Access to Geo-Fenced resources from registered locations

Anusha Salam, MTech Scholar in CSIS,ICET,Enakulam,Kerala,India,PH-8547838721,E-mail:anusalam90@gmail.com,
Arunkumar M, Assistant Professor, Dept of CSE,ICET,Ernakulam,Kerala,India,PH-9961967044,E-mail:arunpvmn@gmail.com.

Abstract—Nowadays companies prefer to restrict access to their resources. Geo-fencing can be used to restrict access to such resources within the fence. These resources can include data or management and utility tools. With geo-fencing; it will be advantageous to access such resources at n different locations providing the flexibility of working from home location for all staff. In such a scenario, access control must be ensured based on location along with some rewards. Location accuracy is ensured by considering verification mechanism based on information from multiple sources such as Global Positioning System (GPS), Wireless Fidelity (Wi-Fi) and IP address. This system adds more security as well as benefit passionate IT professionals.

Index Terms— Authentication, Authorization, Geofencing, Location based authentication,Lcation based authorization.

1 INTRODUCTION

Geo-fencing means setting boundaries. The applications which uses geo-fencing include child location services, telematics, location specific advertisements etc. Usually the geo-fence is set with the help of Global Positioning System (GPS) or Radio Frequency Identification (RFID) or Google Earth or web based maps. Most of the applications check fencing criteria either entering or leaving the fence to send alerts. This can be used as an authentication criterion while the person is within the defined fence.

While defining fence for accessing resources in a company, there comes an issue that staff will be able to access such resources only from company. In such cases it will disrupt the workflow of passionate people who also work from home. To enable access to geo-fenced resources from home, home locations have to be preregistered and limited accesses have to be provided.

Access from registered locations can be done with the concept of location based authentication and authorization since here also it is the location criteria along with some credentials provided by user authenticate and authorize staff. Location is used as a factor for authentication using Smartphone. Along with geo-fencing location from location sources such as IP address, Wi-Fi BSSID along with GPS can also be used for authentication and providing security.

New generation IT professionals are more passionate in their work .Most of them too work from home. The proposed idea guarantees access of such geo-fenced resources at registered home locations of users. Moreover in the current scenario each of these workers is not benefited for their extra effort at home. The proposed idea can identify such passionate people and reward them as per their true effort. True effort is no longer hidden.

2 RELATED WORK

Some of the existing geo-fencing applications are discussed in [9],[10],[11],[12]. Location based authentication was first introduced to improve network security using a special GPS sensor in [1].Access granted within specific locations was earlier done by identifying overlapping region of multiple access points in LAAC [2].Websites using location information from mobile phone was used in e-learning environment[3].The studies show that GPS and WLAN has an accuracy of below 300 m[4].Combining authentication mechanisms can improve both reliability and security [5].Location aware services using Smartphone are introduced[6].Location based authentication and authorization is discussed in [7].Location based authentication as a new approach for information security is discussed in [8].

The rest of the paper is organized as follows. A novel architecture for authenticating client and location based access in section 3.1.Section 3.2 describe the messages used for communication in detail. Section 3.3 describe the implementation details. The experimental set up is covered in section 3.4. The idea is concluded in section 4. The main advantage of this approach is that it can be easily integrated into the existing system for improving security. The approach is inexpensive and feasible as no new hardware is needed as a company usually have Wi-Fi and network connection.

3 METHODOLOGY

The scenario is as shown in Fig. 1.Here user have full access to resources when inside company and partial access from home. Whether the staff is inside the company is identified by making use of information such as GPS, Wi-Fi BSSID and IP address retrieved dynamically from the mobile application of

