ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Secure Login Using Encrypted Password and Email Based Login Approach

[I]V.Balalojanan, [II]T. Jeyaperatha, [III]K.Thiruthanigesan, [IV]N.Thiruchchelvan
[I]University of Vocational Technology Ratmalana, Sri Lanka
[II]College of Technology, Jaffna, Sri Lanka.
[III]University College of Jaffna, University of Vocational Technology, Sri Lanka.
[IV]University College of Anuradhapura, University of Vocational Technology, Sri Lanka.

Abstract
In the software development progress login page most important module it is a security module for the internal whole system offline based application most of them are used dynamic and static passwords. In that they follow several technologies to secure their developed systems. Such as password encryption methods, session password and bio matric technics. Our proposed system is enhance the security level of the developed system by using the encrypted password and email based login approach.

Keywords
Secure login, email based Login, Encrypted password.

I. Introduction

The secure login system is software for detecting and preventing unauthorized access to user account. Providing highly security for the developed software modules. In this research paper, we were designed the following algorithm and developed login module which can be used for implementing the account locking system and password recovery by using the emails. In this research paper we were propose a login module it can be used as login module for any developed software such as student, hotel, super market management system or any other administrative maintenance systems. Our research is based on the secure account login system using C#.Net [1] and Microsoft SQL Server. Figure 1, simply represented the design of the system.

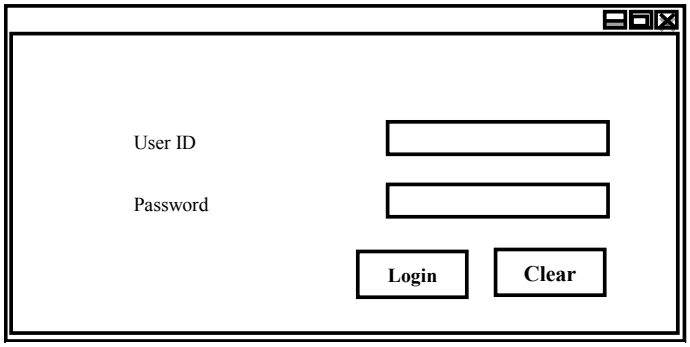

Fig. 1: Sample Login Form

Algorithm

Step 1: Check the given ID entered by the user is available in the data base or not. If it is available Then go to step2 otherwise go to step 7
Step 2: Take the suitable password (decrypted) from the database which is equivalent to Entered user name, then go to step 3 otherwise go to step 7
Step 3: Set the count variable as count = count +1, then go to step 4
Step 4: If the count is equal to one success fully login the main module otherwise go to step 5 and 6
Step 5: Count is greater than 1 duplicate user name available in the database
Step 6: Count is less than 1 user go to step 7
Step 7: Display the message ID is not available
Step 8: If the user forget the password then go to forget password module
Step 9: Get email ID as input then send the auto generated verification code to email address

II. Material and Methods

The proposed system is providing the highly secure login module for the developed systems. We have proposed an idea to enhancing the performance of the Login module to provide Authentication for the developed system. This system as the first stage during the user account creation save the password as the encrypted format in the database by using following encryption mechanism [2,3]

Code for password encryption:

```
class Password   {
      const char fillchar = '*';
      static string cvt =
      static string cvt = "
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz0123456789+/";
      public static string encrypt(string data) {
         int i;
         int c;
         int len = data.Length;
         string ret = "";

         for (i = 0; i < len; ++i)    {
           c = (data[i] >> 2) & 0x3f;
           ret += cvt[c];
           c = (data[i] << 4) & 0x3f;
           if (++i < len)
              c |= (data[i] >> 4) & 0x0f;
           ret += cvt[c];
           if (i < len)              {
              c = (data[i] << 2) & 0x3f;
              if (++i < len)
                 c |= (data[i] >> 6) & 0x03;
              ret += cvt[c];      }
           else      {
              ++i;
              ret += fillchar;   }

           if (i < len)  {
```

```
            c = data[i] & 0x3f;
            ret += cvt[c];    }
         else     {
            ret += fillchar;    }
      }

      return (ret);
   }
```

The proposed system during the login time retrieves the password from the database as decrypted format by using following decryption mechanism

Code for password decryption:

```
   public static string decrypt(string data)        {
      string ret = "";
      int i;
      char c;
      char c1;
      int len = data.Length;

      for (i = 0; i < len; ++i)            {
         c = (char)cvt.IndexOf(data[i]);
         ++i;
         c1 = (char)cvt.IndexOf(data[i]);
         c = ((char)((c << 2) | ((c1 >> 4) & 0x3)));
         ret += c;
         if (++i < len)                {
            c = data[i];
            if (fillchar == c)
               break;
            c = (char)cvt.IndexOf(c);
            c1 = (char)(((c1 << 4) & 0xf0) | ((c >> 2) & 0xf));
            ret += c1;    }

         if (++i < len)   {
            c1 = data[i];
            if (fillchar == c1)
               break;
            c1 = (char)cvt.IndexOf(c1);
            c = (char)(((c << 6) & 0xc0) | c1);
            ret += c;
         }   }
      return (ret); } }
```

The developed system during the login time convert the given password as encrypted format with the same encrypted mechanism and retrieve the password from the database with the decrypted mechanism Finally check whether the given password is matching with the database if is it matching user can able to access the software.

