Implementation of Security Mechanism

# Overview

This is one of the most important modules of any project. This is that part of the project which handles the data security of the system. Data security is very important to prevent unauthorized users from viewing confidential data’s. Now day’s companies spend a lot of earning to maintain a perfect security system so that no one can hack in to the system.

When ever we talk of security the most important thing which is to be discussed are access rights. This refers to which system user is granted with what kind rights to the system. This can also refer to setting the working boundaries for a user. This is maintained by providing a login module to the system. Users log in by entering a valid login ID and password. This decides the rights for the user. During login security checking is performed.

# Security Implies

* Physically limit access to computers to only those who will not compromise security
* Hardware mechanisms that impose rules on computer programs, thus avoiding depending on computer programs for computer security.
* Operating system mechanisms that impose rules on programs to avoid trusting computer programs.

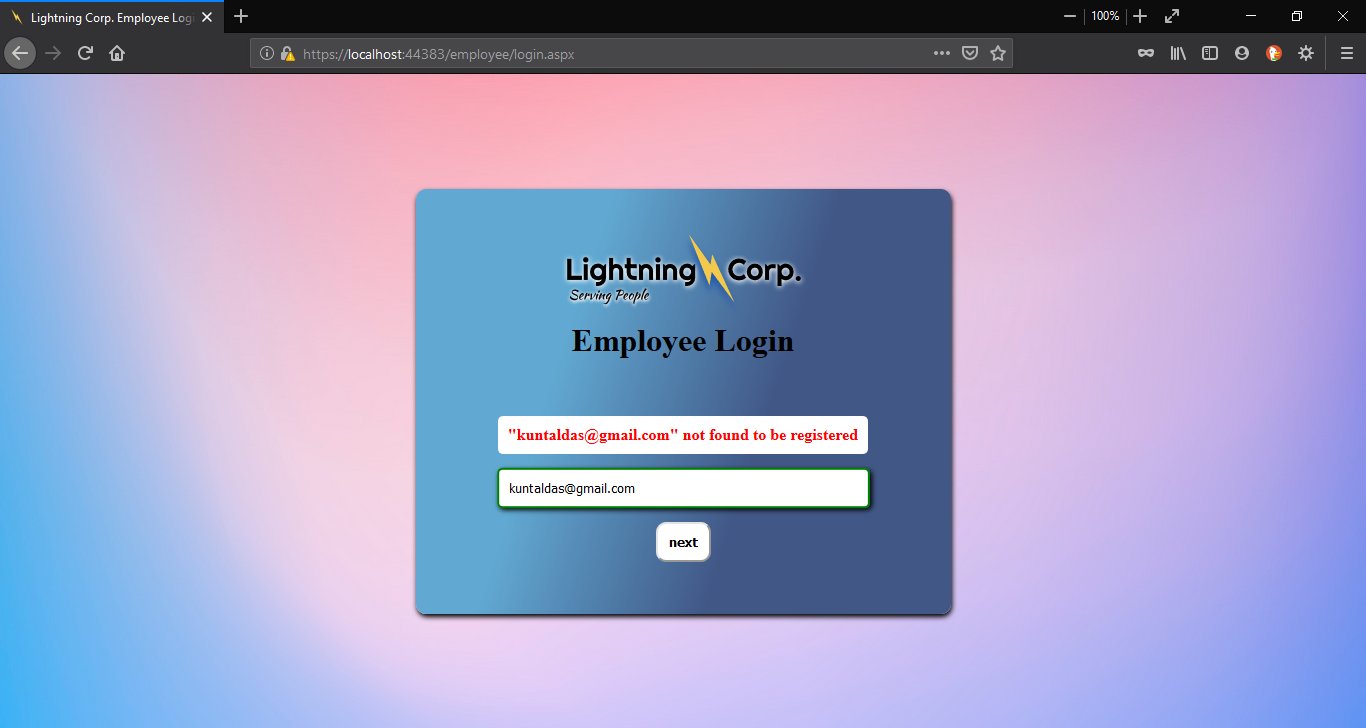
There are Two types of security are implemented in this system.One is **Application security** and another is **Database security.**

