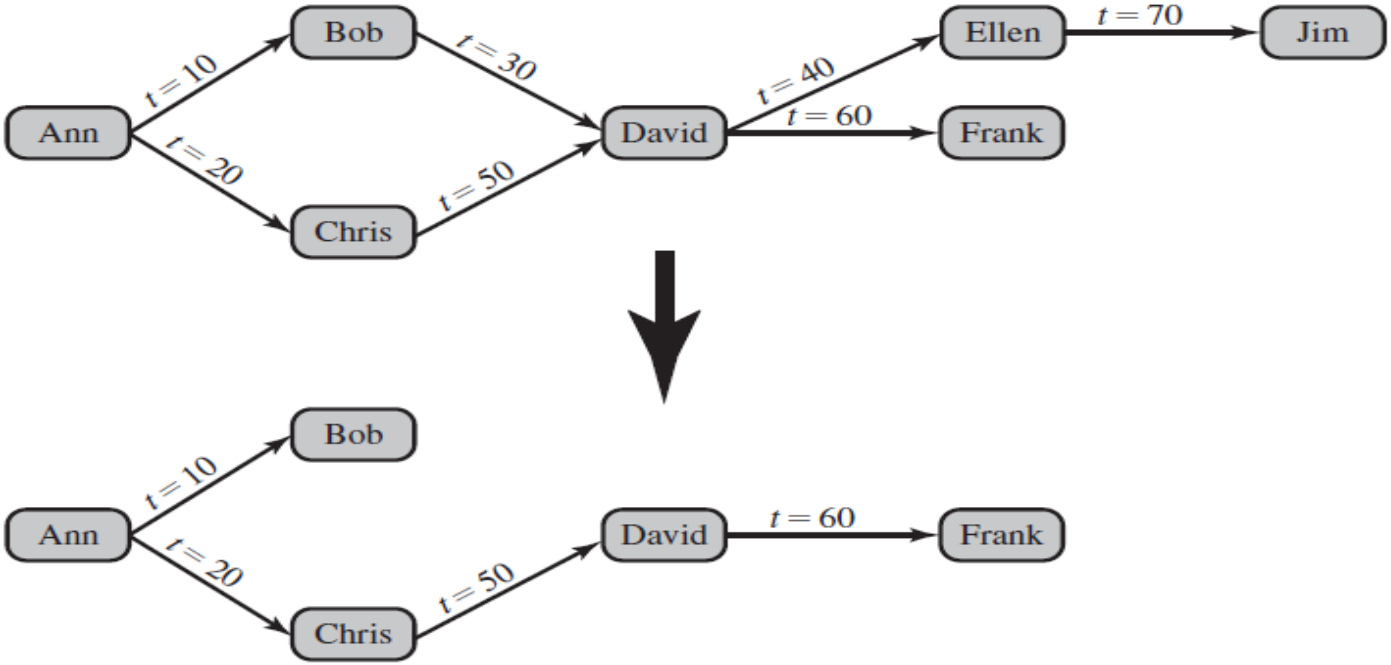
SQL-Based Access Definition…

```
REVOKE      { privileges | role }
[ON         table]
FROM        { user | role | PUBLIC }
```

Thus, the following statement revokes the access rights of the preceding example:

```
REVOKE SELECT ON ANY TABLE FROM ricflair
```

Cascading Authorizations



- To generalize, the convention followed by most implementations is as follows.
- When user A revokes an access right, any cascaded access right is also revoked, unless that access right would exist even if the original grant from A had never occurred.

Inferential attack (gathering info)

- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
  - Illegal/logically incorrect queries: lets an attacker gather important information about the type and structure of the backend database of a Web application

Out-band attack

- This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax (not sufficiently strict)

Role-Based Access Control

- Role-based access control work well for DBMS
  - eases admin burden, improves security
- Categories of database users:
  - application owner
  - end user
  - administrator
- DB RBAC must manage roles and their users

