Database Security and Auditing: Protecting Data Integrity and Accessibility

Chapter 5

Database Application Security Models

Objectives

- Describe the different types of users in a database environment and the distinct purpose of each
- Identify and explain the concepts of five security models
- List the most commonly used application types

Objectives (continued)

- Implement the most common application security models
- Understand the use of data encryption within database applications

Types of Users

- Application:
  - Solves a problem
  - Performs a specific business function
- Database: collection of related data files used by an application
- Application user: user within the application schema

Types of Users (continued)

- Types:
  - Application administrator
  - Application owner
  - Application user
  - Database administrator
  - Database user
  - Proxy user
  - Schema owner
  - Virtual user

Security Models

- Access Matrix Model:
  - Represents two main entities: objects and subjects:
    - Columns represent objects
    - Rows represent subjects
  - Objects: tables, views, procedures, database objects
  - Subjects: users, roles, privileges, modules
  - Authorization cell

Security Models (continued)

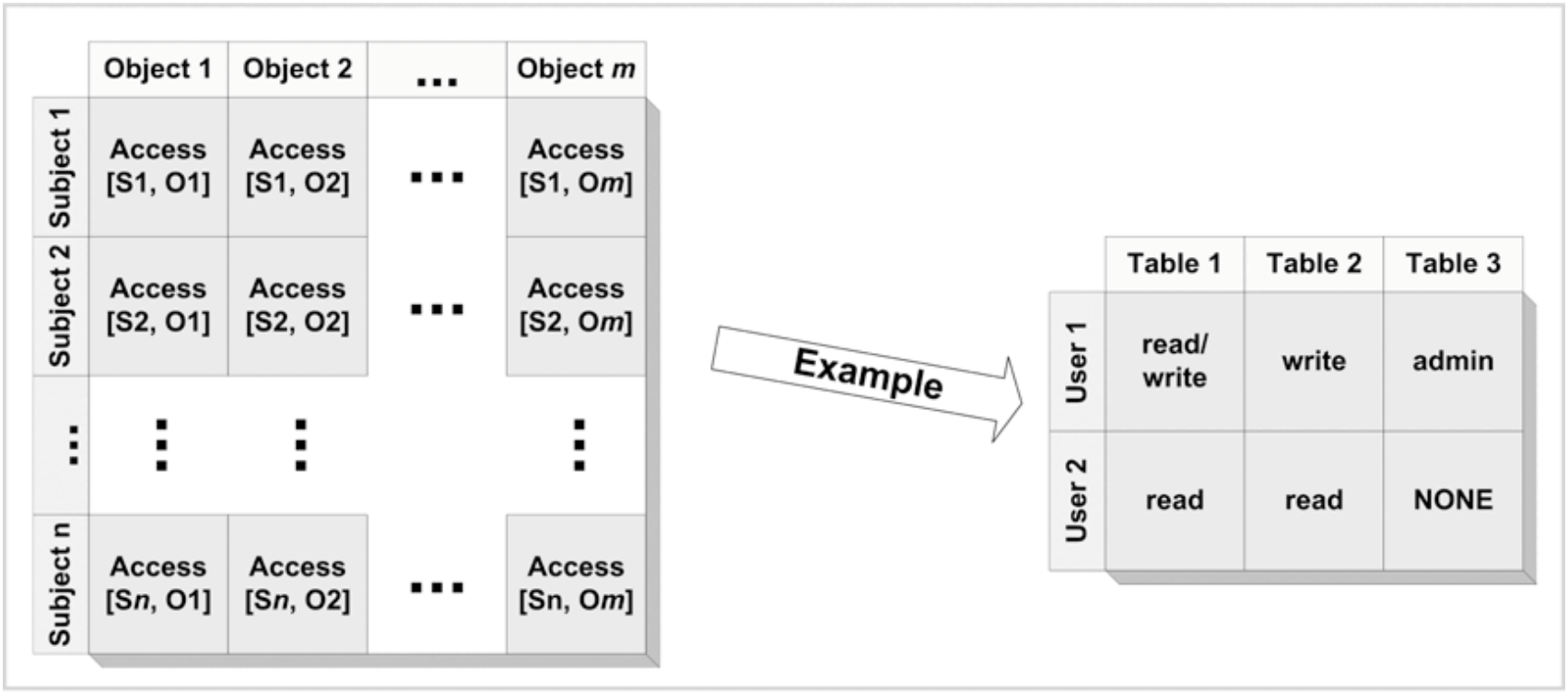

FIGURE 5-1 Access matrix security model

Security Models (continued)

- Access Modes Model:
  - Based on the Take-Grant model
  - Uses objects and subjects
  - Specifies access modes: static and dynamic modes
  - Access levels: a subject has access to objects at its level and all levels below it

Security Models (continued)

Table 5-1 Access modes

Static Modes

Access Mode	Level	Description
use	1	Allows the subject to use the object without modifying the object
read	2	Allows the subject to read the contents of the object
update	3	Allows the subject to modify the contents of the object
create	4	Allows the subject to add instances to the object
delete	4	Allows the subject to remove instances of the object

Security Models (continued)

Table 5-1 Access modes (continued)

Dynamic Modes

Access Mode	Level	Description
grant	1	Allows the subject to grant any static access mode to any other subject
revoke	1	Allows the subject to revoke a granted static access mode from a subject
delegate	2	Allows the subject to grant the grant privilege to other subjects
abrogate	2	Allows the subject to grant the revoke privilege to other subjects

Application Types

- Client/Server applications:
  - Management Information System (MIS) department:
    - Thirty year ago centralized information
    - Developed mainframe projects
    - Was a bottleneck
  - Personal computer was introduced: developing need for client/server applications
  - Based on the business model