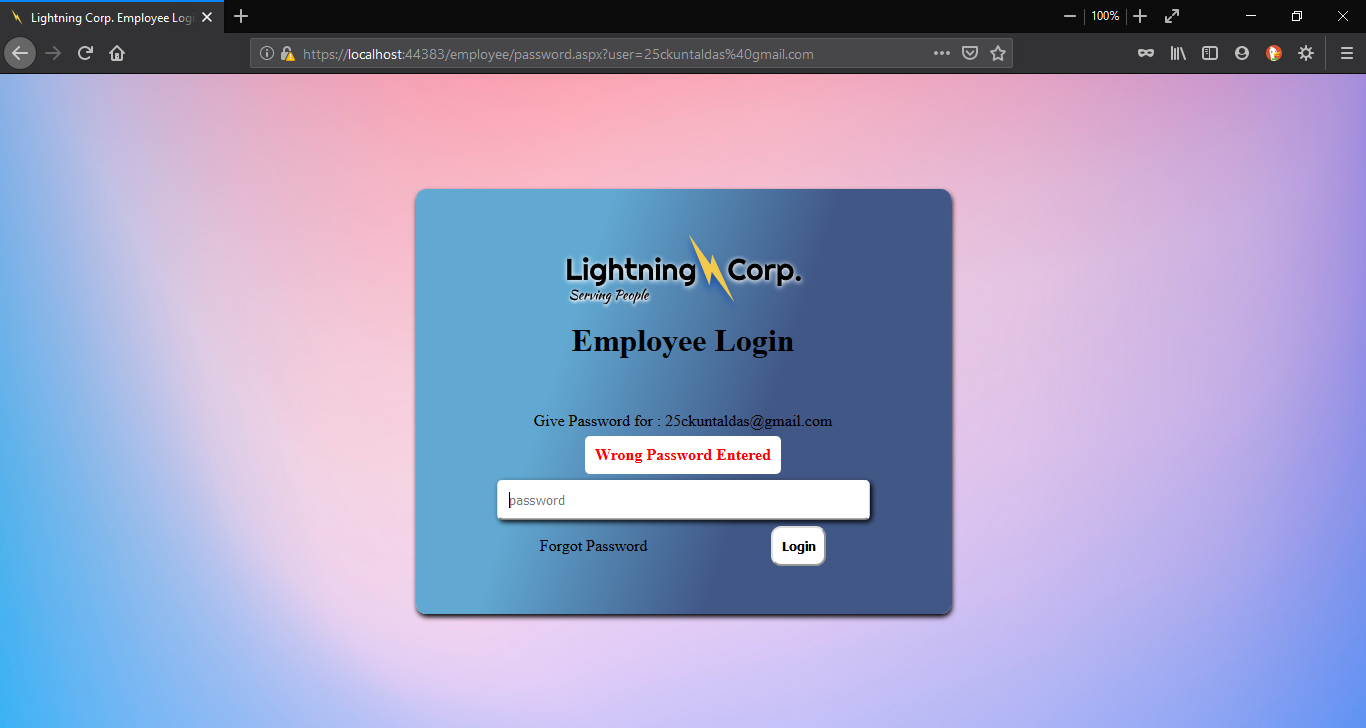
1. **Application Security**

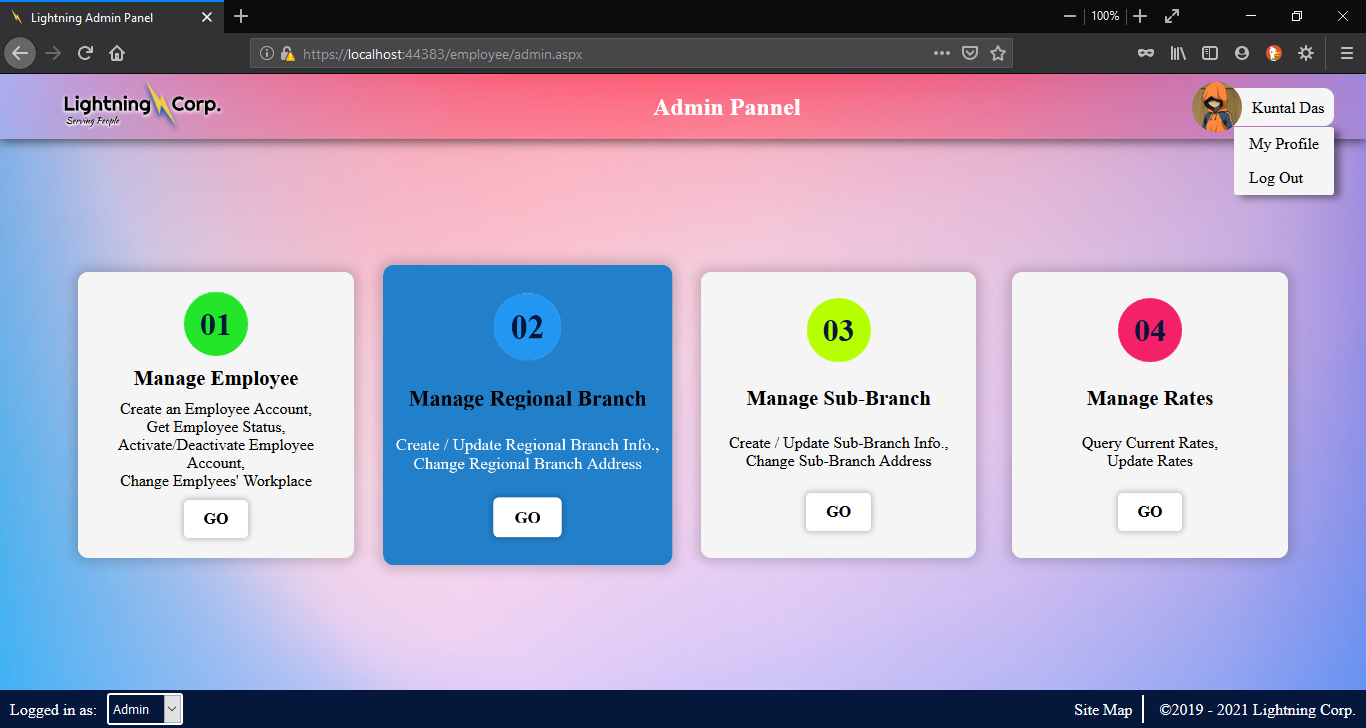
**There are five types users who can access the system:**

* Administrator
* Manager
* General Employee(Customer Support, Delivery Person, Cashier, IT)
* Registered Customer
* Anonymous Customer

**Administrator** can access the whole system. The **Administrator Home Page** is accessed by only Administrator by providing correct email/phno. and password. **Administrator** can also create, activate, deactivate any Employee account.







**Manager** can access the **Manager** and **General Employee** **Page** providing correct email/phno. and password. **Manager** can also create, activate, deactivate any Employee account.

In password.aspx it is desided wheather the user should be logedin as **Admin** or a **General Employee**

This piece of code does that by using IsAdmin() function in Employee Class

protected void logIn(object sender, EventArgs e)

{

try

{

emp = new Employee(Convert.ToInt64(euser));

}

catch (FormatException)

{

emp = new Employee(euser);

}

epass = Apass.Text.Trim();

emp.Filldata();

this.id = emp.CheckPassword(epass);

if (id >= 1000)

{

if (emp.IsAdmin())

{

Session["LightAdm"] = id.ToString();

Response.Redirect("~/employee/admin.aspx");

}

else

{

Session["LightEmp"] = id.ToString();

Response.Redirect("~/employee/emp.aspx");

}

}

else

{

status.Text = "Wrong Password Entered";