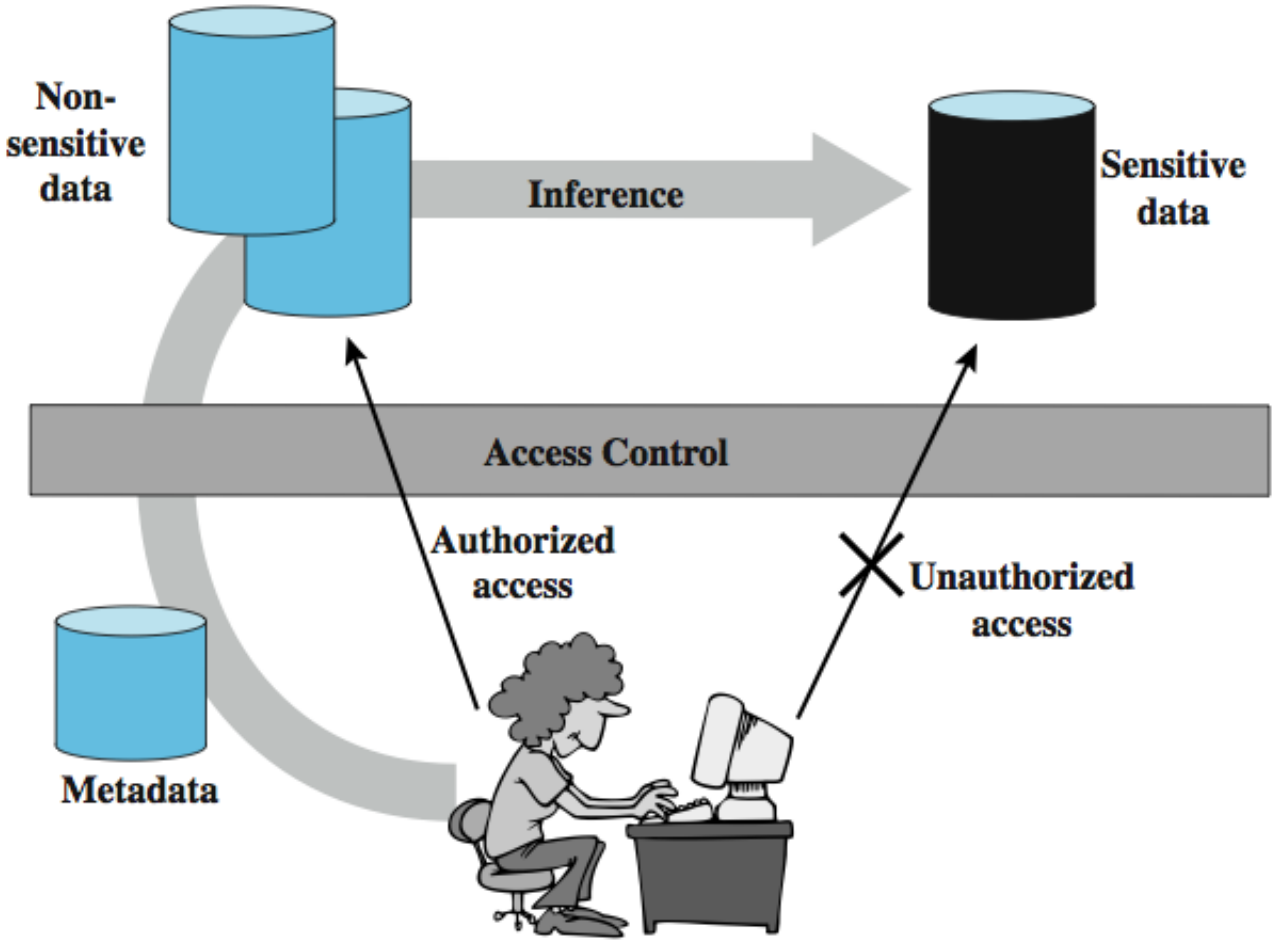
Role-Based Access Control…

Role	Permissions
Fixed Server Roles	
sysadmin	Can perform any activity in SQL Server and have complete control over all database functions
serveradmin	Can set server-wide configuration options, shut down the server
setupadmin	Can manage linked servers and startup procedures
securityadmin	Can manage logins and CREATE DATABASE permissions, also read error logs and change passwords
processadmin	Can manage processes running in SQL Server
Dbcreator	Can create, alter, and drop databases
diskadmin	Can manage disk files
bulkadmin	Can execute BULK INSERT statements
Fixed Database Roles	
db_owner	Has all permissions in the database
db_accessadmin	Can add or remove user IDs
db_datareader	Can select all data from any user table in the database
db_datawriter	Can modify any data in any user table in the database
db_ddladmin	Can issue all data definition language statements
db_securityadmin	Can manage all permissions, object ownerships, roles and role memberships
db_backupoperator	Can issue DBCC, CHECKPOINT, and BACKUP statements
db_denydatareader	Can deny permission to select data in the database
db_denydatawriter	Can deny permission to change data in the database

Inference

- Inference, as it relates to database security, is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.
- In general terms, two inference techniques can be used to derive additional information:
  - analyzing functional dependencies between attributes within a table or across tables,
  - merging views with the same constraints.

Inference


Non-
sensitive
data
Inference
Sensitive
data
Access Control
Authorized
access
Unauthorized
access
Metadata

Inference…

```
CREATE view V1 AS
SELECT Availability, Cost
FROM Inventory
WHERE Department = "hardware"
```

```
CREATE view V2 AS
SELECT Item, Department
FROM Inventory
WHERE Department = "hardware"
```

- Users of these views are not authorized to access the relationship between Item and Cost.
- A user who has access to either or both views cannot infer the relationship by functional dependencies.
- That is, there is not a functional relationship between Item and Cost such that knowing Item and perhaps other information is sufficient to deduce Cost.

Inference…

- A user who knows the structure of the Inventory table and who knows that the view tables maintain the same row order as the Inventory table is then able to merge the two views to construct the table shown in Figure.
- This violates the access control policy that the relationship of attributes Item and Cost must not be disclosed

Inference Example

Name	Position	Salary ($)	Department	Dept. Manager
Andy	senior	43,000	strip	Cathy
Calvin	junior	35,000	strip	Cathy
Cathy	senior	48,000	strip	Cathy
Dennis	junior	38,000	panel	Herman
Herman	senior	55,000	panel	Herman
Ziggy	senior	67,000	panel	Herman

(a) Employee table

Position	Salary ($)
senior	43, 000
junior	35,000
senior	48,000

Name	Department
Andy	strip
Calvin	strip
Cathy	strip

(b) Two views

Name	Position	Salary ($)	Department
Andy	senior	43,000	strip
Calvin	junior	35,000	strip
Cathy	senior	48,000	strip

