CHAPTER – 4

METHODOLOGY
Main purpose of my research is to implement the setup of banking application in Middleware technology by using weblogic application server including the main feature of for banking application. Once the setup is completed, explain the security feature provided by weblogic application server because security is the major concern in banking sector. [12]

4.1 Objective

This chapter will explain the methodologies used, including the hardware, software, design and analysis and validation methodology.

Complete analysis that have been done previously to adopting the three tier architecture technology and what was the disadvantage and created a new testing environment through the middleware technology weblogic

Scalability: This is one of the key features in 3-tier or N-tier architecture, when we change the size or volume of running application to meet the user requirement without impacting is called Scalability. Like an example, I have an application that taking the load of 100 users. In futures 200 user or more will access the same application. Initially we have design the application according to 100 user but if the same application will be used by 200 user, it's quite obvious performance will be degrade. If we will have the 3-tier or N-tier architecture, we can scale our application in each area either infra wise or application wise.

Better Re-use: it’s also a feature of reusable, like suppose an application that are running with some configuration of system or computer like, same business logic we can use in after changing the configuration etc.. Suppose our application is running on JBOSS application server as it’s also java based application server, in future we don’t want this JBOSS application server then we can also use same application on any other java based application server.

Improved Data Integrity: In 3-tier or N-tier architecture all the communication happen through the middle tier because business logic is deployed on middle tier. All data into the database passed through the middle tier, its middle tier responsibility to update the database with valid data or remove the corrupting data.

Improved Security: Security is a measure concern for any application specially in banking system and it can be implement on different level as we cannot provide the direct access to the database to client or customer. For a client it's very difficult to get the unauthorized data. In 3-tier or N-tier architecture business logic is placed in center server and it should be more secure however business logic is already secure and deployed in center server. Oracle developed such kind of product that provide good security feature like Oracle Access manager.

Reduced Distribution: when we want to change or update the business logic then need not to do on all distributed to all the clients, it's required to change only in application where business logic is deployed.
Improved Availability: It’s also good advantage to improve availability in 3-tier. We can reduce the application server or database server as backup server so we can use those when the live or network system failure. Or we can share the load of application in different server in cluster. When we used the cluster architecture in 3-tier, in cluster architecture when one server will go down the load of application passed to another server available in cluster. [1][4][21]

Hidden Database Structure: However for a customer or caller the database structure becomes hidden, this is possibility or we can make changes in database with transparently. This is the reason while exchanging information and data with other application in middle tier can maintain its original interface however database was upgrading and enhancing during new release of application.

4.2 Clustering with high available and scalable mechanism

![Figure 3 (Basic setup for weblogic domain)](image)

As per above figure the admin server will control all the resources in the domain. Admin server contain all the configuration information about the cluster, in above figure there are three managed are in cluster and an Admin server. When the servers in cluster are running, there is no effect on admin server
with load-balancing and failover capabilities of the cluster. In live business environment, the administration server is not configured as part of a WebLogic cluster because it should be available for monitoring all other WebLogic instances and hence should not be overloaded with client requests. As per the above figure client will send the request through load balancer and it route to managed server according the load on different server, if one server will already handling the load then request will route to another weblogic instances. And through admin console we can control, manage and monitor all the servers in cluster therefore admin console is single point of control to all resources in weblogic domain and node manager should be there to control managed server like start and stop etc. As per admin view each WebLogic cluster is managed as a single logical entity in the domain. [36][2]

4.3 SSL Feature and implementation for better security

SSL (Secure Socket Layer) is a protocol used to transfer the data and information on internet in secure manner. Before discuss how the SSL technology work, First need to understand what happen without SSL.

Let I explain an example, suppose we have dialed a number over the phone to talk someone at first time. Question is how we are sure that when we dialed a number, right person will pick up the call? What will happen if the call is routed and someone else is giving the answer of your dialed call? There is no way to identify. Nowadays we are seeing the phone calls are easily tapping, so it’s a very big problem. Same happen while transferring the data and information over the internet, not sure either our communication is tapped or not.

How we can sure that, we are reaching with right server and the data which we are transferring is safe, especially in banking sides, with SSL we can sure that communication is going in safe mode.

4.4 Example, how SSL technology work

SSL technology works on the concept of “public key cryptography” to achieve these tasks. In simple encryption, sender and receiver communicating share a “password” and this password used to encrypt and decrypt the message.