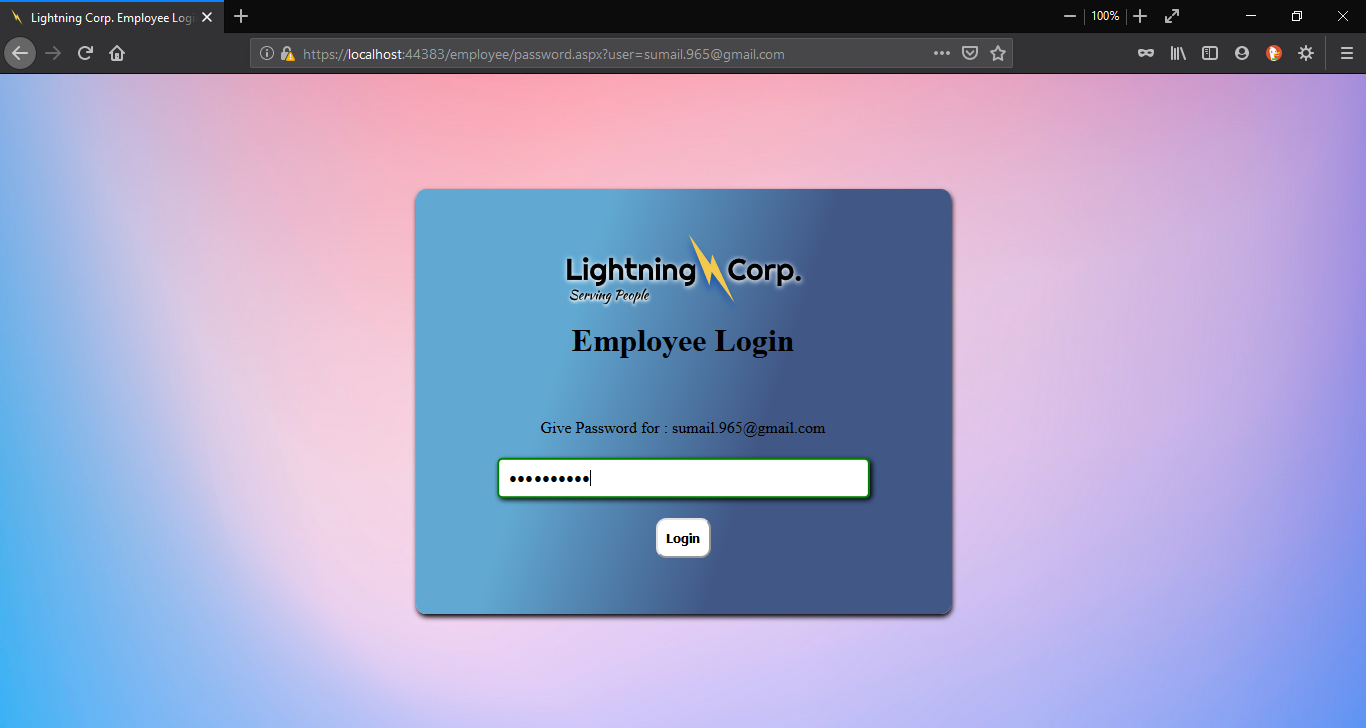
status.Visible = true;

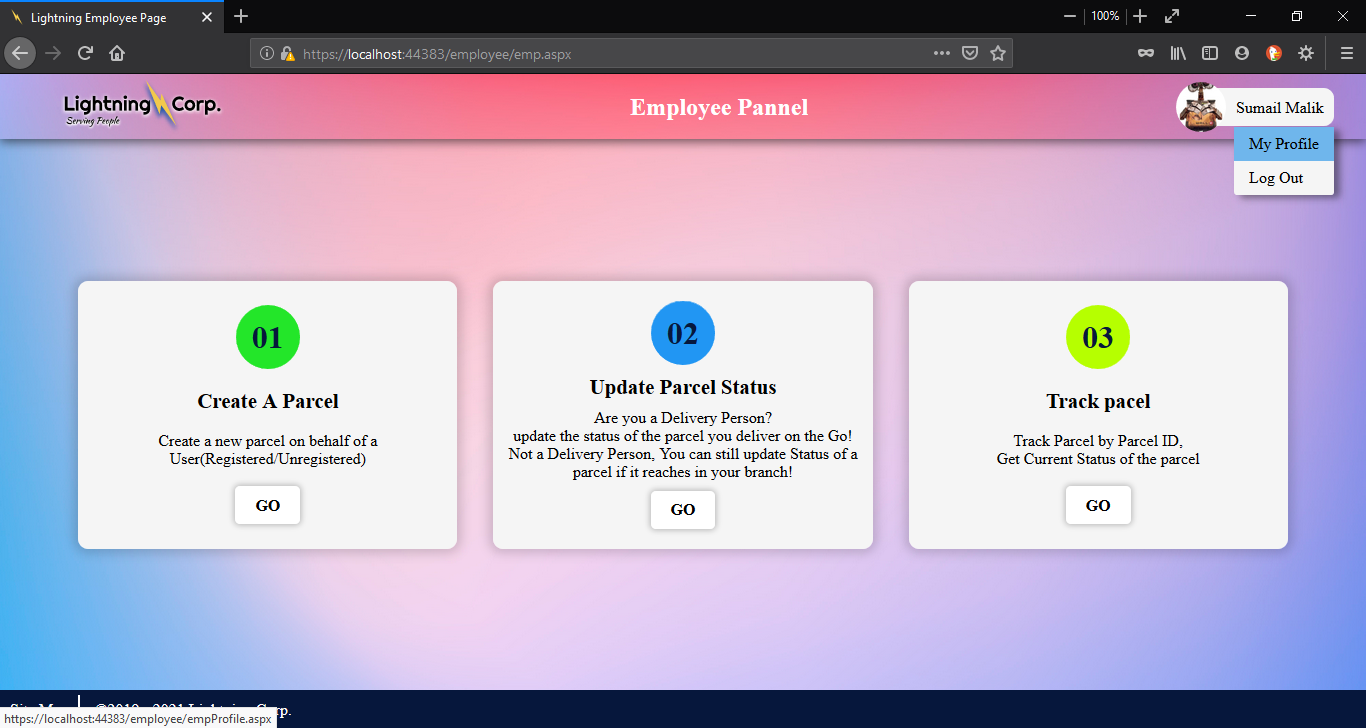
forgotPass.Visible = true;