Client/Server Applications

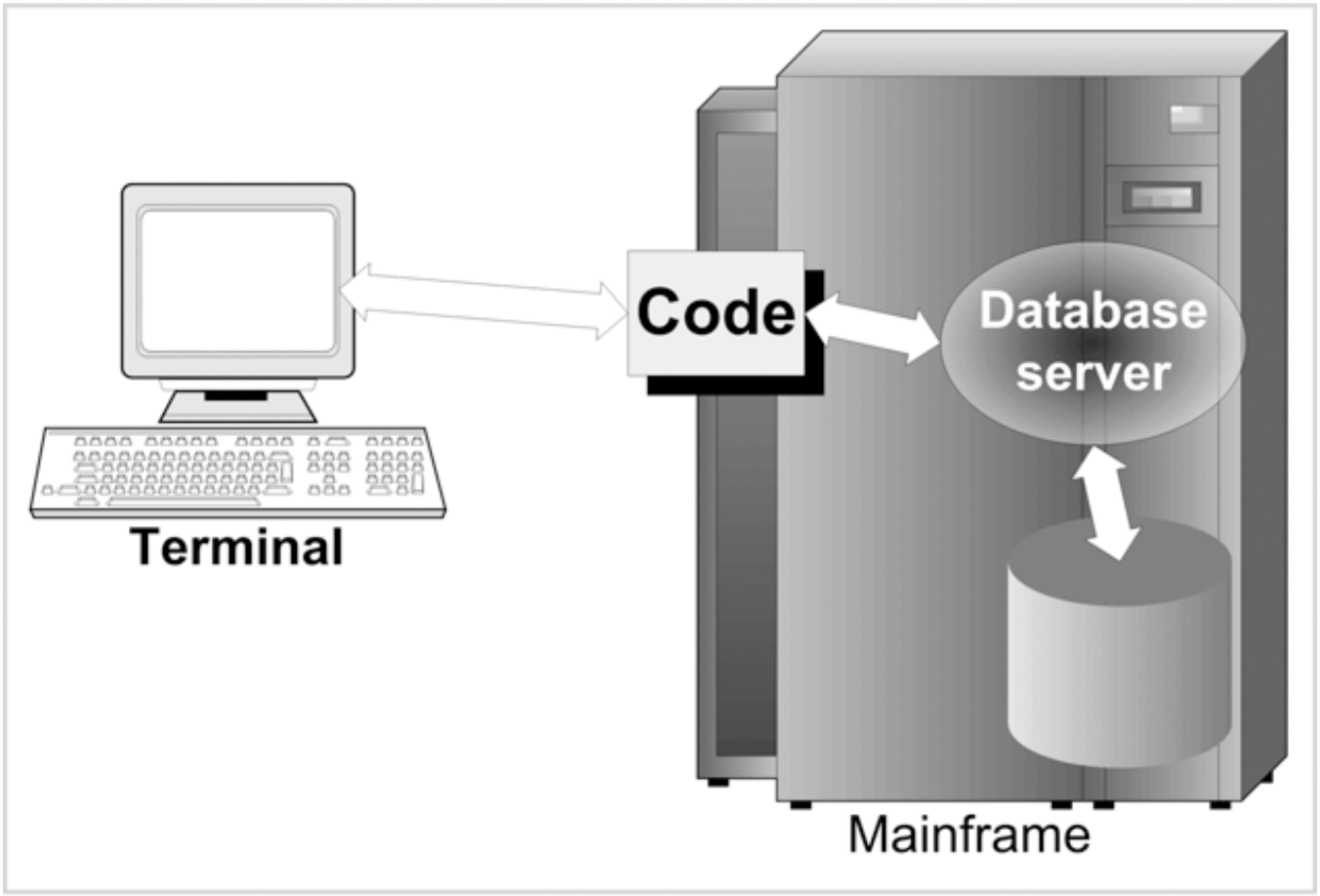

FIGURE 5-2 Mainframe application architecture

Client/Server Applications (continued)

- Provides a flexible and scalable structure
- Components:
  - User interface
  - Business logic
  - Data access
- Components usually spread out over several tiers:
  - Minimum two
  - Normally, four to five

Client/Server Applications (continued)

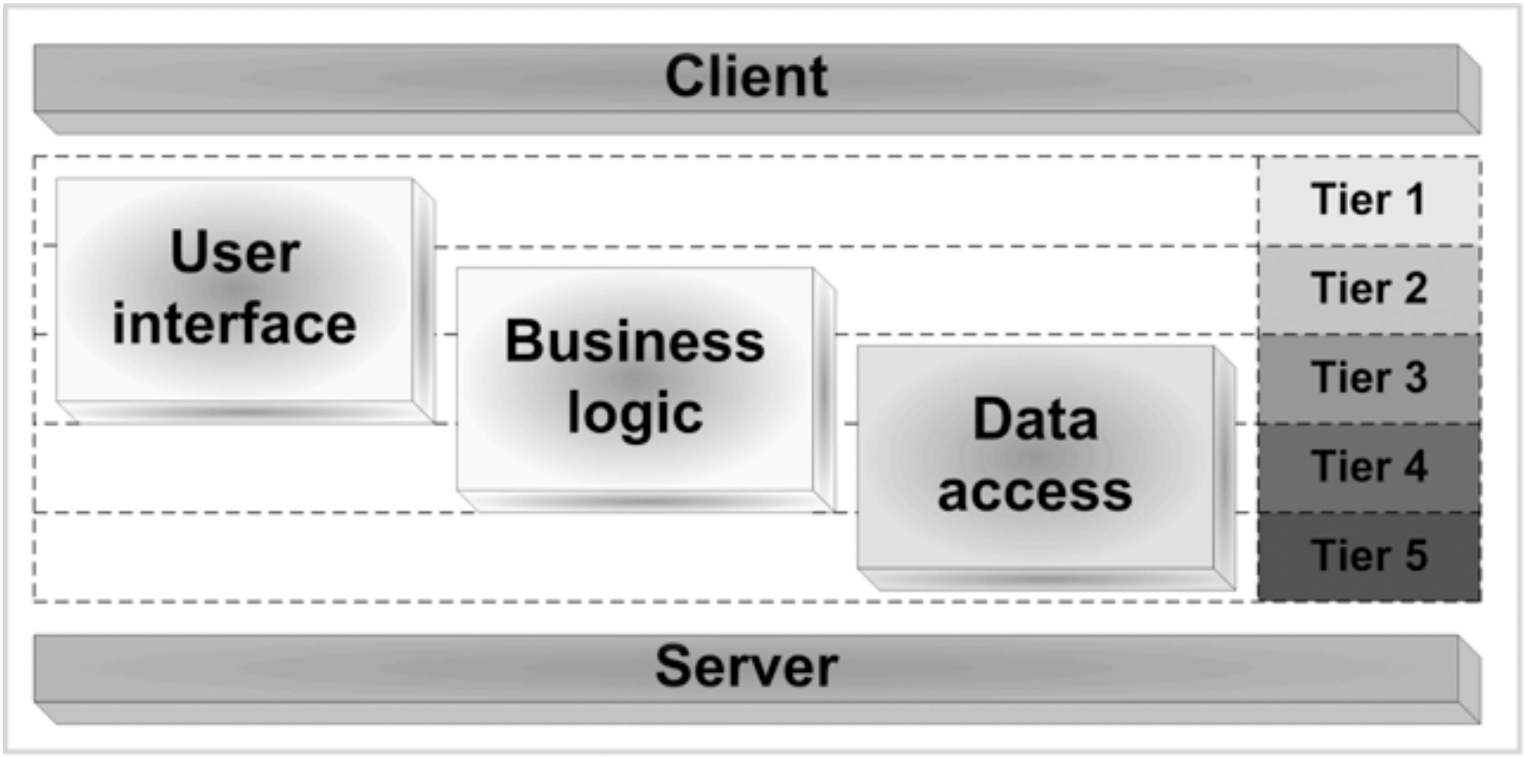

FIGURE 5-3 Logical components of a client/server application

Client/Server Applications (continued)