(c) Table derived from combining query answers

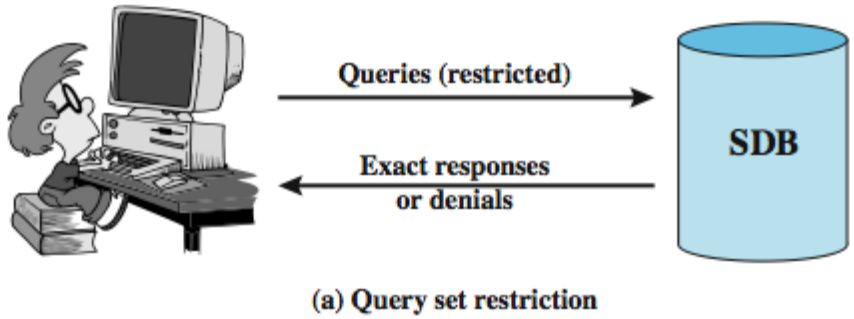
Inference Countermeasures

- Inference detection at database design
  - alter database structure or access controls
  - Examples include removing data dependencies by splitting a table into multiple tables or using more fine grained access control roles in an RBAC scheme.
  - Techniques in this category often result in unnecessarily stricter access controls that reduce availability.
- Inference detection at query time
  - If an inference channel is detected, by monitoring and altering or rejecting queries
- For either of the preceding approaches, some inference detection algorithm is needed. This is a difficult problem and the subject of ongoing research.

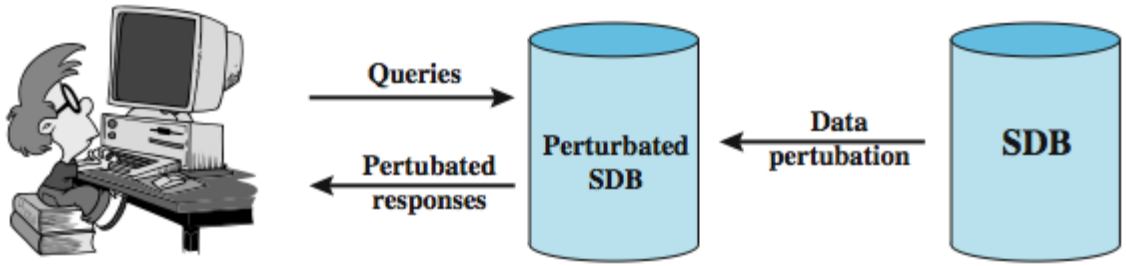
Statistical Databases

- Provides data of a statistical nature
  - e.g. counts, averages
- Two types:
  - pure statistical database
  - ordinary database with statistical access
    - some users have normal access, others statistical
- Access control objective to allow statistical use without revealing individual entries
- Security problem is one of inference

