International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

2 FAUS: Two Factor Authentication Using Smartwatch and Google Cloud Messaging Service

Prof. Purnima Ahirao[1], Khushang Mehta[2]

[1]Asst Prof, Dept of IT, KJSCE, Mumbai, India
[2]Student, University of Cincinnati, Cincinnati, OH

Abstract - Two-factor authentication is an important technique used for providing Security to all types of Login features used worldwide. Users are prompted to provide something they know using something they have. The proposed system provides Two-factor Authentication using Smartwatch. The system is aimed at providing a convenient and secure access to user accounts. This method delivers a service which can be used for all authentication purposes such as User Login Authentication, Online Payment Authentication, Remote Access Authentication, etc. Existing two factor authentication methods rely on SMS and/or e-mail services for sending temporary codes to users in order to verify the user's authenticity, on top of the user/password combination. It also requires the users to remember and input lenghty codes everytime a login is attempted. This paper presents a novel two-factor authentication scheme where a user's smartwatch receives a notification from the service using the proposed protocol. This notification will prompt the user to enter his own selected password in the application built for the smartwatch.

Key Words: Authentication, Security, Smartwatch, Android Wear, Privacy and Two Factor Authentication.

1. INTRODUCTION

Current authentication systems rely on one or multiple usually complex passphrases to be remembered by the users which are sometimes required to be changed periodically. Any of these common actions could put the users at risk of having their password stolen: i. Using the same password on more than one site ii. Downloading software from the Internet iii. Clicking on links in email messages The proposed system introduces another layer of security where the authenticity of the user is verified more than once. Current methods for two step verification rely on SMS or email which are time consuming and require unnecessary user interactions. The proposed system will allow users to use a two-step authentication system, first login and authenticating the login throught the use of a smartwatch. The system will eventually help in saving time and reducing the amount of user actions required. Use of smartwatches worldwide are increasing by a huge percentage. This proposed system can be used as the base for most of the security applications that will be developed for smartwatches. The two factor authentication system presented in this paper utilises a smartwatch (something you have) to authenticate themselves to any Login Interface. The system uses a 4 digit code that is set by the user while registering with the system. The system will send a notification to the user's smartwatch (using Google Cloud Messaging), prompting the user to input a password. Entering the correct password will grant the user access to the web service. This system will enable faster secured access to a service. Multiple accounts, from different services, of the same user can be used on the same applicaiton for two step authentication. Two factor authentication using smartwatch, can be coupled with multiple web services to provide a faster mechanism for authentication.

2. EXISTING SYSTEM

The current two-factor authentication system as in [1] uses a classic way, sending a SMS or an E-mail with an OTP(One Time Password) to the corresponding number or mail ID. This system require users to spend more time in signing in to the account than required. The traditional system also causes an inconvenience to the user, either to login everytime to his email id or fetching his phone from the pocket or desk which may be in another room. The user is then required to enter the OTP recieved in the web application to gain access. Hence, users according to a study do not opt for a two factor authentication for the same reason. In paper [2] Giri and Srivastav explains the flaws in existing remote authentication systems relying on smart cards and proposes a better system to replace this one. It improves upon the existing systems by overcoming its flaws. The method proposed in this paper is a dynamic ID-based remote user authentication using smart cards. One of the ways it accomplishes this is by providing the users with the choice to set and change their passwords. In [3] Google provides an overview of various security features that are in Place at the OS level and at the Google services layer. It also introduces the new device management capabilities developed for work, which give enterprises the ability to manage and develop applications on their users devices, prevent work data leakage, secure the communication back to the enterprise, and manage the applications installed in their workspace, preventing any unapproved apps from

being installed for work. Smartwatches is in hype in the technological world due to its feature of interactions with the smartphone[4]. These smartwatches can display text messages and emails. The pebble watch also has an e-reader-style display. So the smartwatches are being pitched to be used for convenient communciation in the electronic form.

3. PROPOSED SYSTEM

Our proposed system enables users to quickly and easily get through the steps of the two factor authentication system. The user only requires to have a working internet connection from the smartwatch to the internet. Google Messaging Service(GCM) is used to automatically send a message to user's device. Opening this message allows the user to authenticate himself on the smartwatch.