Code for Login Button:

```
private void button2_Click(object sender, EventArgs e){
//ramdom number generate
string code;
int min = 000001, max = 999999999;
Random r = new Random();
code = r.Next(min, max).ToString();
txtcode.Text = code;

if (txtid.Text == ""){
MessageBox.Show("Enter the Userid");}
else if (txtpassword.Text == ""){
MessageBox.Show("Enter the Password");}
else{
//defoult user
if (txtid.Text == "1" && txtpassword.Text == "1"){
this.Hide();
Main f = new Main(textBox1.Text, txtid.Text, txtcode.Text);
f.Show();}
else{
sqlc.Connection1();
SqlCommand c = new SqlCommand("Select User_ID from user_
details WHERE User_ID='" + txtid.Text + "';", Sql_Connection.
sc);
SqlDataReader x = null;
x = c.ExecuteReader();
if (x != null && x.HasRows){
try//Login(in Database){
sqlc1.Connection1();{
SqlCommand cmd = new SqlCommand("SELECT User_
ID,Password1,Accound_Type,Status FROM user_details WHERE
User_ID='" + txtid.Text + "';", Sql_Connection.sc);
SqlDataReader read = cmd.ExecuteReader();
while (read.Read()){
txtpassword1.Text = (read["password1"].ToString());
textBox1.Text = (read["Accound_Type"].ToString());
st = (read["Status"].ToString());}
read.Close();
string x1 = Password.decrypt(txtpassword1.Text);
if (st == "ON"){
if (x1 == txtpassword.Text){
//to insert login history
sqlc2.Connection1();
ccmd = new SqlCommand("insert into login_History(ID,User_ID,
Log_in) values('" + txtcode.Text + "','" + txtid.Text + "','" +
txttime.Text + "')", Sql_Connection.sc);
ccmd.ExecuteNonQuery();
this.Hide();
Main f = new Main(textBox1.Text, txtid.Text, txtcode.Text);
f.Show();}
else{
MessageBox.Show("Password is incorrect.. Please enter correct
Password ");}}
else{
MessageBox.Show("Your ID Was Cancelled Please Contact
librarian");}}}
catch (Exception ex){
MessageBox.Show(ex.Message);}}
else{
MessageBox.Show("This ID is invalid");}}}}
```

Below mentioned codes were specially established maintain the password recovery and reset the User forgets the password by using email address he can easily recover or reset the password by generating the security codes for the passwords changes and it is sent to the own emails. This kind of facility the system well aware from the hackers.

Recover or Reset password:

```
private void button1_Click(object sender, EventArgs e)       {
         if (txtpass1.Text == txtpass2.Text)          {
            sqlc1.Connection1();             {
```

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

```
            //to select password
             SqlCommand cmd = new SqlCommand("SELECT
Password1 FROM user_details WHERE User_ID='" + txtid.Text
+ "'", Sql_Connection.sc);
            SqlDataReader read = cmd.ExecuteReader();
            while (read.Read())                {
                txtdpass.Text = (read["password1"].ToString());
}
            //decrypt password
            textBox1.Text = Password.decrypt(txtdpass.Text);
            string y1 = Password.encrypt(txtpass1.Text);
            string y2 = Password.encrypt(txtpass2.Text);
            //check password is correct or not
            if (textBox1.Text == txtold.Text)                {
               sqlc3.Connection1();
                SqlCommand ccmd = new SqlCommand("insert
into password_History(User_ID,Oldpassword ,change_time)
values('" + txtid.Text + "','" + txtold.Text + "','" + txttime.Text
+ "')", Sql_Connection.sc);
                ccmd.ExecuteNonQuery();
                sqlc2.Connection1();
             SqlCommand ccm = new SqlCommand("UPDATE
user_details SET Password1=@p1,Password2=@p2 Where(User_
ID='" + txtid.Text + "')", Sql_Connection.sc);
                ccm.Parameters.AddWithValue("@p1", y1);
                ccm.Parameters.AddWithValue("@p2", y2);
                ccm.ExecuteNonQuery();
                sqlc2.Connectionclose();
                        MessageBox.Show("Password Change
Sucessfully");
                sqlc3.Connectionclose();    }
            else {
                MessageBox.Show("Old Password is incorrect..
Please enter correct Password "); }    }
            sqlc1.Connectionclose(); }
        else  {
            MessageBox.Show("New Password is not Match..
Please enter Same Password "); }}
```