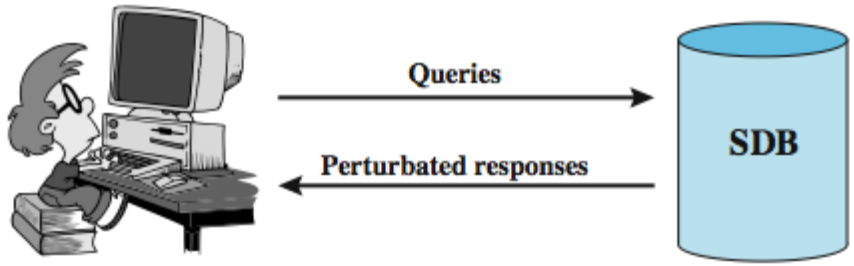
Protecting Against Inference



(a) Query set restriction



(b) Data perturbation



(c) Output perturbation

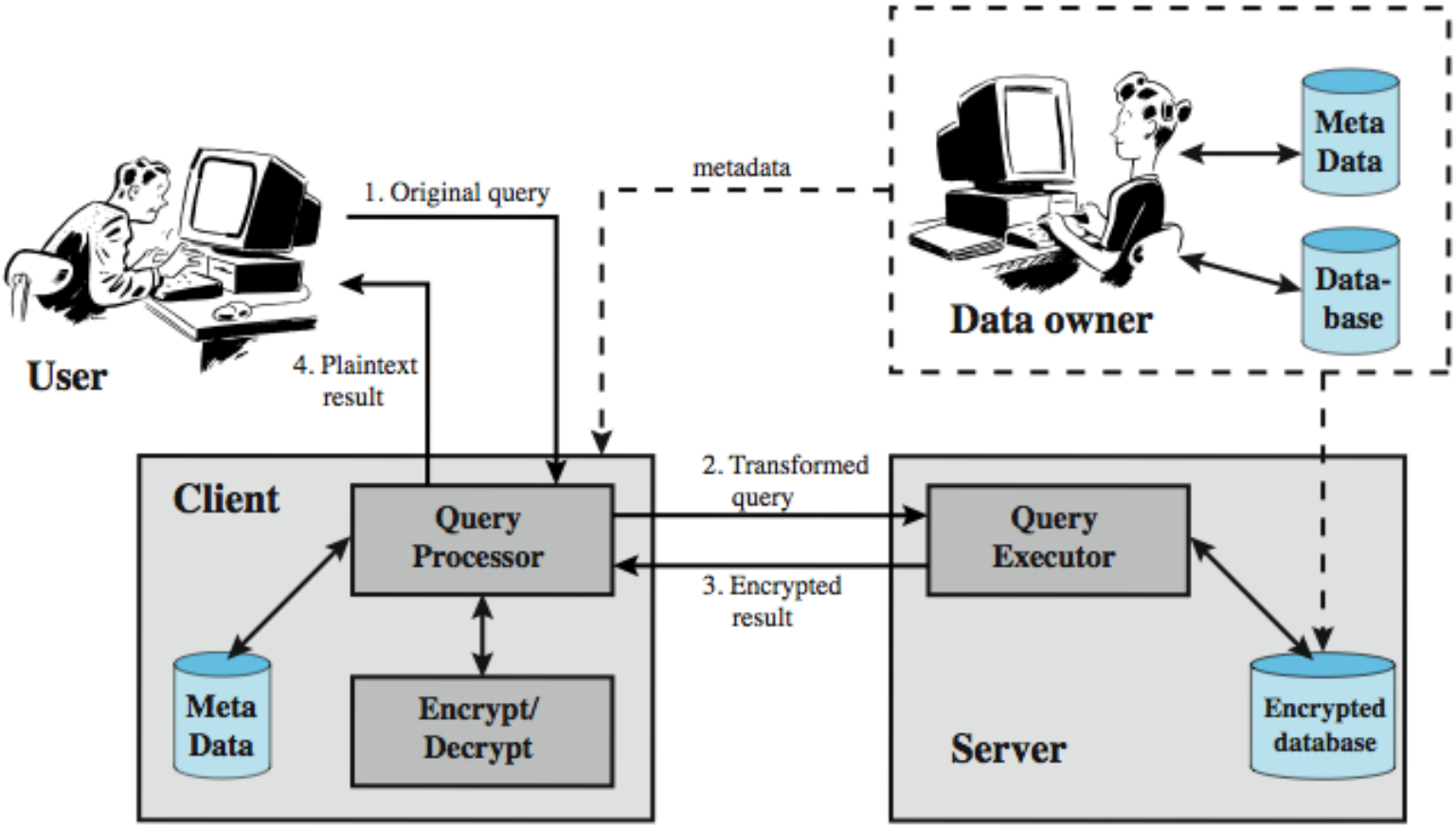
Perturbation

- Add noise to statistics generated from data
  - will result in differences in statistics
- Data perturbation techniques
  - data swapping
  - generate statistics from probability distribution
- Output perturbation techniques
  - random-sample query
  - statistic adjustment
- Must minimize loss of accuracy in results

Database Encryption

- Databases typical a valuable info resource
  - protected by multiple layers of security: firewalls, authentication, O/S access control systems, DB access control systems, and database encryption
- Can encrypt
  - entire database - very inflexible and inefficient
  - individual fields - simple but inflexible
  - records (rows) or columns (attributes) - best
    - also need attribute indexes to help data retrieval
- Varying trade-offs