3.1 Overview of Implementation

Fig1. Presents the block diagram of the proposed system.Chart -1:

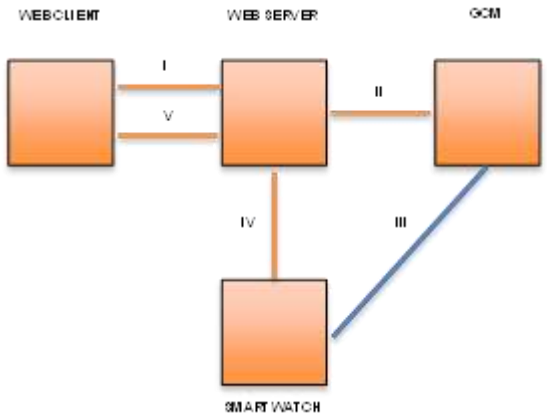

Fig -1: Name of the figure

As shown in Fig 1 the System is divided into 4 Phases
•Implement the Watch App UI and Mobile App UI: In this phase the Android Wear and Mobile UI was developed using Android Studio.
•Implement the Website UI: In this phase we were able to develop a website page using HTML5 and CSS. 14
•Implement the Data Layer between Watch App and Phone App: The Watch App and the Phone App were further developed to work together and enable more features.
•Implement the Web api to connect to the Mobile and Watch App: The website needs to be connected to the Watch interface for the user to authorize himself.
• Implement Encryption and Authentication algorithms: Encryption and Authentication algorithms will be used to make the interface more robust and Secure.

3.2 2 Factor Authentication using Smartwatch(2FAUS)

The 2FAUS system enables users to quickly and easily get through the steps of the two factor authentication system. The user only requires to have a working internet connection from the smartwatch to the internet. GCM 25 is used to automatically send a message to user's device. Opening this message allows the user to authenticate himself on the smartwatch.

A. Logging in through 2FAUS enabled service: User logs in t by providing login credentials as shown in Fig2

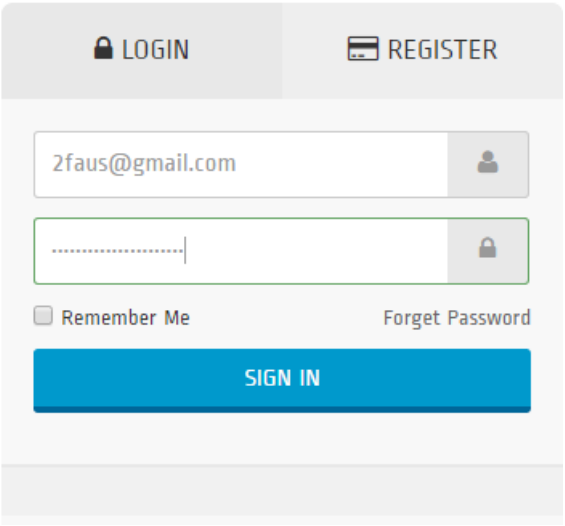

Figure 2. Login using 2FAUS

B. Sending Message through Google Cloud Messaging: Once the web service authenticates the user, it sends a message to the user's smartphone via the Google Cloud Messaging (GCM) service for second level of authentication.
C. Notification to Smartwatch: The smartphone sends a message to the smartwatch as shown in figure 3, informing of a log-in attempt and requesting second level of user verification for a web service.

