|  |  |
| --- | --- |
| Ch 9  The Term | Definition |
| Web | distributed information system based on HyperText Markup Language (HTML) |
| Web browsers | have become the de-facto standard user interface to databases. providesa graphical user interface |
| forms | enabling users to enter data which can then be sent back to the Web server |
| Uniform Resource Locators (URLs). | is provided In the Web, functionality |
| HTML | HTML provides formatting, hypertext link, and image display features also provides input features |
| HyperText Transfer Protocol (HTTP) | used for communication with the Web server (**connectionless**) |
| http://www.acm.or g/sigmod | the document is to be accessed using the Hyper Text Transfer Protocol. \*second part gives the unique name of a machine on the Internet. \*The rest of the URL identifies the document within the machine. |
| document name in a URL | may identify an executable program, that, when run, generates a HTML document. |
| Common Gateway Interface (CGI | a standard interface between web and application server |
| Motivation | reduces load on server |
| Solution | use a cookie |
| cookie | Is small piece of text containing identifying information. can be stored permanently or for a limited time |
| Servlets | Application program (also called a servlet) is loaded into the server is defines an API for communication between the Web/ application server and application program running in the server |
| Servlet Sessions | Sets a cookie on first interaction with browser, and uses it to identify session on further interactions |
| Server-side scripting | simplifies the task of connecting a database to the Web Define an HTML document with embedded executable code/SQL queries. |
| PHP | is widely used for Web server scripting. Extensive libaries including for database access using ODBC |
| Client-side scripts/programs | allow documents to be active Browsers can fetch certain scripts (client-side scripts) or programs along with documents, and execute them in “safe mode” at the client site |
| Security | mechanisms needed to ensure that malicious scripts do not cause damage to the client machine . Disallows dangerous actions such as file writes |
| Javascript functions | \*Can check input for validity \*modify the displayed Web page, by altering the underling **document object model (DOM)** tree representation of the displayed HTML text |
| Application layers  1-Presentation or user interface | **model-view-controller (MVC)** architecture   * + - 1. **model**: business logic       2. **view**: presentation of data, depends on display device       3. **controller**: receives events, executes actions, and returns a view to the user   **business-logic** layer   1. provides high level view of data and actions on data 2. often using an object data model 3. hides details of data storage schema   **data access** layer   1. interfaces between business logic layer and the underlying database 2. provides mapping from object model of business layer to relational model of database |
| Business Logic Layer | Provides abstractions of entities  Enforces business rules for carrying out actions |
| The Hibernate | object-relational mapping system is widely used |
| Entity Data Model | developed by Microsoft |
| Web Services | Allow data on Web to be accessed using remote procedure call mechanism |
| Representation State Transfer (REST) | allows use of standard HTTP request to a URL to execute a request and return data |
| Big Web Services | uses XML representation for sending request data, as well as for returning results |
| Disconnected Operations | **Tools for applications to use the Web when connected, but operate locally when disconnected from the Web** |
| rapid application development (RAD) | tools even before advent of Web |
| Single sign-on | allows user to be authenticated once, and applications can communicate with authentication service to verify user’s identity without repeatedly entering passwords |
| Security Assertion Markup Language | (SAML)standard for exchanging authentication and authorization information across security domains |
| OpenID | standard allows sharing of authentication across organizations |
| Audit Trails | Applications must log actions to an audit trail, to detect who carried out an update, or accessed some sensitive data |
| Symmetric-key encryption | same key used for encryption and for decryption |
| *Data Encryption Standard* (DES) | substitutes characters and rearranges their order on the basis of an encryption key which is provided to authorized users via a secure mechanism |
| Advanced Encryption Standard (AES) | is a new standard replacing DES, and is based on the Rijndael algorithm, but is also dependent on shared secret keys |
| Public-key encryption | each user having two keys: *public and private key* |
| public key | publicly published key used to encrypt data, but cannot be used to decrypt data |
| *private key* | known only to individual user, and used to decrypt data.Need not be transmitted to the site doing encryption |
| Hybrid schemes | combining public key and private key encryption for efficient encryption of large amounts of data |
| salt bits | extra bits |
| Password based authentication | is widely used, but is susceptible to sniffing on a network. |
| Challenge-response | systems avoid transmission of passwords |
| Digital signatures | are used to verify authenticity of data |
| Digital signatures also help ensure nonrepudiation: | Sender cannot later claim to have not created the data |