User Authentication Approaches in Different Applications

Kumar Vishal, Ajay Shriram Kushwaha

School of Computer Science & Engineering, Lovely Professional University, Phagwara, Punjab, India.

Abstract:

This paper represents importance of user authentication over the applications, user authentications in different type of applications either it is web-based applications or mobile based applications or window-based applications it has been our protections by acting to prevent one's data from unauthorized access. With the achievement of new technologies, the way we have been using User Authentication has been changed and transformed into ample safe yet more easily than they were ever been in the past few years. This paper discusses the different approaches for developing user authentication for web based and mobile based applications [1][2].

Keywords: user, authentication, security, face recognition, fingerprint

I. Introduction:

The meaning of user authentication is users are going to be check for access the system. If we want to use some applications where user has to interact with the system in that case user authentication is needed. User authentication can be done in different way. There are many ways which define user authentication it can be by using face recognition techniques, biometric based techniques, fingerprint-based techniques or many more [3][4]. User authentication is depending upon where it is going to be apply in which system it is going to be apply this question is important. For example, if we want to access any devices like our laptop or mobile phone the approaches is different. Here this paper discusses about user authentication approaches in applications based. Security is the very important dimension of any software development application which include different ways to processes of user authentication, the user or software developer of the application, should manage these aspects while using and developing the applications. As we know there are many users use different applications in daily life [5][6]. So, in the past decade has forced the developers to come up with more secure strategies and user authentication approaches to handling security mechanisms. One of the most sensitive issue in application is validity of a user is considered which requires special attention especially in the case of user interaction applications. We should take care of unauthorized access specially in case of password which is also very sensitive data in applications [2].

II. User authentication for web based:

If we want to access any web application or web portal, we have to gone through user authentication process which is also called user validation process. For that user is valid or not user credentials are required to check.

Generally, user credentials have been stored in our logical database. There are many ways to store these login credentials in database. This is also depending upon the technology used to develop web-based applications [7][8]. Let say if application has been developed in asp.net technology in that case we can stored login credentials in SQL server database. In the same manner if we use php technology we can store login credentials in MySQL database. It means user authentication in web-based application is also different according to server-side technologies. We know web-based application is based on client server relationship. User which is also called client who is responsible for sending request to the server through login page by posting the login credentials to the server, after that server verifies the login credentials and send response back to the client. This is basic process of web application to check login credentials [9] [10].

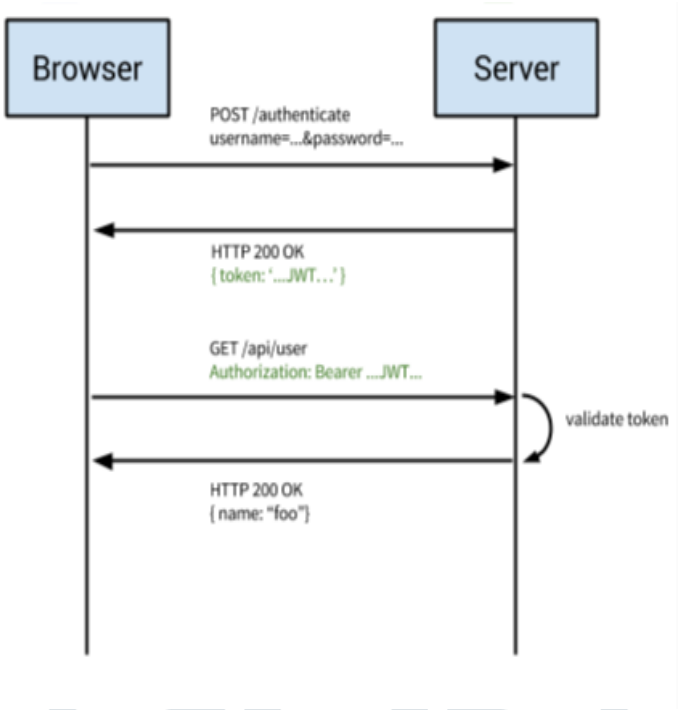

Fig. 1

III. User authentication for mobile based:

The process of user authentication in mobile based applications is also different according to mobile platforms. It can be a login credentials checked from database or user authentication can check through fingerprint, through voice and even through face recognition. But in general, if we want to access mobile devices in that case fingerprint, voice or face recognition approaches are performed. But in mobile applications either it is native based or hybrid base mobile application user authentication is a basic requirement. This is also depended which type of mobile applications users are using. Now a day's mobile applications are authenticated by using their social login credentials such as Facebook login LinkedIn login or Google login.