In “public key cryptography”, there are two key (public and private) with sender and receiver. Anything encrypted with the user’s public key can only be decrypted with the private key and vice versa. Each person then tells the world what his public key is and keeps his private key safe and secure, and private.

Suppose a banking company wants a secure communication to their server banking.co.in, for it they will create a SSL certification or we can say will create a public and private key for server banking.co.in.

For it then need to go with third party like Thawte or Verisign etc and these companies provide its identity that is specific for only a company approved and give the right to company to use banking.co.in domain. For this complete process, like getting the certificate etc., we have to pay and need to do some paper work also.
Once verification will done, third party will provide a new public key that will have some additional information in it. This information is the certification from third party that this public key is for the company and banking.co.in and that this is verified by Thawte. This certification information is encrypted using Third part’s private key.

Now when we want to reach or send any information or we can say communication with banking.co.in, need to create a connection to banking.co.in with our system. Once connection will establish it will create a special port or address on banking.co.in and that is only for secure communication. When we want to connect with banking.co.in with its secure port then company provide us its public key and other information if it will correct otherwise it will rejected.

Client gets the public key and confirms if it is ok, otherwise

There would be a problem if the public key is expired.

Public key claims to be for some domain that is not banking.co.in that could be a problem.

We have a public key for third part, stored in its system because these come with the system. Thus, we can decrypt the validation information, prove the validation is from third party and verify that the public key is certified by third party. If we trusts third party, then we can trust that he/she is really communicating with Company. If we don’t trust third party, or whatever Third Party company is actually being used, then the identity of who is running the computers to which Client is connecting is suspect.

Here is the basic diagram for communicating with SSL concept.

**SSL Basic diagram for communicating**

![SSL Basic Diagram from communicating](image)

Communication will terminate if the client does not trust the server.
If there will be own certificate with client, it will send that certificate to the server and here to see if the server trusts the client. There is no Client-side SSL certificates are commonly used, but give a procedure like without asking username or password client to authenticate itself with the server. Here in scenario, server needs to verify the client certificate also in same way to how client verified the server. Connection terminated if this condition is not satisfied and this step will be skipped if the client side certificate is not needed.

After satisfaction of client with the server, Server provide a list of encryption methods and client chooses an SSL Cipher from that list and create a password for use with that Cipher. By using the server’s public key, client encrypts this password and sends it back to the server. Sever set this password after decrypting this message, now both client and server share it.

With this password and chosen Cipher, client encrypts all data or information and will start communication with company. Normal “symmetric” (password-based) encryption takes place from this point forward because it is much faster than using the public and private keys for everything. To prove its identity and right to domain.co.in, these keys need to enable and to create securely communicate a common password by enabling both client and server.

One Way SSL

Internet banking site is one of the best example of one way SSL authentication. When we open these types of sites it’s generally popup a warning. This popup shows us to certificate and these certificates are the authentication of the applications which we are going to access. If there is a lock sign at the right bottom corner of the status bar of the browser then double click on it get the details about the certificates. The certificates have expiry date and issuing authority details, which will confirm you the identification of the application. Means, the application which we are going to connect is SSL server and the browser which will connect to the application is a SSL client. SSL client initiates a contact with a SSL server. A certificate with signed is presented by SSL server to SSL client. SSL client verifies the identity of the server with the private key of the server stored in it (client) and the authentication is complete.

Figure 5 (One way SSL)

Two way SSL
As the name indicates two way SSL, means authentication happens from both sites. Means client authenticate to server and server also authenticate to client also, here in both server and client, certificates are present and client application verifies the identity of server application and server application also verifies the identity of the client application.

As I have discussed, here not only the server authenticates to the client, also client authenticates itself to the server, that’s why two way SSL is also referred to as client authentication.

Example of two way SSL would be applications which deals with sensitive and confidential data which is intended for a particular recipients. Thus the client who is having the certificates to authenticate itself to the server will only be able to access the application.

In the two way SSL applications, SSL client initiates a connection to a SSL server and server is set to use two way SSL client authentication. The SSL server presents its certificate [which is a public key of the server] to the client for verification. The SSL client verifies it with the private key store of the server. Then SSL server requests SSL client to send its public key to the SSL server to verify with the private key of the SSL client stored in the SSL server.

![Figure 6 (Two way SSL)](image)

4.5 SSL cycle
While internet banking, security is the major concern. While doing transaction our information should be secure and safe that means information should be transferred securely. There are various methods in internet banking to secure the data; one of them is monitor the integrity and security of the system.