III. Result and Discussion

According to our research all the user creates an authentication and the information regarding his/her username and password is stored in the database through the Figure 2 graphical user interface strong password is advisable that the password length should be between 8 to 20 characters including symbols. Normally this kind of system database totally hided from the user only administrator can access the database. User of the system he/she needs to login with the usage of Figure 2.

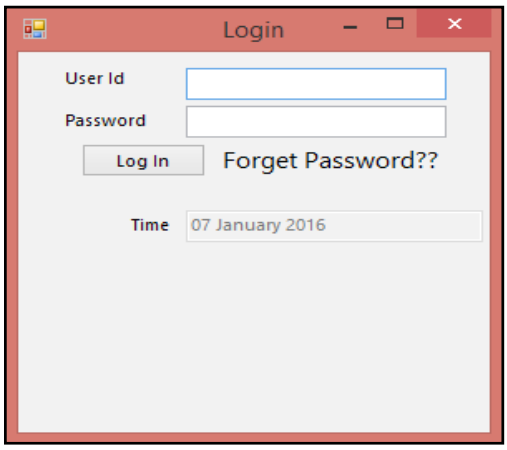

Fig. 2: Login Module

Login page contains user id, password and login button only if the user id and password are given correctly then user can be access the system or software. When both of details are not given, the message is given as "Please enter the correct user name" if the user id entered password is not entered the message is given as "please enter the correct password" to give the password detail, if the details are given incorrectly the message is given as "login failed" if the both user name password details are correctly the user allow to enter the account.

User forgot his/her password by using the interface figure 3 he/she can easily retrieve the password. To find the account details username of relevant email address is required with that email address user can get the verification code it were generated by the system. Finally the required code given correctly the bottom part of this module call reset password is activated.

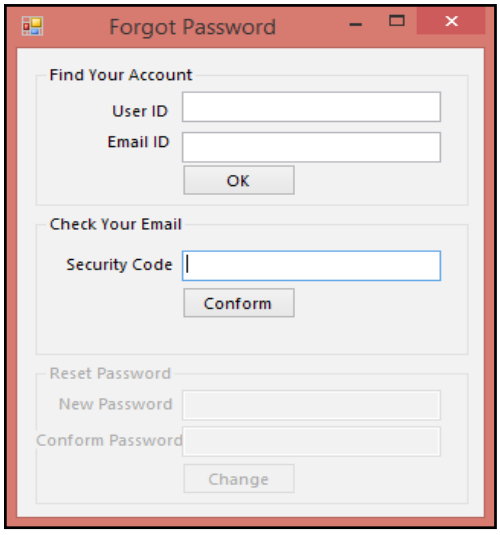

Fig. 3: Forgot Password

The given e-mail id is wrong you will get this message. Figure 4 email ID is wrong.

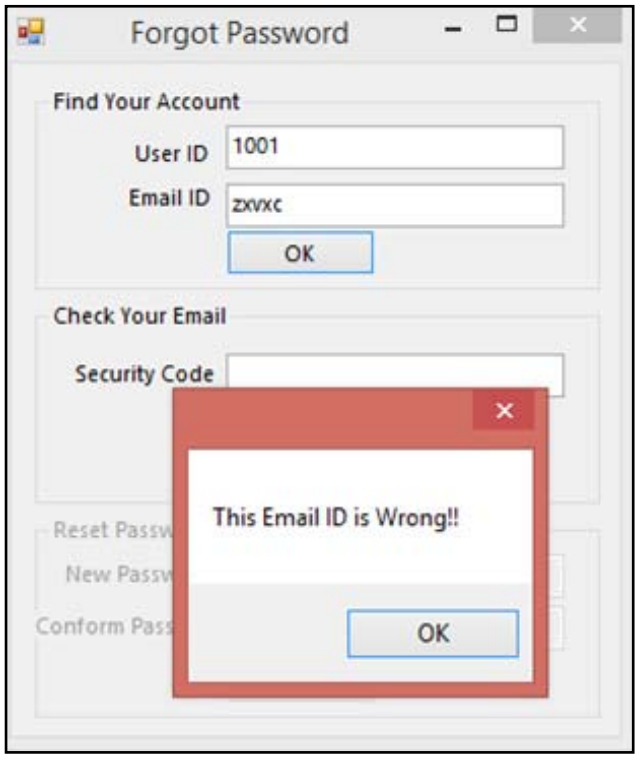

Fig. 4: Email verification

The given user ID is wrong you will get this message you are not registered or your insert wrong ID Figure 5.