}

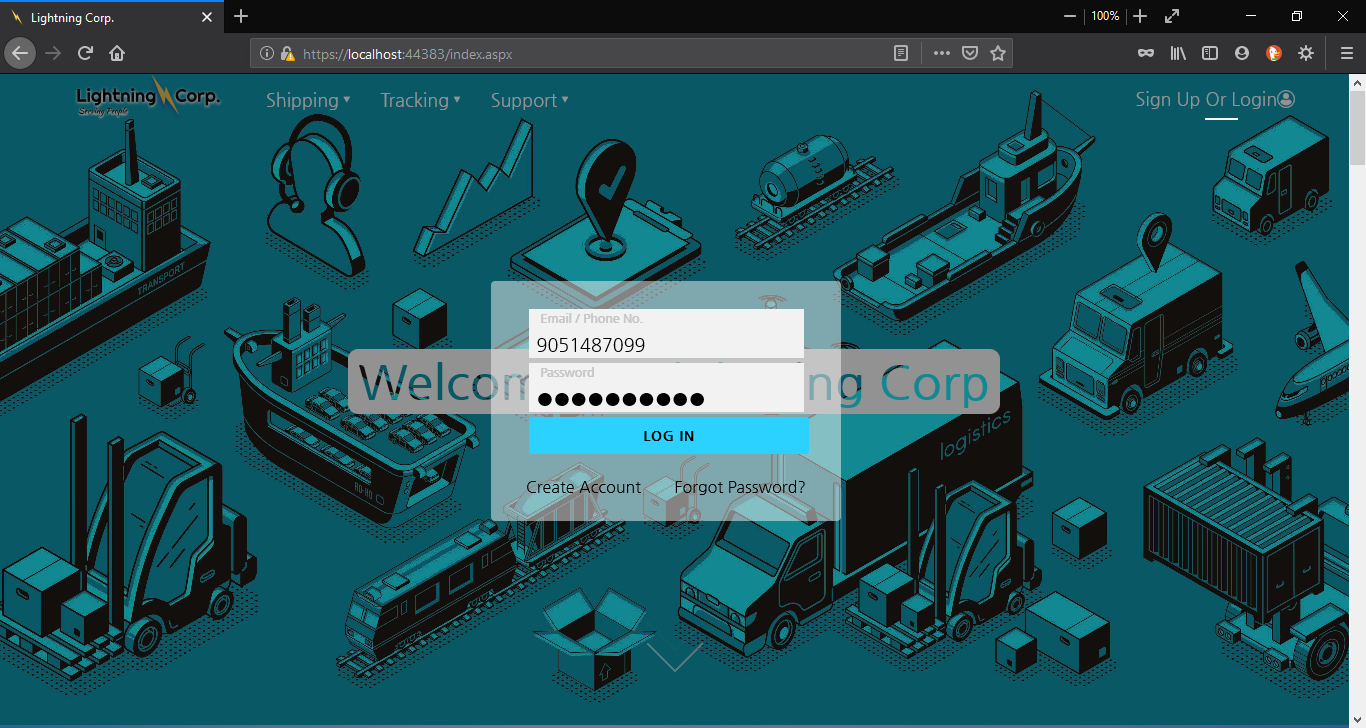
}

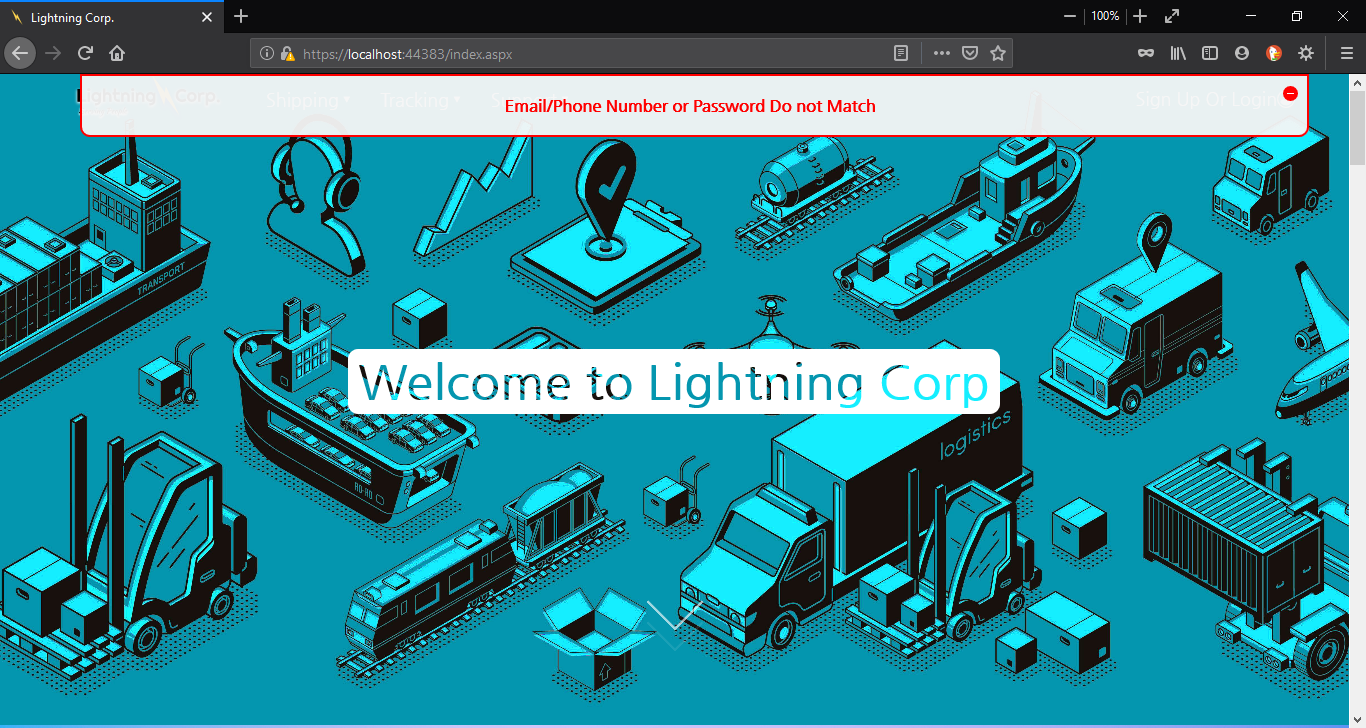
**General Employee** can access the **General Employee Home Page** by providing their email/phno. and pasword.





**Registered Customer** can access all customer Pages by logging in with their email/phno. and password.







**Anonymous Customer** can access only some specified pages like, Rate of transport, Create parcel, Track Parcel.

1. **Database Security**

# Overview

Database is the storage device. That means the data is getting stored in the database server. Thus it is very important to secure the data residing in the database. Thus every database server provides a login procedure. This technique is similar to application level security. The entity which is willing to use the database has to supply in a login ID and password to access and manipulate the data in the database. Every database server provides a default login ID and password to access the data. Apart from this the database administrator can also create other database user.

In this project the User defined login ID and password has been used. Since the database server used in this project the connection string used for connecting to database through C# code is:

Data Source=DESKTOP-74RBQ7M\KUNTALSQLS;Initial Catalog=CourierService;Persist Security Info=True;User ID=sa;Password=\*\*\*\*\*\*\*\*\*\*\*

# Database Connectivity:

In Database Connectivity I have used **4-tier architecture** to fetch data form DataBase



In **Presentation Tier** ASP.NET Web Forms, Web Forms with Master Page etc. is used .Here User interraction happens and output data is shown.

In **Business Tier** all the business logic is defined as C# code in C# class file. It takes input fom Presentaon Tire and forwards the input to next Tire(Data Tire), and the output received from Data Tire is sent back to Presentaon Tire.

In **Data Tire** SQL SERVER Stored Procedures are executed to get desired output, these Stored Procedures are saved inside the DataBase. Business Tire calls Stored Procedures in Data Tire and the procedured executes DataBase Queries necessary and sends the necessary output to Business Tire.