Security of internet banking application is noted at different level. First concern is security of customer information because it’s sent from his PC to browser. Second is the security of the environment in which customer information resides in database and internet banking server. At last security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web site.

![Figure 7 (SSL Cycle)](image)

Basically SSL (Secure Sockets Layer) control the data security between the customer browser and Webserver. SSL provides server authentication, data encryption and message integrity for an Internet connection. Apart from that SSL provides a security mechanism called handshake is used to establish the connection, once successfully handshake will done then client and server agreeing on the level of security they will use and fulfill authentication requirements for the connection. And it’s depending on browser how much level of encryption is there like 128 bit or higher.

After that the request passed from web browser to internet banking server. And this internet banking server is designed by three tier architecture and all the things like application server and application is deployed in application server however multi tier architecture provides a double firewall, completely isolating the Web server from the customer information SQL database.

Internet banking server send the information to database and all login attempts constantly taken care by security analyzer and when it find number of failure and those failures will say unauthorized attempt to log into an account. When this kind of unauthorized attempt found automatically a step will be taken to safe that account from being used.
In every area, security concern is noted in Internet banking application architecture. It's ensures from customer that authenticated data will come at his end when there will be a implementation of the SSL security protocol on the Web server and his browser. A double firewall is created when we use the banking application in three-tiered architecture mode and over the dedicated network that is designed for specific function, it performs the information request. It create a well-controlled or managed environment which allow quick incorporation of Internet security as evolve when all business logic will be in placed in internet banking server.. At the end I want to say, prevention of unauthorized logins during login attempts is taken care by security analyzer.

4.6 Software’s and configuration use for testing

Below software’s and mechanism I have used for complete setup

1. Installation of Weblogic.
2. Weblogic Domain Creation.
3. Database Installation.
4. Manager server configuration in weblogic Domain.
5. Nodemanager configuration.
6. Developing test application.
7. Deployment of test application in single server.
8. Deployment of test application in clustering and also test the failover concept.
9. Database user creation, permission granting and table creation for my testing application.
10. Apache server installation.
11. Security implementation

4.6.1 Version of the Software’s

Database
Oracle 11.2.0.2: Database is the main important part of any business environment. It’s used to the Physical data of any organization. I have used oracle database version 11.2.0.2.

OHS (HTTP) Server

Oracle OHS server: It’s an oracle web server just like attaché http server

Application Server

Oracle Weblogic Server 11G: Weblogic server is the Java J2EE based application servers.
Development Application

Application is created in J2EE and deployed in application server.

During my testing I have used Standard X86 Oracle Linux servers because they are globally used by all of the organizations in the market as well as fully certified by the Oracle itself for any FMW set up with weblogic and for other component also.

4.6.2 Testing Environment setup block Diagram

![Diagram](image-url)

**Figure 8 (Testing Environment setup)**

Install weblogic, database OHS http server and created an application as per the above mentioned version.

After installing the weblogic in both machines (machine 1 and machine 2), create a weblogic domain only with admin server in first machine then copy complete weblogic domain to machine 2, for it below steps are executed.

1] Created a tar file in machine 1 with complete domain

2] Then transfer the tar file to machine 2

3] Then untar the tar file in machine 2

Once domain is created, started admin server from machine 1. Once the admin server is up, through console I have added managed server, cluster and deploy the application. As per my testing there are
two managed and Admin server are in machine 1 and two managed server are there in machine 2 and node manager is also configured on both machine, we can control all managed server through the admin console.

Install the database and created necessary user, schema and give the privileges as per requirement and finally created the table also. Then finally deployed a banking application on application server and access the application in different scenario and validate all the things through logs and from DB.

4.6.3 Testing with Apache Webserver

![Figure 9 (Apache with weblogic)](image)

Here client accessing the request with browser to apache Webserver, then through the apache server request will route to managed server according to load. As both server managed server 1 and 2 are in cluster then equal load will be there and it’s improve the performance of application.

For this we need to add the entry of managed server in apache configuration file httpd.conf, like below:

```xml
<Location />
  SetHandler weblogic-handler
</Location>

<IfModule mod_weblogic.c>
  WebLogicCluster localhost:7010,localhost:7011
</IfModule>

WebLogicCluster localhost:7010,localhost:7011
Debug ON

WLLogFile d:/temp/wlproxy.log

WLTempDir d:/temp

</IfModule>

So load balancing can improve the performance of the system.