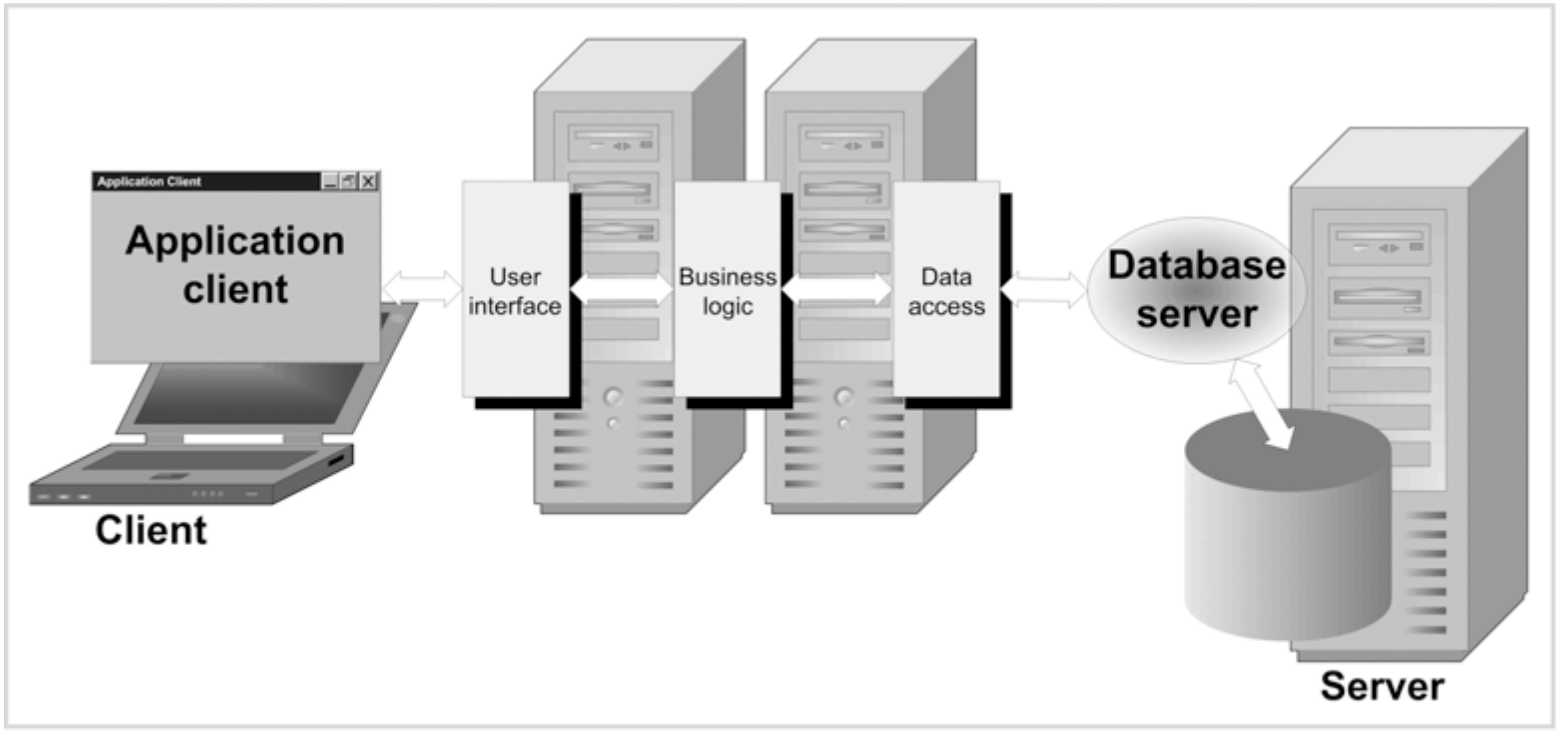

FIGURE 5-4 Physical architecture of a client/server application

Web Applications

- Evolved with the rise of dot-com and Web-based companies
- Uses the Web to connect and communicate to the server
- A Web application uses HTML pages created using:
  - ActiveX
  - Java applets or beans
  - ASP (Active Server Pages)

Web Applications (continued)