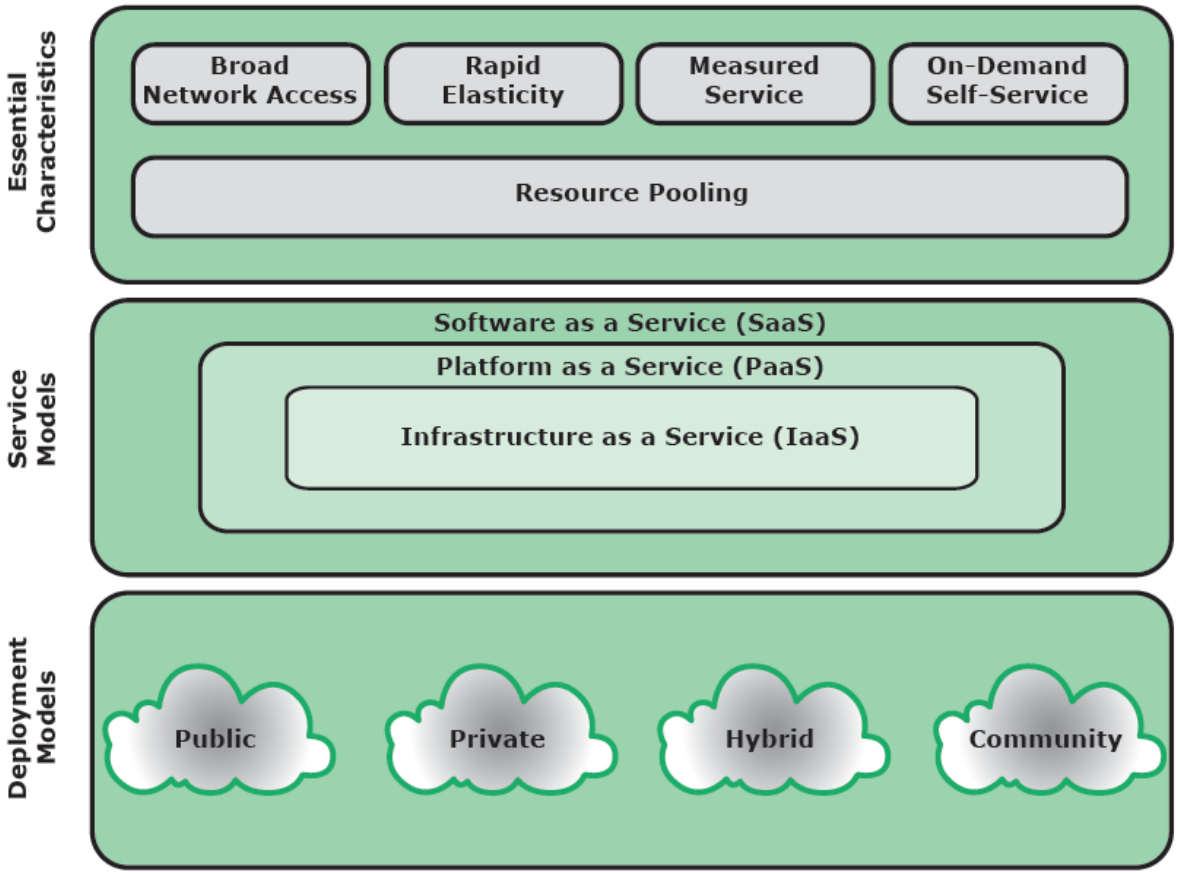
Database Encryption



Cloud computing

- An increasing trend in many organizations to move a substantial portion (or all) of their IT to cloud computing
- NIST SP-800-145 defines cloud computing as: "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. …"

Cloud computing elements



Essential characteristics: Broad network access

- Capabilities available over a network
- Accessed thru standard mechanisms
- Use by heterogeneous client platforms (desktops, laptops, tablets, cell phones)

Essential characteristics: Rapid elasticity

- The ability to expand/reduce services to specific requirements
- Large numbers of servers during the holidays
- Smaller number of resources during off-peak periods
- Release a resource when a task is completed

Essential characteristics: Measured service

- Cloud system automatically
  - Control and optimize resource use by leveraging a metering capability appropriate to the type of service
  - Storage, processing, bandwidth, active users

Essential characteristics: On-demand service

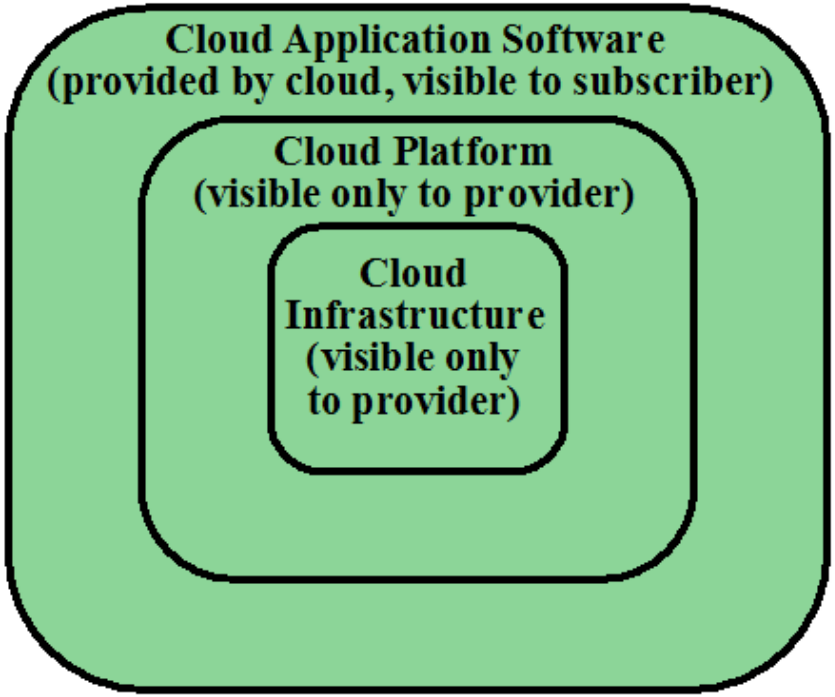
- A consumer can unilaterally provision computing capabilities without requiring human interaction
  - Server time, network storage
  - Resources wont have to a permanent part of the client's IT infrastructure

Essential characteristics: Resource pooling

- As a consequence of the above
- The providers resources are pooled to serve multiple consumers using a multi-tenant model
- Multiple resources assigned and re-assigned to clients
  - Storage, processing power, bandwidth …
- Consumers need not to know the physical location of the service

