

## Android Application for Password less Login for Web Application

Aakash Kanvinde

Be Student,

Department Of Information Technology,  
K.J. Somaiya Institute Of Engineering And Information  
Technology,  
University Of Mumbai, Maharashtra, India  
*Akash.K@Somaiya.Edu*

Swapnil Panchal

Be Student,

Department Of Information Technology,  
K.J. Somaiya Institute Of Engineering And Information  
Technology,  
University Of Mumbai, Maharashtra, India  
*Swapnil.Panchal@Somaiya.Edu*

Shamini Palrecha

Be Student,

Department Of Information Technology,  
K.J. Somaiya Institute Of Engineering And Information  
Technology,  
University Of Mumbai, Maharashtra, India  
*Shamini.P@Somaiya.Edu*

Prof. Reena Lokare

Assistant Professor,

Department Of Information Technology,  
K.J Somaiya Institute Of Engineering And Information  
Technology,  
University Of Mumbai, Maharashtra, India  
*Reena.L@Somaiya.Edu*

**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**—SMS, Android, QR code , 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<sup>[9]</sup>. 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. LITERATURE SURVEY

Existing system requires username to create an account using a combination of unique username and password. It is confounding when the number of registered accounts are increased considerably as user as to memorize

distinct username and password combination for distinct linked accounts. It is also a demanding experience when one needs to recover its account in case of loss of passwords. For this we have surveyed different IEEE papers and studied any development in case if proposed or existed.

The numbers of papers published and proposed on these issues were very few. We came across 3 distinct IEEE papers which provided a solution in one or the other way but had some constraints and limitations.

In paper <sup>[1]</sup>, a solution was proposed to access online accounts by registering the mobile using its IMEI number with the web service or application. With the help of push message service, an OTP (One Time Password) would be sent to the registered IMEI cell phone <sup>[1]</sup>. On successful receipt of the OTP, the individual is required to enter the OTP in the log-in page of the site thereby enabling access to the service. This process is a bit time consuming as OTP may arrive late when the user is under unhealthy network coverage. The regeneration of OTP is dilatory scenario as once the session time gets expired, a new OTP will be required which would again consume considerable amount of time.

In paper <sup>[2]</sup>, the idea of logging online accounts through mobile was proposed by reading the CAPTCHA image displayed on submitting the username or user-id<sup>[4][5][7]</sup>. This was naïve approach and not that efficient as mobile phones have been technologically much advanced today.

In paper <sup>[3]</sup>, the action of registering the user with the particular website only was performed. A session token will be shared by that website with the user <sup>[3]</sup>. When the user attempts to access that particular website, the token would be verified and accordingly on successful authentication and authorization, access will be granted to the individual. Since, token shared will be for limited session (time constraint); on time expiry, a new token will be required to be generated and again the same procedure needs to be followed <sup>[6][8]</sup>.

### III. SYSTEM ARCHITECTURE OF 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:

#### 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. 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.

#### 4) Module 4:

Online Shopping Website:

After successful registration, the user enters the unique username (username entered for registration) and should click the submit button on the shopping website. If the username is registered with the android applications database, it will be accepted on submitting on website or else an error will be displayed to enter registered username.