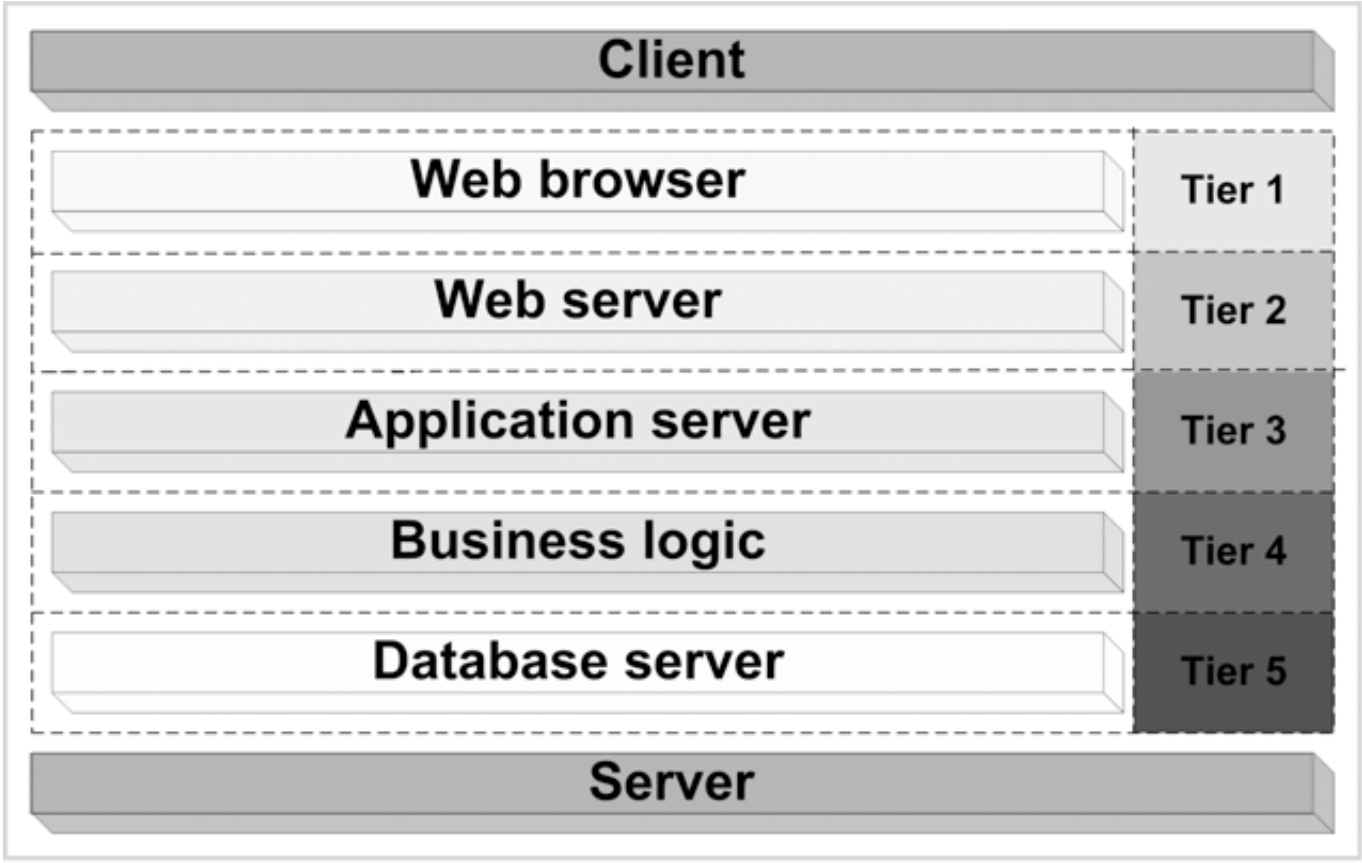

FIGURE 5-5 Logical components of Web application architecture

Web Applications (continued)

- Components:
  - Web browser layer
  - Web server layer
  - Application server layer
  - Business logic layer
  - Database server layer

Web Applications (continued)

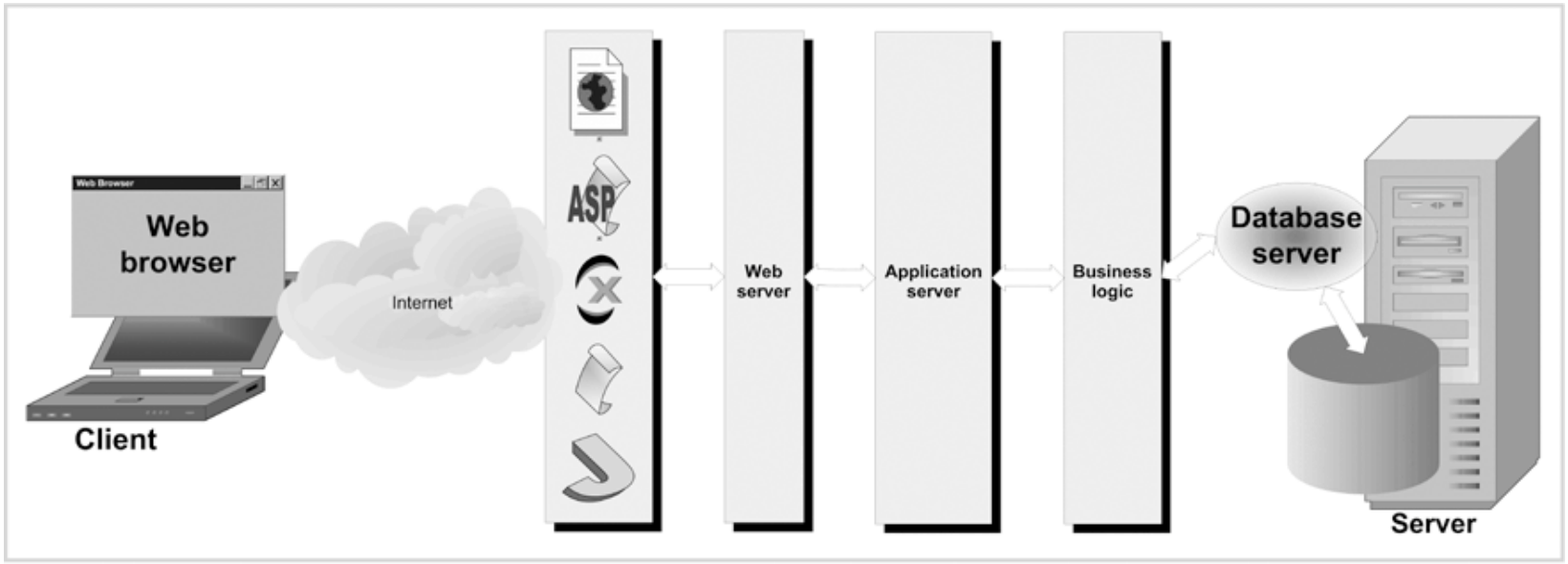

FIGURE 5-6 Physical structure of a Web application

Data Warehouse Applications

- Used in decision-support applications
- Collection of many types of data taken from a number of different databases
- Typically composed of a database server
- Accessed by software applications or reporting applications: online analytical processing (OLAP)

Data Warehouse Applications (continued)