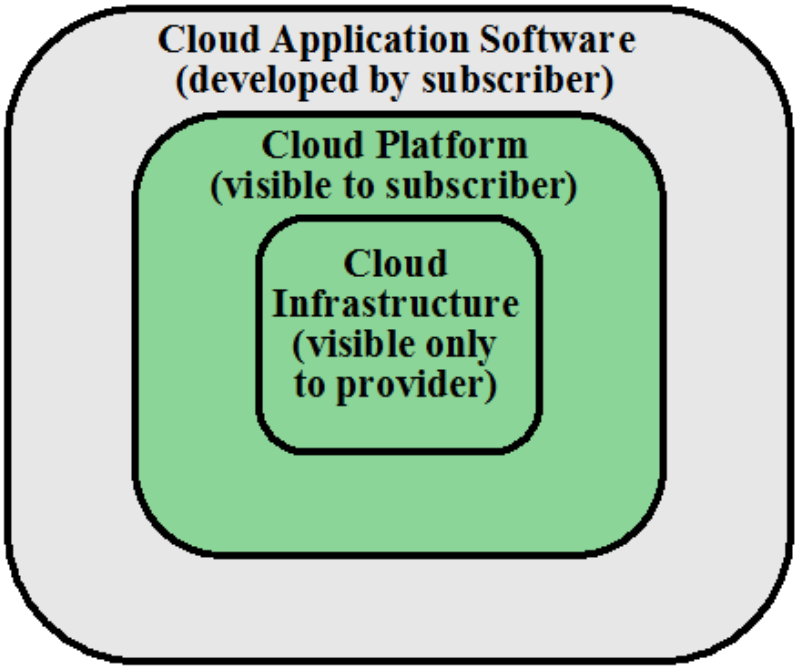
Service model: SaaS

- provides service to customers in the form of application software
- Clients need not to install
- Clients can access application via various platforms thru a simple interface (often a browser)



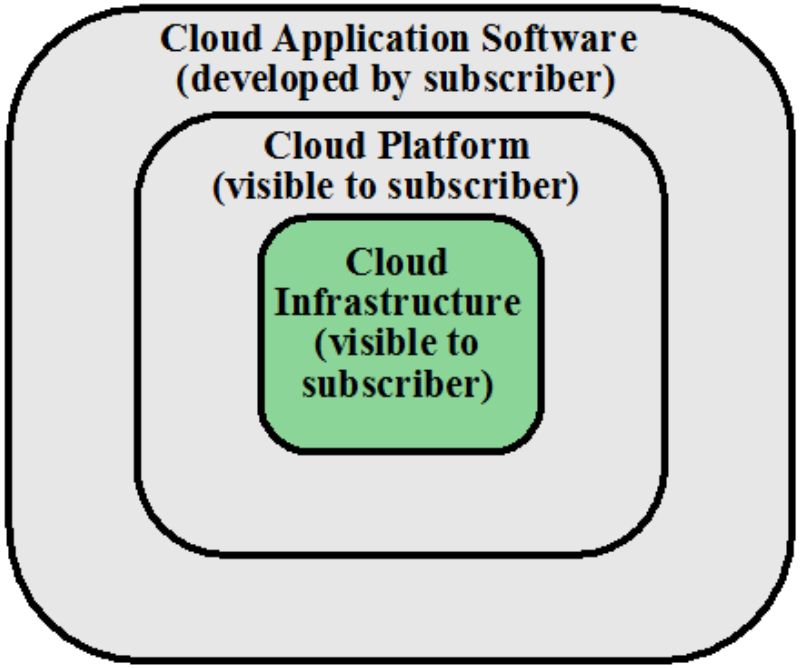
Service model: PaaS

- Provides service to customers in the form of a platform on the which the customer apps can run
- Clients deploy on the cloud
- PaaS provides useful building block/tools



Service model: IaaS

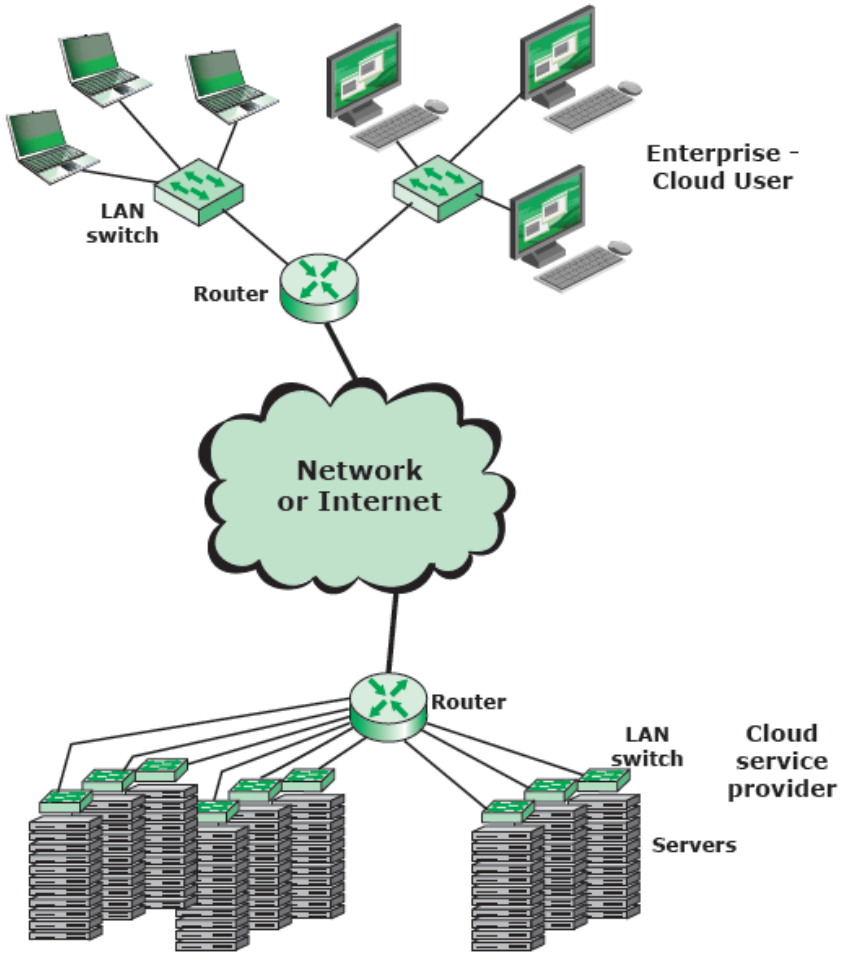
- Provides clients access to the underlying cloud infrastructure
- VM and other abstracted hardware, OS, APIs
- Amazon Elastic Computing (EC2) and Windows Azure