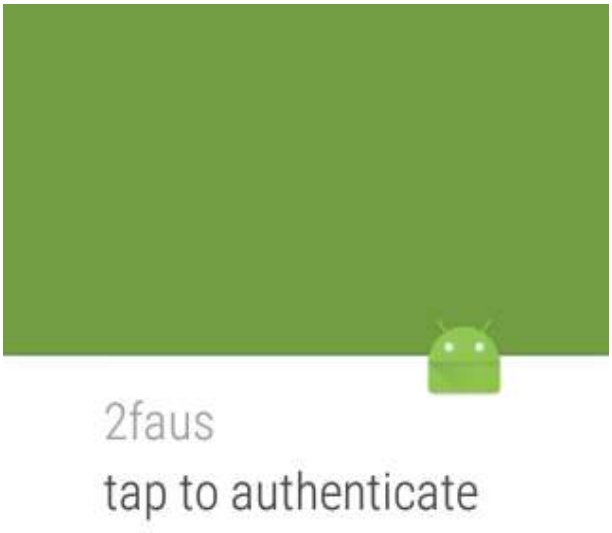

Figure 3. Notification on Smartwatch

D. Verification using code on Smartwatch: As shown in Fig 4 On clicking the notification, the user is prompted to enter a four digit code that is set by the user . The notification sent to the Watch will trigger an application launch.This application as shown in the figure 4 will display a 4 pin password lock. _ The user can use this password lock to verify himself in the 2 step authentication process. Entering the right password would trigger a call to the Web Service letting the user to be let into the web site. 24 This code is set to the device and is same for any service using 2FAUS for a user. On the password input screen, the user needs to press the button corresponding to the digits in the code, once for every digit. Traditional 10 button input is not suitable for a screen of such size. Android wear devices have a resolution of either 240x240 pixels or 320x320 pixels.

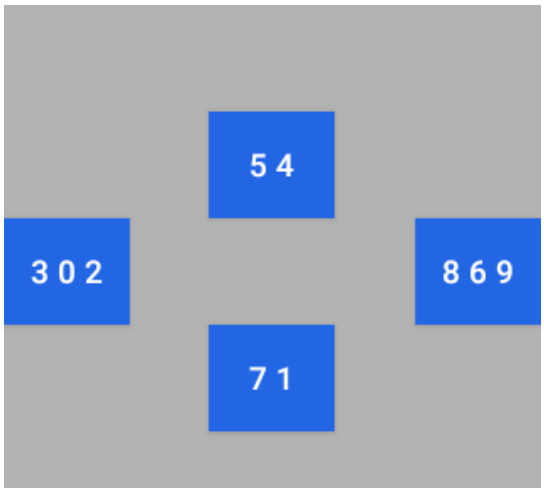

Figure 4: Password Input on Smartwatch

E. After entering the correct code, the 2FAUS application on the watch sends a message back to the phone using DataLayer. The smartphone then informs the web service and the user is then allowed access.

This communication between smartphone and web service is handled by either the GCM. Since the smartwatch cannot directly communicate with any online web service as of now, all the communication between the web service and the smartwatch is done with the user's smartphone as an intermediary. The smartphone application will connect the smartwatch to the web service using GCM .

4. CONCLUSION

Online accounts today, protected by a single factor authentication such as passwords are prone to hacking. Two factor authentication has already been introduced, but in most cases, user's are more of frustrated rather than thinking of it as a helpful security measure. The smartwatch industry has its sales increasing quarts-over-quarter by a huge percentage, sources show 160 million smartwatches to be shipped in the year of 2019 alone. This shows that a huge base of users to be qualified for using our technology. This paper focuses on the implementation of two-factor authentication methods using smartwatches. It provides the users with an ease of use and faster response to the traditional two factor authentication system. The proposed system has the option of notifying the user on the smartwatch and enabling him to enter the pin in a small amount of time. This method also helps the users to be able to share their account ID's and Passwords while keeping the shared user's access in check. This system also allows users to keep the same or easy to remember for different accounts without compromising its security.

5. REFERENCES

1. Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. Ms.E.Kalaikavitha
2. Cryptanalysis and Improvement of a Remote User Authentication Scheme using Smart Cards (IEEE), D. Giri and P. D. Srivastava.
3. Android for Work Security White Paper, Google .
4. https://sensiblemicro.com/smart-watches-the-start-of-the-wearable-electronics-revolution/
5. THE SMARTWATCH MARKET: Growth, Consumer Attitudes, And Why This Is The New Device Category To Bet On, Tony Danova.
6. Two Factor Authentication Using Mobile Phones, Fadi Aloul, Sye