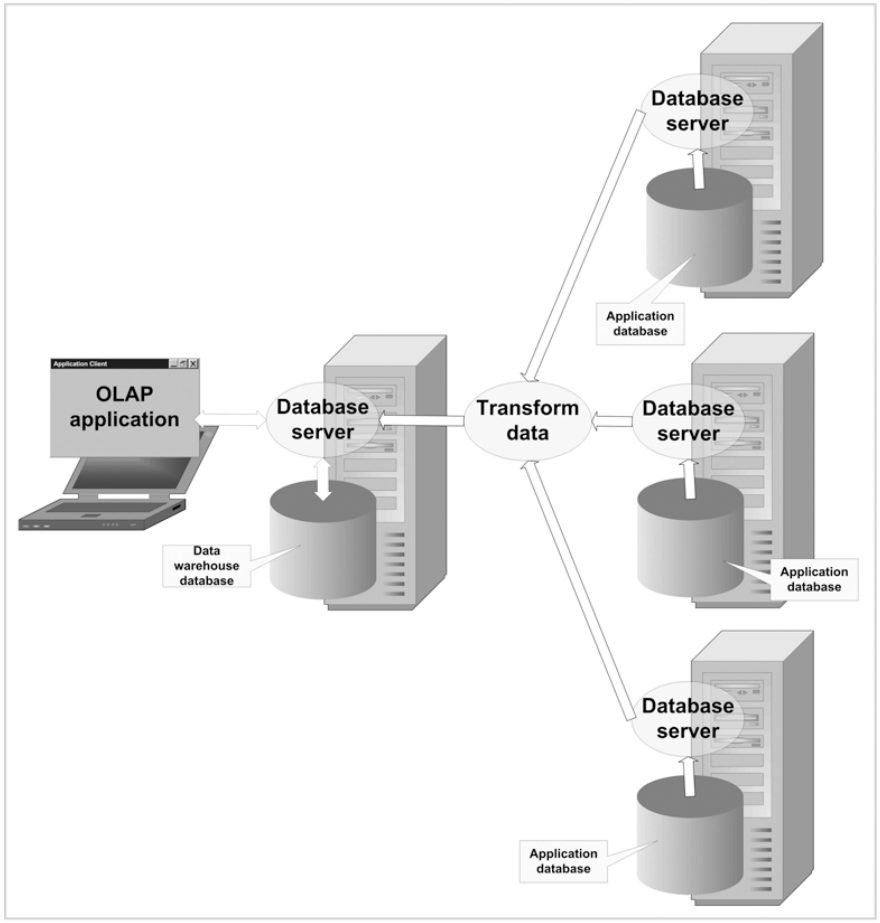

FIGURE 5-7 Physical and logical architecture of a data warehouse

Application Security Models

- Models:
  - Database role based
  - Application role based
  - Application function based
  - Application role and function based
  - Application table based

Security Model Based on Database Roles

- Application authenticates application users: maintain all users in a table
- Each user is assigned a role; roles have privileges assigned to them
- A proxy user is needed to activate assigned roles; all roles are assigned to the proxy user
- Model and privileges are database dependent

Security Model Based on Database Roles (continued)

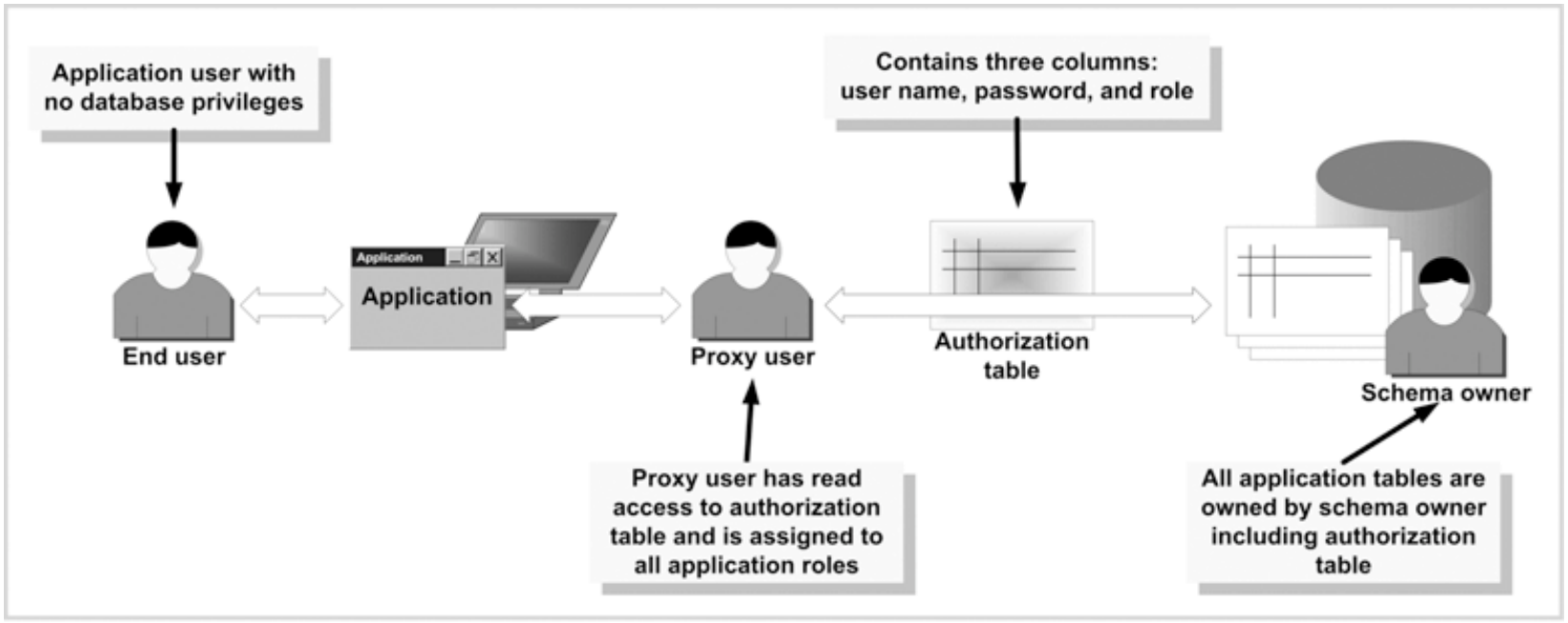

FIGURE 5-10 Architecture of a security data model based on database roles

Security Model Based on Database Roles (continued)

- Implementation in Oracle:
  - Create users
  - Add content to your tables
  - Add a row for an application user
  - Look for application user's role
  - Activate the role for this specific session

Security Model Based on Database Roles (continued)

- Implementation in SQL Server:
  - Use application roles:
    - Special roles you that are activated at the time of authorization
    - Require a password and cannot contain members
  - Connect a user to the application role: overrules user's privileges

Security Model Based on Database Roles (continued)

- Implementation in SQL Server (continued):
  - Create and drop application roles using the command line and the Enterprise Manager:
    - SP_ADDAPPROLE
    - SP_DROPAPPROLE
  - You can activate application roles using SP_SETAPPROLE

Security Model Based on Database Roles (continued)

- Implementation in SQL Server (continued):
  - Connect to database as the proxy user
  - Validate the user name and password
  - Retrieve the application role name
  - Activate the application role

Security Model Based on Database Roles (continued)