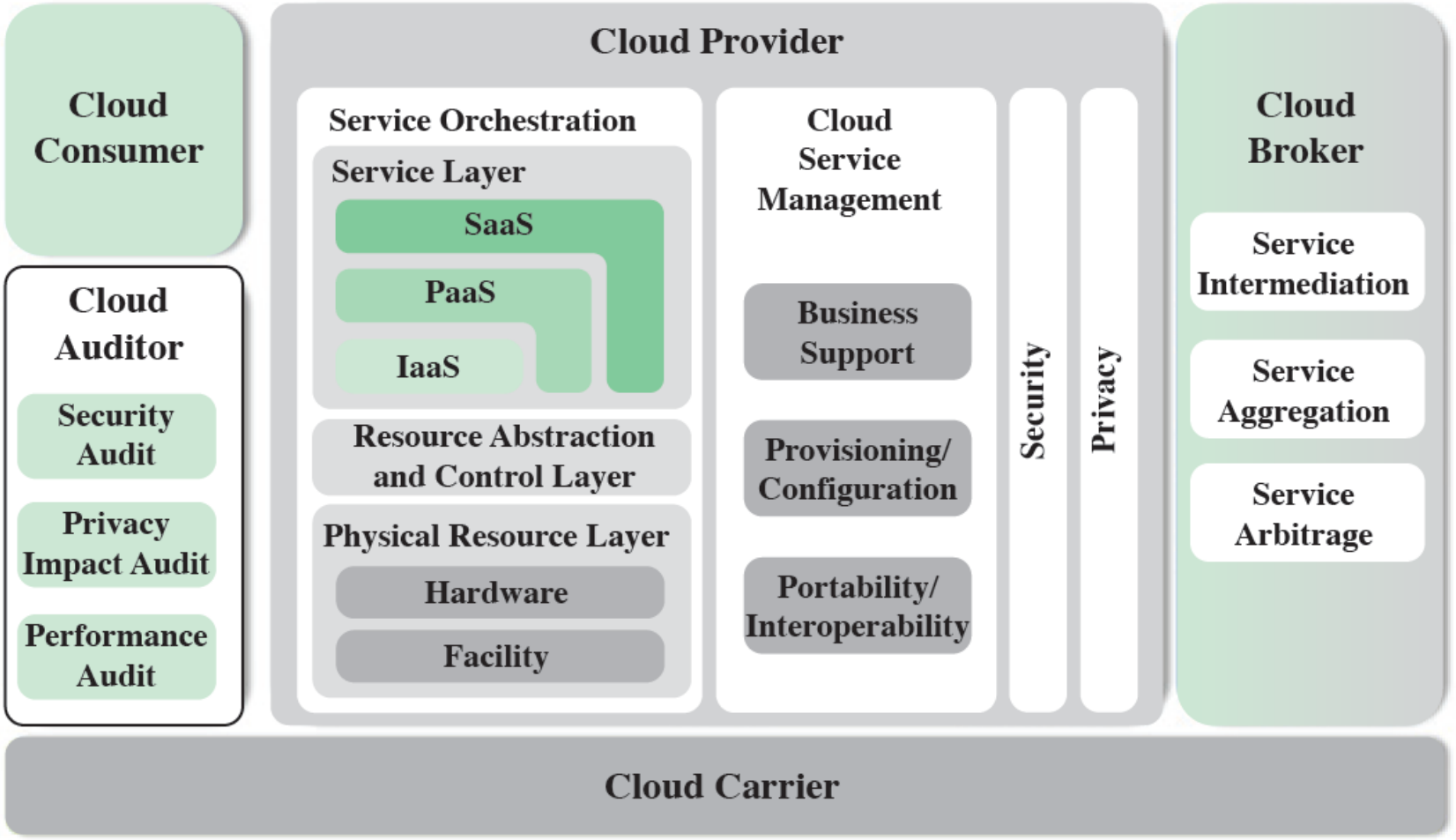
Deployment models

- **Public**: the cloud resources/services are available to the general public
- **Private**: The cloud infrastructure is solely for an organization
- **Community**: the cloud infrastructure is for a specific community and is shared by several organizations
- **Hybrid**: a composition two or more of the above

A typical cloud service context



NIST's reference architecture (conceptual model)



NIST's reference architecture (conceptual model)

- **Cloud customer**: A person or organization that uses or is interested in cloud providers services
- **Cloud provider** (CP): a person or organization that makes cloud services available
- **Cloud auditor**: A party that conducts independent assessment of sources (e.g., security)
- **Cloud broker**: A party that manages use, performance,, negotiations
- **Cloud carrier**: An intermediator that provides connectivity and service transport

Cloud provider (CP)