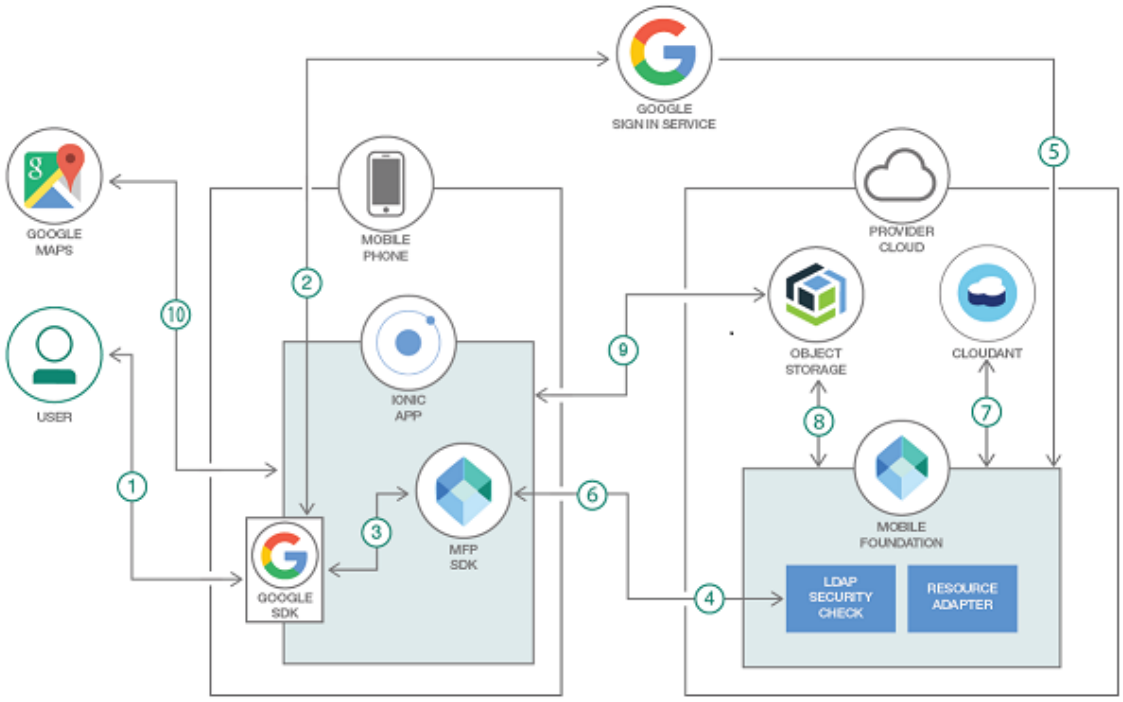

Fig. 2

In the above fig.2 diagram exemplifies the social login flow. The social-login security check user authentication with the token with its web client identifier from the security check configuration mechanism. The social-login returns the authenticated user to the Authorization Server API.

