Android Application for Passwordless Login for Web Applications

Aakash R Kanvinde  
UG Student  
Department of Information Technology  
K.J Somaiya Institute of Engineering & Information Technology, Sion (East), Mumbai: 400022

Swapnil A Panchal  
UG Student  
Department of Information Technology  
K.J Somaiya Institute of Engineering & Information Technology, Sion (East), Mumbai: 400022

Shamini V Palrecha  
UG Student  
Department of Information Technology  
K.J Somaiya Institute of Engineering & Information Technology, Sion (East), Mumbai: 400022

Prof. Reena Lokare  
Assistant Professor  
Department of Information Technology  
K.J Somaiya Institute of Engineering & Information Technology, Sion (East), Mumbai: 400022

Abstract

Passwordless Login for Web Application is an android application, will be used to access online internet accounts of distinct web applications and web services. The user would register with pre-requisite credentials primarily like, an email id, primary mobile number, and a unique username and a secondary mobile number. After successful registration, the user would be required to enter its registered username only. After submitting the registered username, a unique QR code will be popped up on the website. The user would scan the QR code using his/her android mobile phone. After successful scanning of QR code, the authentication and authorization procedure will be performed thereby granting secure access.

Keywords: QR code, SMS, Android mobile phone, passwordless, RSA

I. INTRODUCTION

Internet and technology has grown leaps and bounds within few years. Every traditional approach of our day to day life has been advanced and made online. Right from sending emails or messages to shopping online, booking a cab for travel to booking movie tickets and related number of activities. It is therefore required to maintain accounts with unique usernames and passwords to access and use these kinds of services. But to memorize these numbers of passwords is painstaking and exacting. We are often prone to forget passwords or misinterpret them with different accounts. This often leads to lose access to our account or getting our account compromised. Hence, our idea of precluding the practice of submitting passwords would be an efficient solution to access the online accounts by just entering a username and getting access to the same.

Passwordless Login for Web Application is an android application to access online internet account by entering username and scanning the QR code. There is no need to enter any password for accessing the online account. The registration for the app would be done on the android mobile by entering valid credentials.

After successful account generation, the user is required to enter the registered username and submit it. Thereafter, the login button is required to be clicked, and after scanning the generated QR code, access to the required account will be granted.

II. PROPOSED SYSTEM

Our system consists of an Android Application which would be linked to a database server. This database server would be linked with the online website for which a user desires to get access to:

The application would work as follows:

A. Module 1:

Website module: The website here, we have considered for our conceptual explanation is an e-commerce website. It can be of any category right from social networking sites to online gaming or free email account providers like Gmail, Yahoo, etc. The user is just expected to submit only the registered username on the login page thereby getting access by means of its android application after popping up QR code for specific user.

B. Module 2:

Database module: A database module would store important data required for authorization and authentication. This includes public key, private key, random number generated for specific user, mobile phone number, unique username and other associated...
credentials. The database is mutually accessed by the website and the android application. But the authority to write is only pertained onto the android application and the website can just read and verify the data.

C. Module 3:

Android Application module:
The Android application would be used as a gateway pass or token to access the linked websites. The first and foremost registration procedure is to be performed on the android application. After successful registration, the data is passed and stored in the database server. The QR scanner is deployed in this android application, which is used to scan user specific QR code; decode it and pass it to the database server.

D. Module 4:

Authentication and Authorization Module:
The data forwarded to the database server from the android application and the user input on the website are simultaneously verified whether such an association exists or not. If an exact association among two sources exists, then using RSA algorithm, the user is granted valid access.

In existing systems, there is a constant need to keep record of distinct usernames and passwords\[^{[2]}\]. There may occur instances where same username criteria cannot be achieved for varied accounts or applications. So keeping an accurate log of usernames and passwords linked with all the user’s account is a painstaking experience\[^{[3]}\]. Also, the user is also vulnerable to lose appropriate username, eventually losing access over its account\[^{[5]}\]. It may be a minor loss when the lost account would be of a social networking or entertainment related as they can be recreated and blocked overtime. But losing an account/application which handles one’s economic or commercial activities may be much devastating. The same password combination for multiple accounts is a no wise solution, leading to weak password generation\[^{[5]}\][\[^{[10]}\]]. The CAPTCHA approach consumes much time when compared to current technological standards thereby succumbing to inefficient development approaches\[^{[4]}\][\[^{[7]}\][\[^{[8]}\]].

On the contrary, the online accounts/applications can be managed much more efficiently using the proposed system. The unique username, once selected by the user for registering, can be used as universal username for logging into all the linked accounts/applications. Also, in-case of loss of android phone, the recovery procedure is apt to regain access of all the accounts within few seconds. Once adopted by all the social networking or entertainment and commercial application providers, it may prove a great help to maintain healthy access to the required resources\[^{[10]}\].

![Sequence diagram of the proposed system](image)
Fig. 1.2: Proposed system work flow
III. IMPLEMENTATION

A. Website Module:

1) Start Page

![Start Page requesting Registered Unique Username]

Login Page with QR code on registered username submission

![Login Page with QR code on registered username submission]
3) **Home Page:**

![Home Page Image](image1)

Page after valid log-in

**B. Android Application Module:**

![Android Application Image](image2)
C. Android Application Start Page:

![Android Application Start Page]

D. Registration Page

![Registration Page]


\[ E. \quad \text{Registration Page} \]

\[ F. \quad \text{QR Scanning Page on Registered Username Submission} \]
G. Recovery Page

Recovery Page incase of loss of mobile

II. Characteristics of Each Module:

Our system consists of an Android Application which would be linked to a database server. This database server would be linked with the online website for which a user desires to get access to:

The application would work as follows:

1) Module 1:
Website module: The website which the user desires to have access with should be linked with the database of the android application which will be further shared by all the linked websites as future scenario. The user would submit its pre-registered unique username on the website’s login page and submit it. After successful submission, a QR code would pop up and further steps should be forwarded through android application thereby granting valid access.

2) Module 2:
Database: A database will be created providing mutual access to both the website as well as the android application. The primary tables required to store are the unique username, mobile phone number, public key, private key as well as random number required for generation of unique QR code.

3) Module 3:
Android Application: The android application would be the primary resource, which the user should have access to for getting a valid access on varied websites. The user is required to register on the android application with different credentials and these data would be passed and stored on the database server shared among android application and the linked website.

IV. Future scope

1) With the adoption and use of this application, the need to remember different user id’s and associated passwords can be eliminated.

2) It can be linked with all major social networking sites, thereby providing single sign-on enabling safe, secure and easy means of access.
V. CONCLUSION

The application is very useful in case we forget our password of various accounts. To maintain and access distinct email ids (username) & passwords is a hectic experience. One needs to memorize distinct credentials and passwords to access one’s online account. Users are often succumbed to forget these credentials and lose their authority over these accounts. It also leads to compromising of their accounts leading to loss of information or any other important data. This problem can be countered if a simple mode of accessing one’s account is developed and implemented. Our project can let an individual access its online account and consume the provided service with few simple steps. After successful registration, the user should follow few steps to access its account. Also, these steps just offer the user to enter the username which was being entered at the time of registration, and no password is required.

ACKNOWLEDGMENT

We wish to express our sincere gratitude to Prof. Reena Lokare, Project Guide for providing us an opportunity to do our project work in Android domain. We sincerely thank Mr. Uday Rote, HOD of IT Department and Mr. Harsh Bhor, Project Coordinator for their guidance and encouragement in carrying out this project work. We also wish to express our gratitude to the officials and other staff members of K.J. Somaiya Institute of Engineering and Information Technology, who rendered their help during the period of our project work.

REFERENCES