- For SaaS: CP deploys, configures, maintains, updates app software
- For PaaS: CP manages the computing infrastructure for the platform (middleware, database, OS, programming languages, tools)
- For IaaS: CP acquires physical computing resources: servers, network, storage, …

Cloud security risks

- **Abuse and nefarious use of cloud computing**
  - Relatively easy to register for the services
  - Many cloud services offer free trials
  - Enables hackers to get inside to conduct attacks (spamming, DoS, …)
  - The burden on CP to provide protection
- Countermeasures
  1. Stricter/restrict registration
  2. Enhanced credit card monitoring
  3. Comprehensive monitoring (traffic)

Cloud security risks

- **Insecure interfaces of APIs**
  - CPs expose a set of APIs for customers apps
  - Security depends on APIs: must be secure (from authentication to encryption)
- Countermeasures
  1. Analyzing the security of APIs
  2. Ensuring strong authentication and access control
  3. Understanding the dependency chair between the APIs

Cloud security risks

- **Malicious insiders**
  - Client organization relinquishes many (or all) of its IT and gives to the CP
  - A grave concern: malicious insider activity
- Countermeasures (by client)
  1. Comprehensive supplier assessment
  2. Specify human resource requirements as part of legal contract
  3. Require transparency

Cloud security risks

- **Shared technology issues**
  - IaaS services are delivered in a scalable way by a shared infrastructure (CPU caches, GPUs, …)
  - Probably not designed for multi-tenant architecture
  - Vulnerable to attacks (insider and outsiders)
- Countermeasures
  1. Implement best security practices during implementation, deployment, configuration
  2. Monitor environment for unauthorized activities
  3. Promote strong authentication and access control

Cloud security risks

- **Data loss or leakage**
  - Cloud storage may be the only backup storage
  - Could be devastating for many clients if data is lost
- Countermeasures
  1. Implement strong API access control
  2. Encrypt and protect integrity when in transit
  3. Analyze data protection at design and run time

Cloud security risks

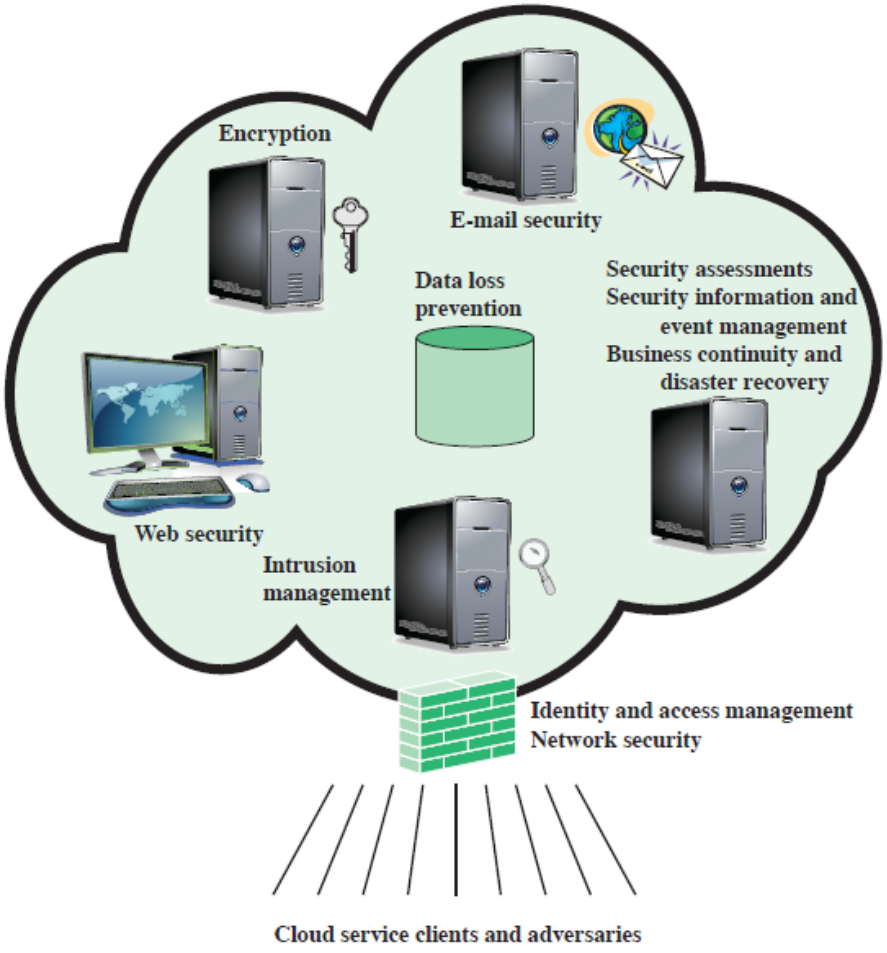
- **Account or service hijacking**
  - Usually with stolen credentials
  - Compromise confidentiality, integrity and availability
- Countermeasures
  1. Prohibit sharing of credentials between users
  2. Leverage strong multi-factory authentication
  3. Employ proactive monitoring

Data protection in the cloud

- Data must be secured while at transit, in use, or at rest
  - Client can employ encryption for transit
  - Client can encrypt data for storage (rest) but can also be CP's responsibility (key management)

Cloud security as a service

- Identify management
- Data loss prevention
- Web security
- E-mail security
- Encryption
- Business continuity
- Network security
- …



Thank You !!!