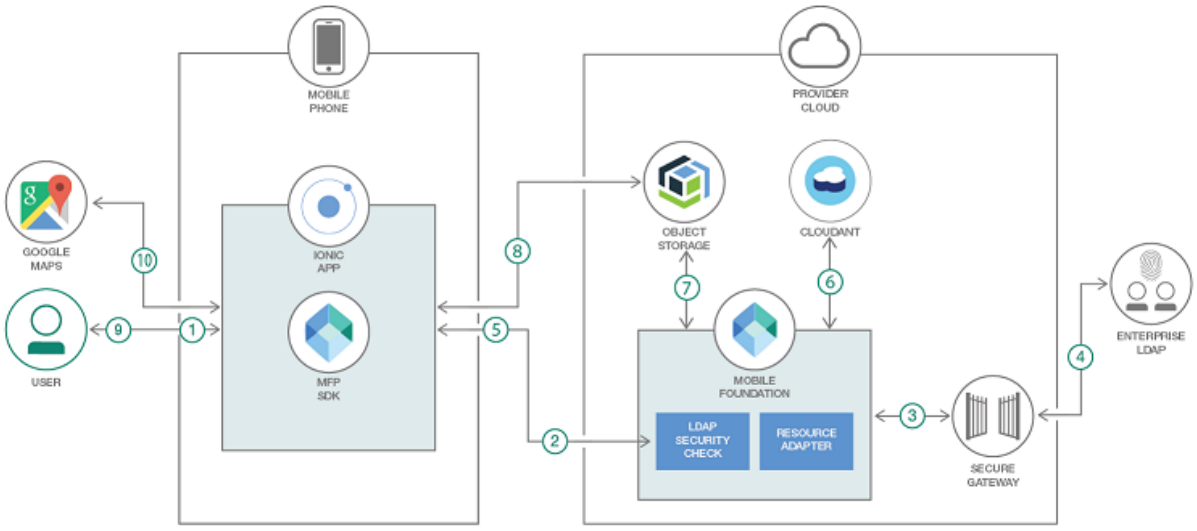

Fig.3

In the above fig.3 diagram user authentication checked by clicks on the login button. If in user authentication user is valid which shows user authentication succeeds, the mobile application shows the home page. Here to validate the user in user authentication, the security check login credentials with the help of adapter which connects to the predefined database server that can be access through a secure gateway.

IV. Implementation of user authentication:

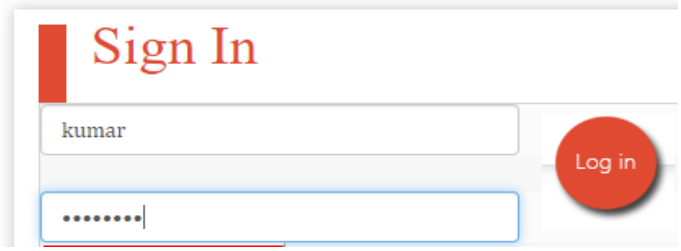

Fig.4

```
using System;
using System.Data;
using System.Data.SqlClient;
using System.Configuration;
namespace StudentManagementSystem
{
   public partial class Login : System.Web.UI.Page
   {
      string connectionString = ConfigurationManager.ConnectionStrings["myCon"].ToString();

      protected void Page_Load(object sender, EventArgs e)
      {

      }
      protected void ImageButtonSubmit_Click(object sender, System.Web.UI.ImageClickEventArgs e)
      {
            SqlConnection con = new SqlConnection(connectionString);
            con.Open();
            SqlCommand cmd = new SqlCommand("select *from adminMaster where admin=@admin and
password=@password", con);
            cmd.Parameters.AddWithValue("@admin", txtUserName.Text);
            cmd.Parameters.AddWithValue("@password", txtPassword.Text);
            DataSet ds = new DataSet();
            SqlDataAdapter adpt = new SqlDataAdapter(cmd);
            adpt.Fill(ds);

            if (ds.Tables[0].Rows.Count > 0)
            {
               Session["admin"] = txtUserName.Text;
               Response.Redirect("homepage.aspx");
            }
            else
            {
               Response.Write("<script>alert('Invalid Login');</script>");
            }
         }
   }
}
```

Here user authentication has been implemented in asp.net web application. Microsoft database file has been used to check login credentials which is stored table named adminMaster. If user is authenticated then homepage will be called. But in case of user is Invalid the message will be display to the user Invalid Login.