In last Tire Data is Saved in Table format in Varous Databases in the Database Engine(in this case SQ L SERVER) .In these tables Insert, Update and Delete is done by Stored Procedures.

**Example :** In the example below index.aspx.cs Web Form calls function **GetCIDbyPass(string password)** and if password matches Customer ID is returned which is then used to login and saved in session else null is sent and Login Fails.

Index.aspx.cs(**Presentation Tier**)

. . .

. . .

protected void Blogin\_Click(object sender, EventArgs e){

if (Page.IsValid){

string CID = null;

Customer Cus;

try{

Cus = new Customer(Convert.ToInt64(TBunm.Text.Trim()));

}catch (FormatException){

Cus = new Customer(TBunm.Text.Trim());

}

CID = Cus.GetCIDbyPass(TBpas.Text.Trim());

if (CID == null){

Notifyuser("Email/Phone Number or Password Do not Match", false);

return;

}

Session["LightCus"] = CID;

Response.Redirect("~/index.aspx");

}else{

Notifyuser("Validation Error, Data Not Saved", false);

}

}

. . .

. . .

**GetCIDbyPass** calls Stored Procedure **GetCIDbyPass** and passes email and/or phone no. with password . The stored Procedure then returns Customer ID if matching email/phno no and password else returns 0;

Customer.cs(**Business Tier**)

. . .

string connectionstr=”Data Source=DESKTOP-74RBQ7M\KUNTALSQLS;Initial Catalog=CourierService;Persist Security Info=True;User ID=sa;Password=\*\*\*\*\*\*\*\*\*\*\*”

. . .

public string GetCIDbyPass(string pass){

this.cid = null;

pass = Password.HashPassword(pass);

using (SqlConnection con = new SqlConnection(connectionstr)){

try{

con.Open();

SqlCommand cmd = new SqlCommand("GetCIDbyPass", con);

cmd.CommandType = CommandType.StoredProcedure;

if (this.email != null){

cmd.Parameters.AddWithValue("@PHNO", null);

cmd.Parameters.AddWithValue("@EMAIL", this.email);

cmd.Parameters.AddWithValue("@PASS", pass);

}else if (this.phno != -1){

cmd.Parameters.AddWithValue("@PHNO", this.phno);

cmd.Parameters.AddWithValue("@EMAIL", null);

cmd.Parameters.AddWithValue("@PASS", pass);

}else{

cmd.Parameters.AddWithValue("@PHNO", this.phno);

cmd.Parameters.AddWithValue("@EMAIL", this.email);

cmd.Parameters.AddWithValue("@PASS", pass);

}

this.cid = cmd.ExecuteScalar().ToString();

return this.cid;

}catch (SqlException){return this.cid;}

catch (Exception){return this.cid;}

finally{con.Close();}

}

}

. . .

. . .

Stored Procedure **GetCIDbyPass** execues select Query in DataBase table(Cpass and Customer) if found VARCHAR(14) CID is sent back else NULL is sent back to the function.

dbo.GetCIDbyPass(**Data Tire**)

USE [CourierService]

GO

SET ANSI\_NULLS ON

GO

SET QUOTED\_IDENTIFIER ON

GO

-- =============================================

-- Author: Kuntal Das

-- Create date: 07/09/2019

-- Description:

-- =============================================

ALTER PROCEDURE [dbo].[GetCIDbyPass]

@PHNO NUMERIC(15,0) = NULL,

@EMAIL NVARCHAR(100) = NULL,

@PASS NVARCHAR(MAX)

AS

BEGIN

SET NOCOUNT ON;

IF(@PHNO IS NOT NULL AND @EMAIL IS NOT NULL)

BEGIN

SELECT CU.CID

FROM Customer CU JOIN Cpass CP ON CU.CID=CP.CID

WHERE Phno=@PHNO AND Email=@EMAIL AND CP.password=@PASS;

END

ELSE IF(@PHNO IS NOT NULL)

BEGIN

SELECT CU.CID

FROM Customer CU JOIN Cpass CP ON CU.CID=CP.CID

WHERE Phno=@PHNO AND CP.password=@PASS;

END

ELSE IF(@EMAIL IS NOT NULL)

BEGIN

SELECT CU.CID

FROM Customer CU JOIN Cpass CP ON CU.CID=CP.CID

WHERE Email=@EMAIL AND CP.password=@PASS;

END

END

dbo.Cpass & dbo.Customer (**Data**)

