WiFi Authentication through Social Networks
Karuna Hasani¹, Yash Vaswani², Ajay Bhagchandani³, Anjali Yeole⁴
Department of Computer Engineering, VESIT, India

Abstract:
With the increase in technology in the field of networking, wifi is nowadays used everywhere, as wireless technology keeps dominating day by day. Almost every homeowner who uses internet uses a wifi. It also is a burden for that homeowner to share his wifi password with every near and dear one who visits him. Hence, the main aim of this project is to authenticate wifi through social network i.e. Facebook. The visitor gets an automatic wifi access if he is a friend of the homeowner on Facebook. It is a decentralized approach where the burden of sharing the wifi password is eliminated.

I. INTRODUCTION

1.1 Motivation

Wireless Technology is increasing day by day in the field of Networking. So is the number of Wi-Fi in household use of internet. It nowadays is a burden to share our Wifi password with each and every friend / relative who visits home quite often. We also can’t trust a friend who knows our Wifi password as he/she can spread it and let many people use it to slow down our Wi-Fi speed. So, the motivation of this project arises with a question, “Why Give our Wifi password to everyone, if we can give them the direct access to our Wi-Fi using a social network?”

1.2 Problem Definition

The main aim of this project is to get the devices of our Facebook friends automatically connected to Wifi whenever they're in our Wifi range. Wi-Fi gets the device details, checks the device's Certificate and the Facebook application and checks for the friendship between the device user and the Wifi owner. If device of a person shows that he is the Facebook friend of the System owner, then his device gets automatically connected to Wifi. This eliminates the burden of sharing the wifi password with everyone.

1.3 Relevance of the project

In the proposed system, we’ll use the Facebook API that allows us to check the Owner’s friend list and Search the profile of the one who has logged in using our Wifi through our pop-up. The digital certificate of that person’s device is also stored into the cloud at that very time. If the person is found to be the friend of the owner, then he/she is said to be the friend on Facebook. In this project, it is mandatory to store the wifi data on the cloud, to ensure the continuous working of the System and ensure it being Computer dependent.

1.4 Methodology used

The implementation of the proposed system is divided into two main parts:
1) Authentication and Certification.
2) Search and Grant / Revoke access

In authentication process, the system will perform 2 tasks.
1) **Check for Certificate**: - If the device that wants to connect to our wifi, has it’s certificate already generated and stored in our wifi database, then just the 2nd part is performed and The wifi access is Granted or Revoked automatically as per the conditions of the system. If the device is not registered (new device), then a pop up is emerged by our system that asks for Facebook authentication details. The certificate of that device is automatically generated and stored into the wifi database at that very moment.

2) **Search and Grant / Revoke access**: - Once the device logs into the Facebook, his profile is checked and is searched into the friend list of the owner. If the search is found, then the device gets connected to the Wifi as the friend relation is confirmed. If the search is not found, then Wifi access is denied and normal method of asking a Wifi password is followed.

The methodology that’ll be used by us in this project is The Waterfall Model. In this Model, we’ll follow the stepwise procedure and will work according to 4 phases:
1) Requirements Gathering phase.
2) Design and Analysis phase.
3) Implementation phase
4) Verification and Testing phase
5) Maintenance phase.

The workflow of this project will proceed according to one phase at a time. Once the necessary and sufficient data for 1 phase is gathered, we’ll move on to the next phase.

II. LITERATURE SURVEY

2.1 A novel Wifi authentication scheme

The referred paper [1], describes a scheme for sharing of Wifi using the trust relation established by social media. It further deals with minimization of search complexity and the results published indicate that usage of cached data can help in quick authentication of direct friends. However, authentication of indirect friend’s results in a much larger trust chain that needs
to be parsed. The quadratic complexity limits the basic scope of our project to direct friends. An additional aspect of this service can be found in the documentation of existing services - Facebook Wifi [2] and social Wifi. These present the scenario where a larger entity such as a hotel can market themselves via ‘check-ins’ and ‘likes’ on Facebook. This scheme of parsing the page’s list is an extension and thus a future scope for our project. Therefore, on the basis of the workflow derived from these established methods, the first iteration of our project includes replacement of password authentication with trust relation based on established relationship on social media.

2.2 Survey on implementation procedures

An established system by Motorola solutions [3] [4] [5] gives insights into the physical implementation of this method on 802.1X access points via the usage of digital certificates. Here, Secure Access Wizard is configured by the network administrator and then deployed to a web server. Users can connect to an open Wifi SSID with their personally-owned smartphone or tablet and open their browser to access the Wizard, which automatically sets up the device, and shifts the user to a secure Wifi connection encrypted by WPA2-Enterprise. Users can set up the initial authentication through one of their social networking accounts. For the user interface pop-ups, there exists Graph API which is an established method used by Facebook apps to extract user data. The permissions for obtaining this data are sought by Facebook login. Facebook for developers documentation describes the procedure to be followed and the format of information obtained as the outcome.

2.3 Patent search

Apparatus and Method for Accessing Wifi Networks

A method and apparatus are provided for accessing Wifi with a social network member’s information by automatically accessing a social network account. The member’s information is used to derive a network detection portion and a security portion. The network detection portion is used as an input and detection is made that the wireless device is within range of a secure wireless network associated with the particular member. The security portion of the member information of the particular member is retrieved from the social network and is used to derive access credentials for the secure wireless network.

Patent “US 2016021540 (A1) - APPARATUS ... WIFI NETWORKS” 21 January 2016

Social network based Wifi connectivity:

An embodiment of the invention provides a method for social network based Wifi. Relationship status (es) between the owner of the mobile electronic device and the owner(s) of the wireless network(s) are determined with an analysis engine. A request to access a wireless network is received from the owner of the mobile electronic device. Access to the wireless network is automatically granted when the relationship status between the owner of the mobile electronic device and the owner of the wireless network is above a predetermined threshold.
What databases can be used in cloud?

Databases like Oracle Database, Microsoft SQL Server, MySQL, MongoDB are the types of database which can run in the cloud.

VI. CONCLUSION

The WiFi authentication systems describe the first decentralized social WiFi AP design freeing the average homeowner from the burden of manual access control. This system introduces the use of context information to reduce the search complexity for establishing indirect trust relations in a distributed online social network, and detail an implementation based on tracking standard probe request messages. The WiFi authentication systems also provide experimental results validating the feasibility of our design, and report on the effectiveness of using context information.

VII. REFERENCES


[4]. https://developers.facebook.com/docs/facebook-login

[5]. https://developers.facebook.com/docs/graph-api/reference/user

[6]. Yunus Durmus Koen Langendoen Delft University of Technology, the Netherlands
