Commerce and E-Business

# MODULE 2 : OVERVIEW OF H/W & S/W TECHNOLOGIES FOR E-COMMERCE

## 2.1:CLIENT SIDE PROGRAMMING(DREAM WEAVER,FRONT PAGE):

CLIENT SIDE SCRIPTING:Client-side scripting generally refers to the class of computer programs on the web that are executed client-side, by the user's web browser, instead of server-side (on the web server).This type of computer programming is an important part of the Dynamic HTML (DHTML) concept, enabling web pages to be scripted; that is, to have different and changing content depending on user input, environmental conditions (such as the time of day), or other variables.Client-side scripts are often embedded within an HTML or XHTML document (hence known as an "embedded script"), but they may also be contained in a separate file, to which the document (or documents) that use it make reference (hence known as an "external script").

## 2.2:SERVER SIDE PROGRAMMING:

Server-side scripting is distinguished from client-side scripting where embedded scripts, such as JavaScript, are run client-side in a web browser, but both techniques are often used together.Server-side scripting is often used to provide a customized interface for the user.These scripts may assemble client characteristics for use in customizing the response based on those characteristics, the user's requirements, access rights, etc.Server-side scripting also enables the website owner to hide the source code that generates the interface, whereas with client-side scripting, the user has access to all the code received by the client.A down-side to the use of server-side scripting is that the client needs to make further requests over the network to the server in order to show new information to the user via the web browser.

## 2.3:DATABASE CONNECTIVITY:

The information in these files may be broken down into records, each of which consists of one or more fields.Fields are the basic units of data storage, and each field typically contains information pertaining to one aspect or attribute of the entity described by the database.

## 2.4:SESSION TRACKING:

HTTP is a "stateless" protocol which means each time a client retrieves a Web page, the client opens a separate connection to the Web server and the server automatically does not keep any record of previous client request.Still there are following three ways to maintain session between web client and web server:Cookies:A webserver can assign a unique session ID as a cookie to each web client and for subsequent requests from the client they can be recognized using the recieved cookie.This may not be an effective way because many time browser does not support a cookie, so I would not recommend to use this procedure to maintain the sessions.Hidden Form Fields:A web server can send a hidden HTML form field along with a unique session ID as follows:This entry means that, when the form is submitted, the specified name and value are automatically included in the GET or POST data.

## 2.5:MIDDLEWARE TECHNOLOGIES FROM E\_COMMERCE PERSPECTIVE

Middleware binds discrete applications, such as Web-based applications and older mainframe-based systems, to allowcompanies to hook up with latest systems anddevelopments that drive new applications without making their in-vestments in legacy systems unyieldingMiddleware functions are generally classified into:Application-specific functions to deliver services for different classes of applications such as distributed-database services, distributed-data/object-transaction processing, and specialized services for mobile computing and multimedia.Information-exchange functions to manage the flow of information across a network—for tasks like transferring data, issuing commands, receiving responses, checking status, and resolving standoffs.Management and support functions to locate resources, communicate with servers, handle security and failures, and monitor performance.The selection of middleware technology is determined by what information is required to be communicated, for example, database middleware will be the choice if database is the main requirement.However, following are the major categories of middleware:Database Middleware,Remote Procedure Calls (RPC)Object Request Broker (ORB),Application Server Middleware,Message Oriented Middleware (MOM),Transaction Processing Monitor (TP),The most widely used, easy to install, and relatively economical middleware, Database middleware,is usually chosen to complement other types of middleware and facilitates communication among applications and local or remote databases but cannot transfer calls or objects.However,database middleware does not allow the two-way communications between servers and clients.SQL type command is generally subjected to the middleware gateway, which would convey the command to the end database to collect and send the reply of the SQL query back.Synchronous point-to-point type of communications is the characteristic of database middleware and can pose problems when multiple demands from multiple users produce huge traffic and congestion.Database middleware is the most mature middleware technology.Remote Procedure Calls (RPC) permits a client program to call procedures located on a remote server program.Remote procedure calls is not isolated as distinct middleware level and is entrenchedinto the application with calls embedded into the client portion of the client/server application program.Stubs are developed for both the client and the server to call up synchronously when the client makes a call to the server.The intricacies of distributed processing are reduced by remote procedure calls by maintaining the semantics of a remote call no matter the client and server are located on the same system or not.The synchronous nature of the remote procedurecalls makes it most appropriate for smaller applications where all communications are one-to-one and not asynchronous.Object Request Brokers (ORB) are language-independent, object-oriented, synchronous remoteprocedure calls in which an affiliate function of an object can be brought into play remotely by means of the same essential notation.Asynchronous communication suitble to large applications can be made possible by extending the main standards as in CORBA and DCOM, the main competing standards.ORB technologies are based on the reliability of the transport layer, which is required for the functioning.The application programmer is secured from the details of the client/server approach by using IDL interfaces that allows the application code to call a remote object,as if it were locally supported.Thus, the maintainability is improved as the object communication details are concealed from the application and isolated on the ORB.Hence, ORB-based middleware applications are becoming standard for the multi-tier model.Message Oriented Middleware (MOM) or enterprise message technology (EMT), provides asynchronous message delivery.The messages are lined up, just as objects, permitting the application that sends messages, to carry out other tasks without getting blocked till it receives the response.Generally located at a higher level than that of remote procedure calls, MOM assembly provides Middleware Components for E-commerce Infrastructure more than simply passing information.

## 2.6 SECURITY ASPECTS w.r.t E-COMMERCE:

A wide variety of commerce is conducted via e‐commerce, including electronic funds transfer, supply chain management, online transaction processing, electronic data interchange (EDI) and automated data collection systems.Any secure e‐commerce system must meet four integral requirements:privacy – information exchanged must be kept from unauthorized parties, o integrity – the exchanged information must not be altered or tampered with,authentication – both sender and recipient must prove their identities to each other andnon‐repudiation – proof is required that the exchanged information was indeed received.Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for eCommerce providersPrivacy now forms an integral part of any e-commerce strategy and investment in privacy protection has been shown to increase consumer‘s spend, trustworthiness and loyalty.We can see that privacy is of major concern to users and in the event of their privacy being compromised users become very agitated and there is an overall negative effect on trust in e-commerce.In any e-commence system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business.Data integrity is the assurance that data transmitted is consistent and correct, that is,it has not been tampered or altered in any way during transmission.Authentication is a means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place.Proof of data integrity is typically the easiest of these factors to successfully accomplish.A data hash or checksum, such as MD5 or CRC, is usually sufficient to establish that the likelihood of data being undetectably changed is extremely lowNot withstanding these security measures, it is still possible to compromise data in transit through techniques such as phishing or manin-the-middle attacks .