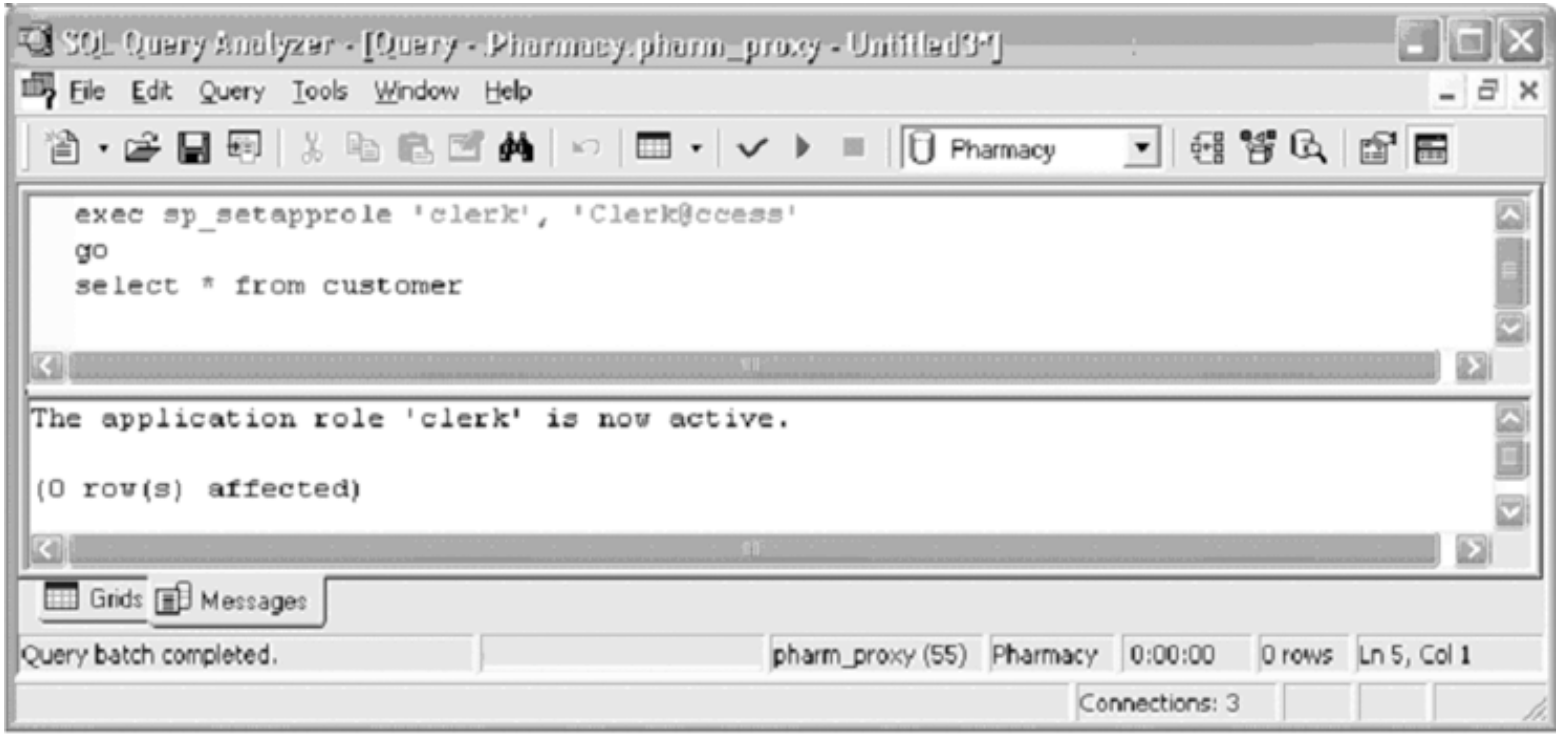

FIGURE 5-13 Application role activation

Security Model Based on Application Roles

- Application roles are mapped to real business roles
- Application authenticates users
- Each user is assigned to an application role; application roles are provided with application privileges (read and write)

Security Model Based on Application Roles (continued)

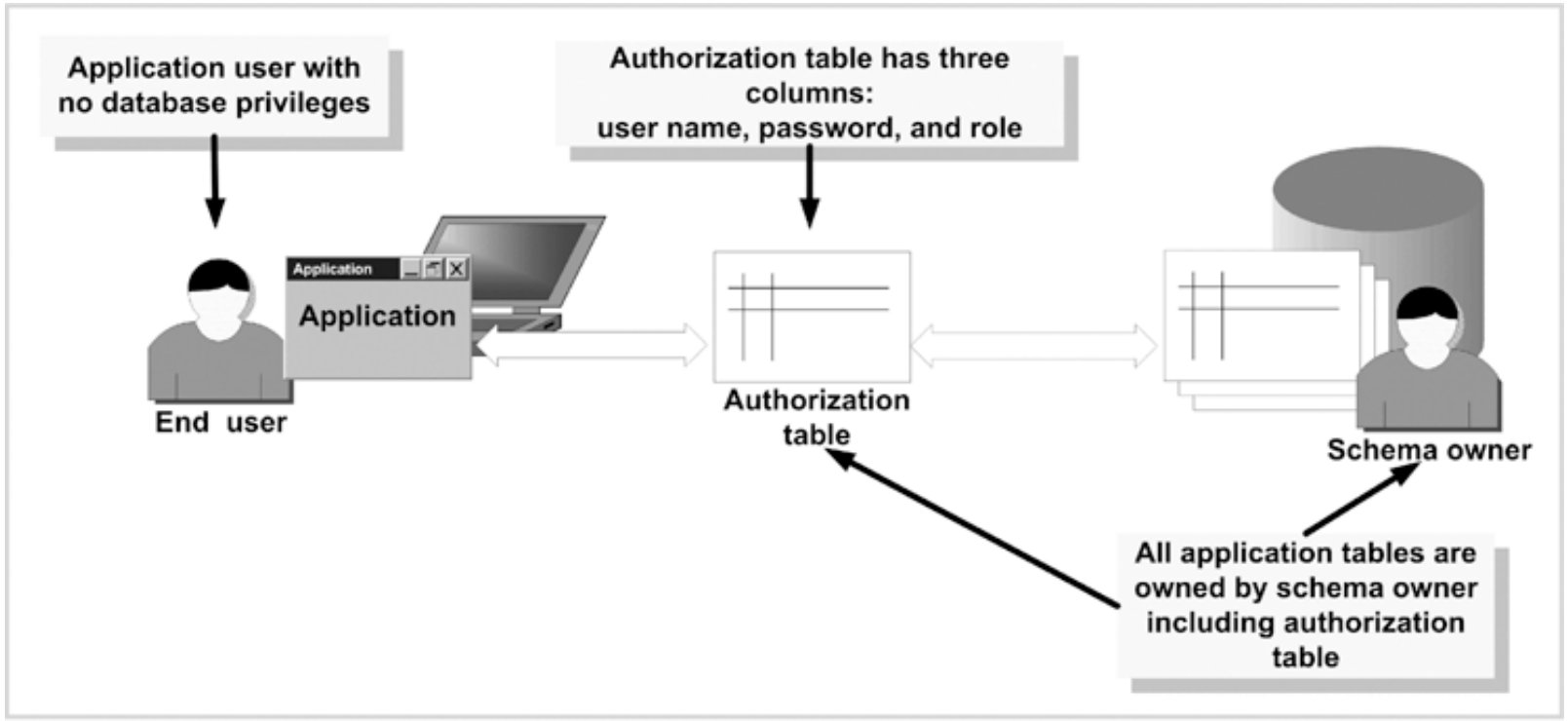

FIGURE 5-15 Architecture of a security data model based on application roles

Security Model Based on Application Roles (continued)