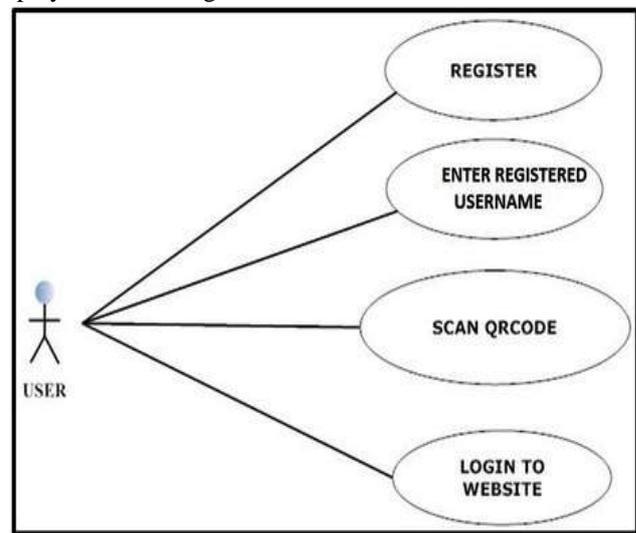
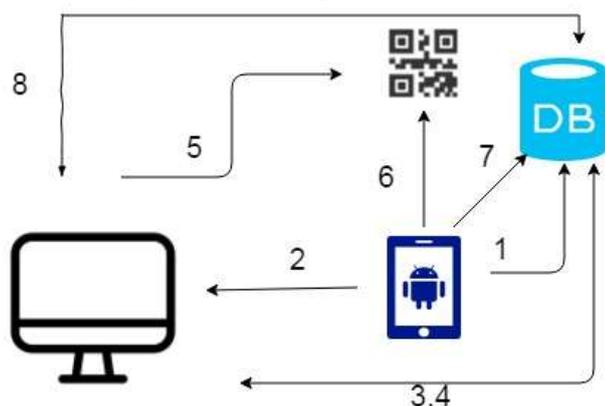


Figure 1.1: Use Case Diagram

### IV. COMPARISON BETWEEN EXISTING AND PROPOSED SYSTEM

In existing systems, there is a constant need to keep record of distinct usernames and passwords. There may be instances where same username criteria cannot be achieved for varied accounts or applications <sup>[5][6]</sup>. So keeping an accurate log of usernames and passwords linked with all the user's account is a painstaking experience <sup>[5]</sup>. Also, the user is also vulnerable to lose appropriate username, eventually losing access over its account.

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 secured and easy access to the required resources.



**Figure 1.2: Working Diagram**

## V. CONCLUSION

The application is very useful since we do not have to memorize distinct passwords linked to varied accounts. To maintain and access distinct email ids (username) & passwords is a hectic experience. One needs to memorize distinct credentials and passwords to access its respective online account. Users are often succumbed to forget these credentials and lose their authority over these accounts. It also leads to compromise 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.

## VI. ACKNOWLEDGEMENT

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 Prof. Uday Rote, HOD of IT Department and Prof. Harsh Bhor, Project Co-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

- [1] Bo Zhu, Xinxin Fan and Guang Gong. Loxin – A Solution to Password-less Universal Login. 2014 IEEE INFOCOM Workshops: 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data.
- [2] Mohammad Shirali-Shahreza, Sajad Shirali-Shahreza. Passwordless Login System for Mobile Phones Using CAPTCHA. 49th International Symposium ELMAR-2007, 12-14 September 2007, Zadar, Croatia
- [3] Kirit Sælensminde, Prof. Veera Boonjing. A simple password less authentication system for web sites. 2010 Seventh International Conference on Information Technology
- [4] L. Von Ahn, M. Blum, N. Hopper, and J. Langford, "Captcha: Telling humans and computers apart automatically," in Proceedings of Eurocrypt, 2003
- [5] E. H. Spafford, "OPUS: Preventing Weak Password Choices," Computers & Security, vol. 11, pp. 273–278, 1992.
- [6] K. Zetter, "Weak Password Brings 'Happiness' to Twitter Hacker," January 2009. [Online].
- [7] L. von Ahn, M. Blum, J. Langford, "Telling Humans and Computers Apart Automatically", Communications of the ACM, Vol. 47, No. 2, February 2004, pp. 57-60.
- [8] M. Shirali-Shahreza, S. Shirali-Shahreza, "Collage CAPTCHA", Proceedings of the 20<sup>th</sup> IEEE International Symposium Signal Processing and Application (ISSPA 2007), Sharjah, UAE, February 2007.
- [9] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA, pages 553–567, 2012.
- [10] P. Gasti and K. B. Rasmussen. On the security of password manager database formats. In S. Foresti, M. Yung, and F. Martinelli, editors, Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings, volume 7459 of Lecture Notes in Computer Science, pages 770–787. Springer, 2012.