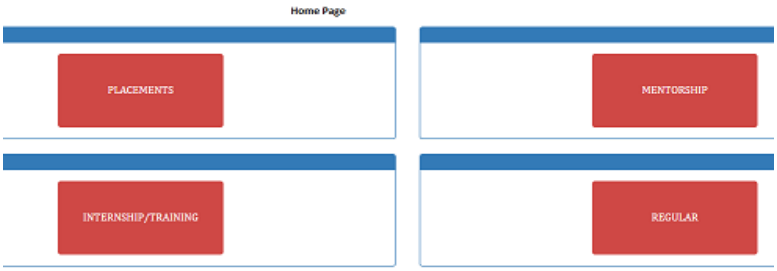

Fig. 5

```
public class LoginActivity : Activity
   {
      EditText txtUsername1, txtPassword1;
      Helper helper;
       protected void OnSubmit(View view)
       {
          txtUsername = FindViewById(R.Id.txtusername1);
          txtPassword = FindViewById(R.Id.txtpassword1);
          helper = new Helper(this);
          string strUsername = txtUsername1.Text.ToString();
          string strPassword = txtPassword1.Text.ToString();
          var user1 = helper.Authenticate(this,new
UserDetails(null,strUsername,null,null,null,null,null,strPassword,null));
                  if (user1 != null)
                  {

                     Toast.MakeText(this, "valid user", ToastLength.Short).Show();
                      Intent intent = new Intent(this, typeof(home));
                      intent.PutExtra("UserName", strUsername);
                      StartActivity(typeof(home));
                      }
                  else
                  {
           Toast.MakeText(this, "Invalid user",ToastLength.Short).Show();
                  }        }            }           }
```

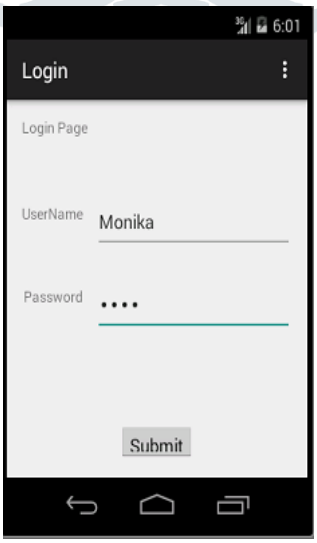

Fig.6

Here user authentication has been implemented in android mobile based application. SQLite database has been used to check login credentials with the help of helper class. If user is authenticated then home activity file will be called. But in case of user is Invalid the message will be display to the user Invalid User.

V. Conclusion:

Now we can say user authentication is important for any application where user interaction is required. Application either it is web based or mobile based or window based everywhere user authentication should be mandatory. There are some challenges because of there are lots of technologies we have and lots of different approaches also we have only we need to take care approaches must be followed by a proper requirement according to target end users means who is going to use that application target user will be those users. If the application is web based it should be followed with the proper client server relationship along with web-based security mechanism.

References:

[1] S. Halevi, H. Krawczyk, Public key cryptography and password protocols, in: Proceedings of Fifth ACM Conference on Computer and Communications Security, 1998, pp. 122-131.

[2] Malika Verma, Radhike Sawhney, Rashmi Chalia. "Biometric Based User Authentication in Smart Phones", 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), 2017

[3] B.T. Hsieh, H.M. Sun, T. Hwang, On the security of some password authentication protocols, Informatica 14 (2) (2003) 195-204.

[4] C.L. Lin, T. Hwang, A password authentication scheme with secure password updating, Computers and Security 22 (1) (2003) 68-72.

[5] M. Peyravian, C. Jeffries, Secure remote user access over insecure networks, Computer Communications 29 (5-6) (2006) 660-667.

[6] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu, YAGP: Yet Another Graphical Password Strategy, Annual Computer Security Applications Conference, 2008

[7] T.L. Horng, Password authentication using triangles and straight lines, Computers and Mathematics Applications 30 (9) (1995) 63-71.

[8] Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, A Graphical Password Based System for Small Mobile Devices, IJCSI International Journal of Computer Science Issues, 2011

[9] Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo and Hongxin Hu, On the Security of Picture Gesture Authentication, 22ND USENIX Security Symposium, 2013

[10] Kwang Il Shin, Ji Soo Park, Jae Yong Lee and Jong Hyuk Park, Design and Implementation of Improved Authentication System for Android Smartphone Users, 26th International Conference on Advanced Information Networking and Applications Workshops, 2012