- Implementation in SQL Server
  - Create a database user
  - Connect the application to the database using this user
  - Create stored procedures to perform all database operations

Security Model Based on Application Functions

- Application authenticates users
- Application is divided into functions
- Considerations:
  - Isolates application security from database
  - Passwords must be securely encrypted
  - Must use a real database user
  - Granular privileges require more effort during implementation

Security Model Based on Application Functions (continued)

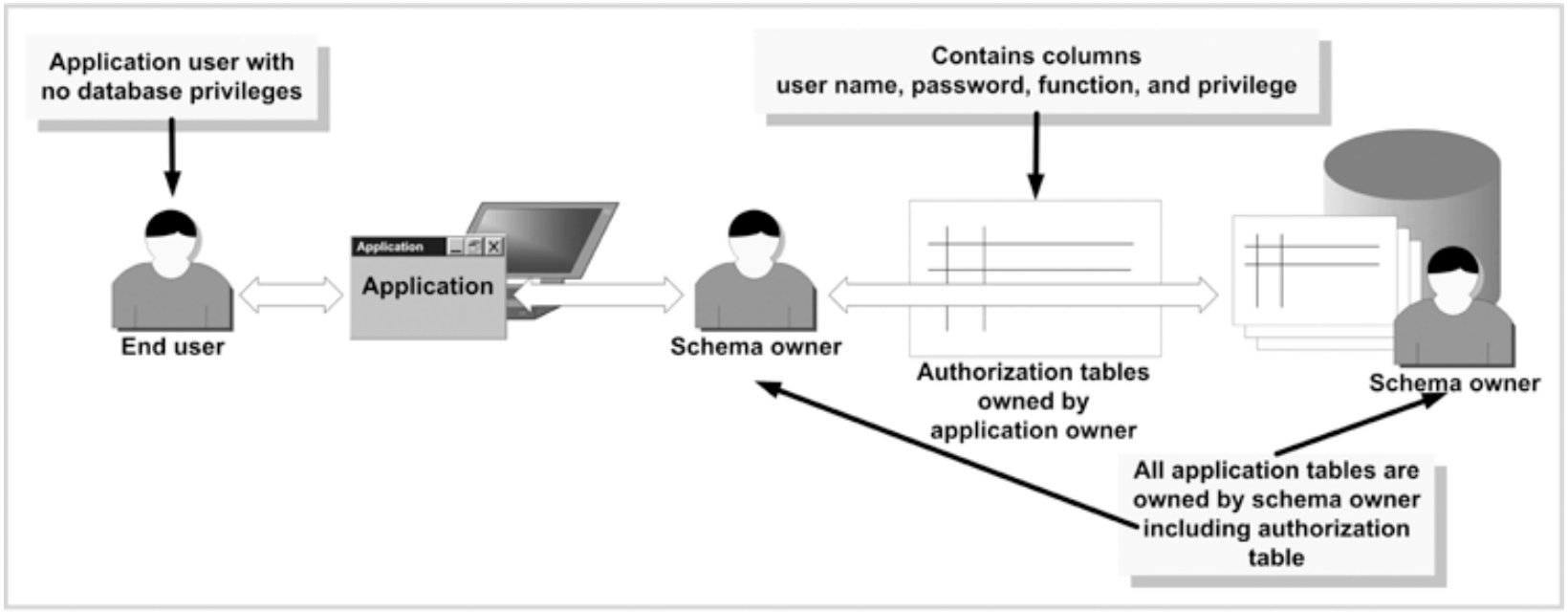

FIGURE 5-17 Architecture of a security data model based on application functions

Security Model Based on Application Roles and Functions

- Combination of models
- Application authenticates users
- Application is divided into functions:
  - Roles are assigned to functions
  - Functions are assigned to users
- Highly flexible model

Security Model Based on Application Roles and Functions (continued)