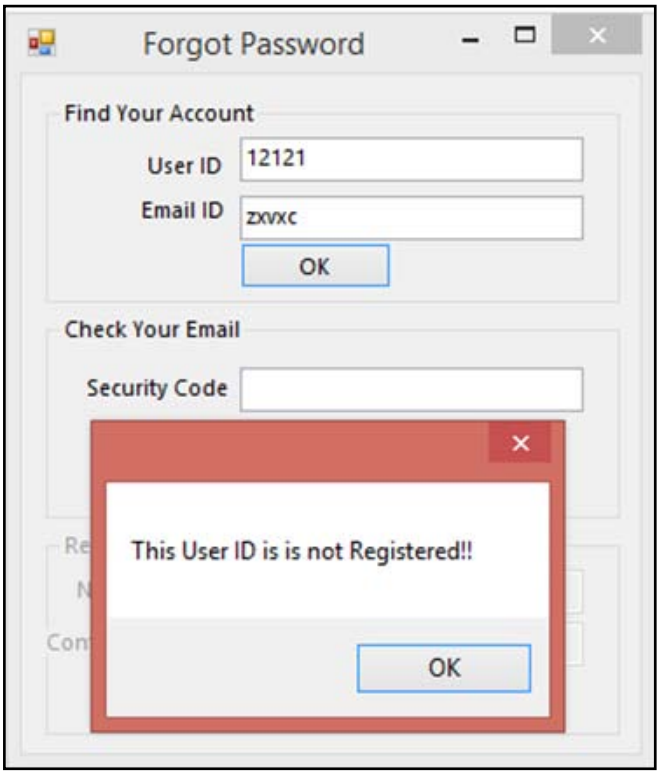

Fig. 5: Not registered emails

The required email ID or user ID given properly you will be get a new email on your email with the verification code is revels in the Figure 6. With that code user can rest his/her account password

Fig. 6: Recovery email

IV. Conclusions

In this paper, we have proposed an idea to enhancing the performance of the Login module to provide Authentication for the developed system. This system normally store the password as the encrypted format during the login time retrieve the password from the database as decrypted format the check whether the given password is matching with the database if is it matching user can able to access the software. User forgets the password by using email address he can easily recover that. This approach provides the high level authentication to the system and preventing unauthorized access.

References

[1]. Kogent Learning Solutions Inc, 2008. C# 2008 Programming: Covers.Net 3.5 Black Book, Platinum Edition. Dreamtech Press, pp: 71-226.

[2]. Kalaikavitha, E., and Juliana Gnanaselvi., 2013. Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology, International Journal of Engineering and Science 2(10): 14-17.

[3]. Imran, Z., and R.Nizami., 2011. Advance Secure Login, International Journal of Scientific and Research Publication 1(1): 1-4.

Author's Profile

VinayagamoorthyBalalojanan isa National Vocational Qualification (NVQ) Level 5 High National Diploma holder in the field of Information and Communication Technology, at College of Technology Jaffna, Sri Lanka. And Reading Bachelorof Technology in Information Technology at University of Vocational Technology Ratmalana, Sri Lanka. His research interest is in the area of Software programming, Database Management System and Embedded system. He is currently working at College of Technology Jaffna as a Visiting Lecturer.

JeyaperathaThangaraja is a National Vocational Qualification (NVQ) Level 5 High National Diploma holder in the field of Information and Communication Technology, at College of Technology Jaffna, Sri Lanka. Her research interest is in the area of Software programming, Database Management System and Embedded system.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

KanagasabaiThiruthanigesanpresently as anInstructorattached to theUniversity College of Jaffna, University of Vocational Technology, Jaffna, Sri Lanka. And Visiting Lecturer College of Technology Jaffna, Sri Lanka. Heis graduate fromthe Loyola College Chennai, India. Affiliated University of Madras, and at present M.Sc. Computer Science at University of Peradeniya. Hisengaged research area areSoftware Programming, Database Management System, Bioinformatics, Object-Oriented Programming and Embedded system.

NagarathnamThiruchchelvan presently as a Lecturer attached to the Department of Post-Harvest Technology, University College of Anuradhapura, University of Vocational Technology, Anuradhapura, Sri Lanka. He is graduated from University of Jaffna and at present M.Phil. Scholar in same University in the field of Biological control. His engaged research area are Entomopathogenic nematodes, Biological control of insect pests, Plant pathology, Nature conservation, Integrated Pest Management, Aquaponics, Storage pest control and Biotechnology.