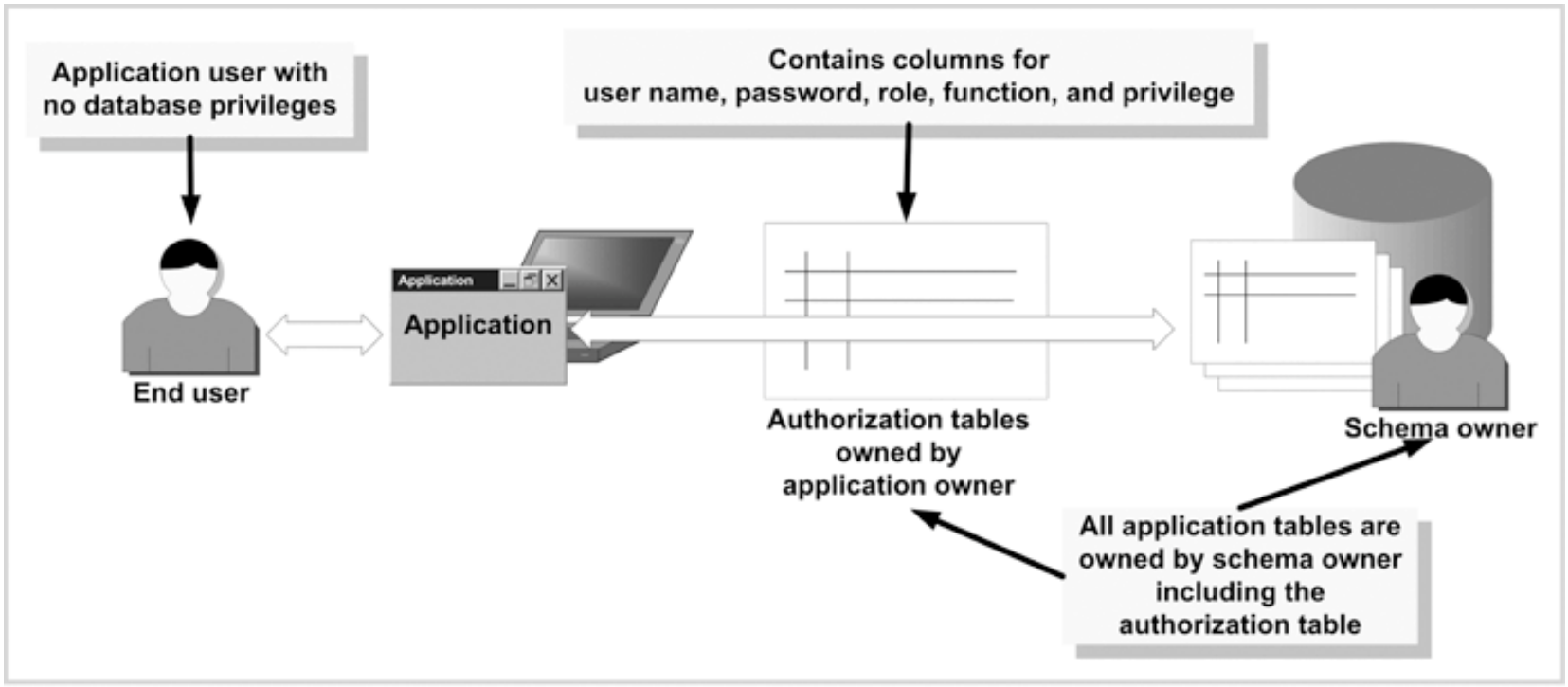

FIGURE 5-19 Architecture of a security data model based on application roles and functions

Security Model Based on Application Tables

- Depends on the application to authenticate users
- Application provides privileges to the user based on tables; not on a role or a function
- User is assigned access privilege to each table owned by the application owner

Security Model Based on Application Tables (continued)

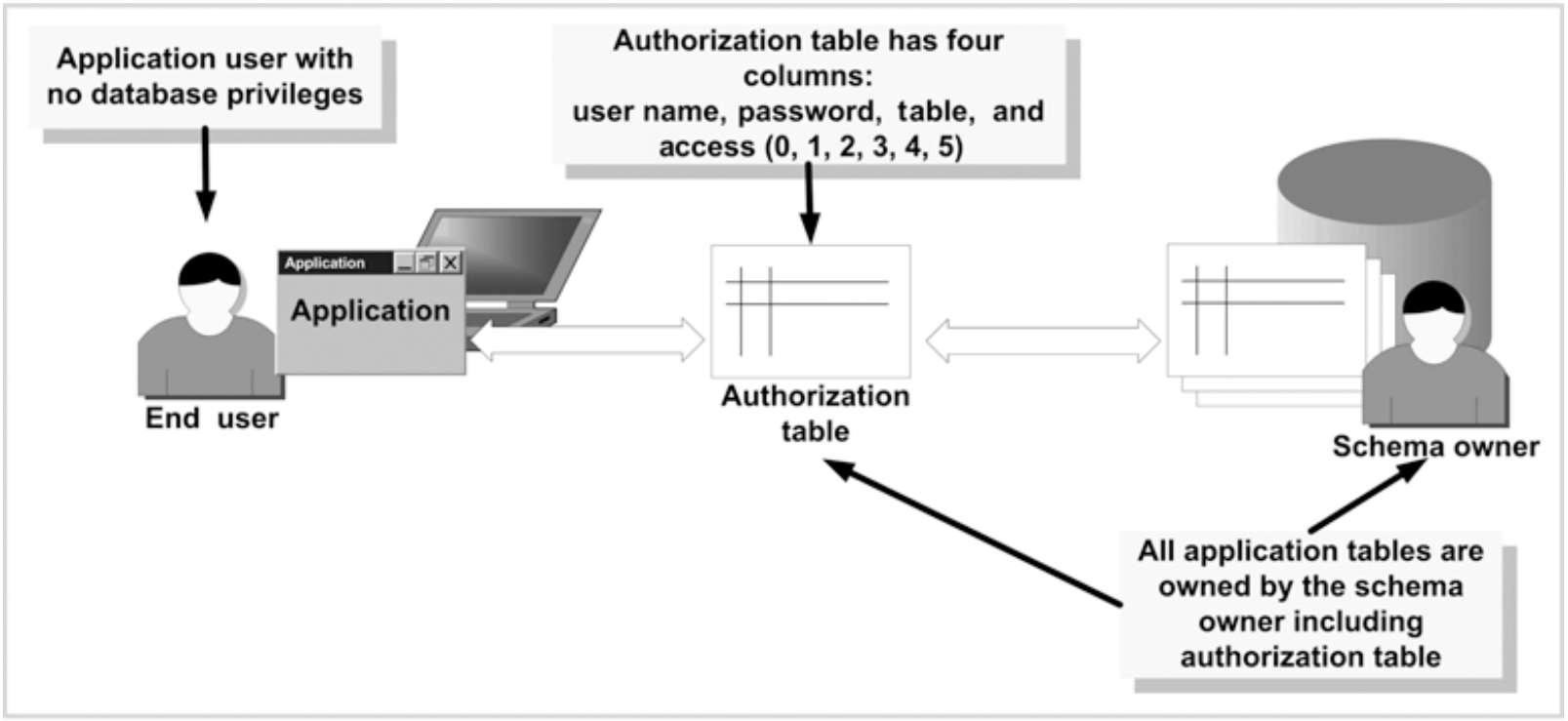

FIGURE 5-21 Architecture of a security data model based on application tables

Security Model Based on Application Tables (continued)

- Implementation in SQL Server:
  - Grant authorization on application functions to the end user
  - Alter authorization table from the security model based on database roles; incorporate the table and access columns required to support model

Application Security Models

Table 5-7 Characteristics of security models

	Security Model				
Characteristics	Database Role Based	Application Role Based	Application Function Based	Application Role and Function Based	Application Table Based
Is flexible in implementing application security	No	No	No	Yes	No
Isolates application security from the database	Yes	Yes	Yes	Yes	Yes
Maintenance of application security does not require specific database privileges	No	No	No	Yes	No

Application Security Models (continued)

Table 5-7 Characteristics of security models (continued)

	Security Model				
Characteristics	Database Role Based	Application Role Based	Application Function Based	Application Role and Function Based	Application Table Based
Password must be securely encrypted	Yes	Yes	Yes	Yes	Yes
Uses real database user to log on	No	Yes	Yes	Yes	Yes
Is business-function specific	No	No	Yes	Yes	No

Data Encryption

- Passwords should be kept confidential and preferably encrypted
- Passwords should be compared encrypted:
  - Never decrypt the data
  - Hash the passwords and compare the hashes

Data Encryption (continued)

FIGURE 5-22 Encryption process using private and public keys

Summary

- An application user is simply a record created for a user within the application schema; usually does not have database privileges or roles assigned
- Access matrix:
  - Columns represent objects
  - Rows represent subjects
  - Authorization cell
- Access mode

Summary (continued)

- Application types: client/server, Web, and Data Warehouse
- Application security models
  - Database roles
  - Application roles
  - Application functions
  - Roles and functions in the application
  - Application tables