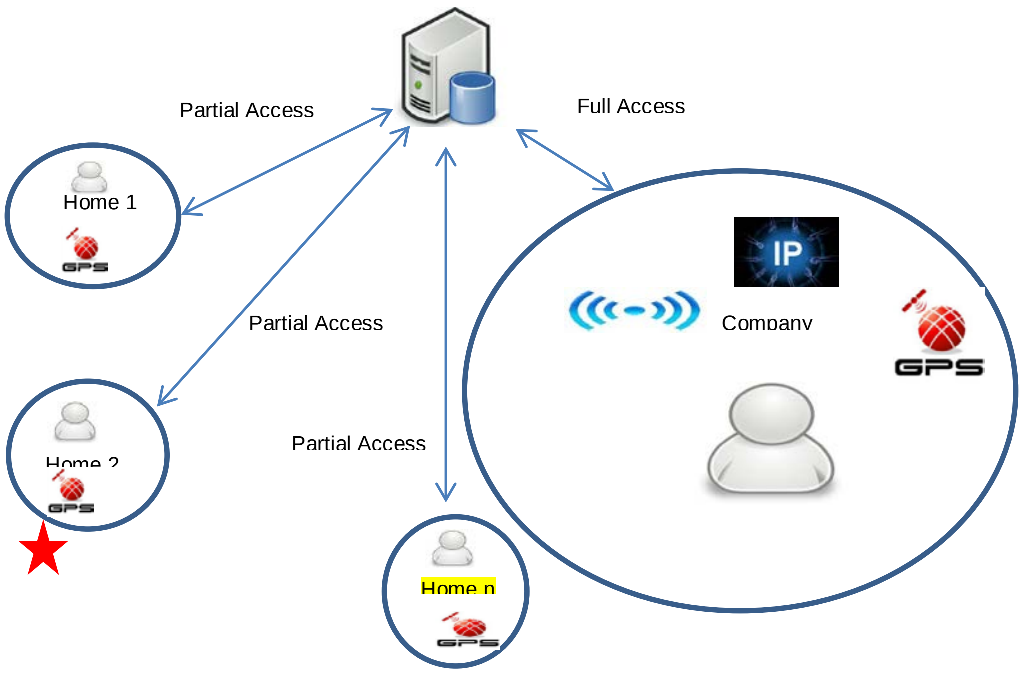

Fig.1 Scenario

staff during each session and comparing with corresponding details of the company. The staff is identified when they are accessing from home by comparing GPS latitude and longitude retrieved from mobile phone with the registered home location with company's administrator.

3.1 Architecture

The architecture comprises of a web portal to access the resources (a software) and a mobile application. User have to login to the portal first(primary authentication).

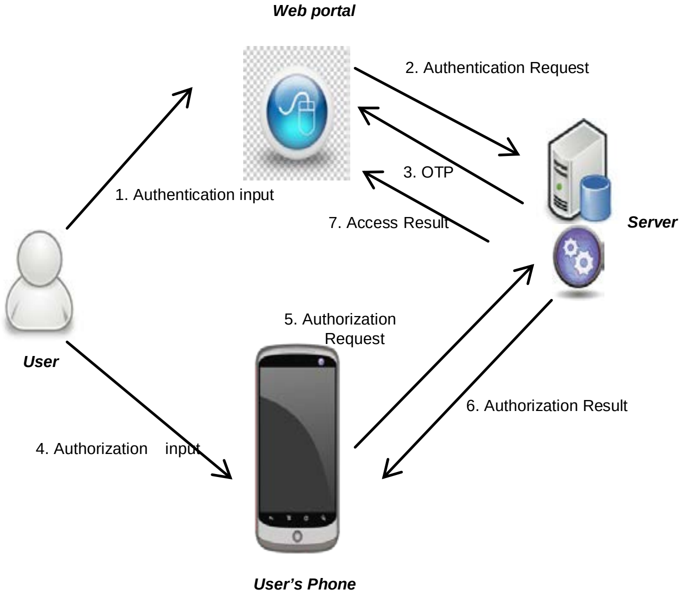

Fig.2.Architecture

On getting an OTP from web portal user have to proceed via mobile application (secondary location based authentication). Web server verifies the information obtained and provide the access result which will be displayed in the interface of web portal. The architecture is as shown in Fig. 2.

User here is the staffs who want to access the management software in web portal. Web Portal provide the GUI of software where staff have to login. User's phone holds the mobile application through which authorization takes place. Server contain the database for storage and web service for authenticating ,authorizing and verifying information retrieved from user's desktop and mobile transparently.

3.2 Messages

The architecture comprises of the following messages:

Authentication Input: User providing username and password.

Authentication Request: Forward username and password for verification to web service in server along with the transparently retrieved IP address of the device used to access web portal.

OTP: Server produces this token which is unique for each session and is displayed on GUI of web portal.

Authorization Input: This include username, password and OTP displayed on GUI of web portal and has to be entered by user on phone.

Authorization Request: This include OTP latitude and longitude if user accessing from home plus public IP address of phone and BSSID if user accessing from company.

Authorization Result: If necessary information for verification is received at server, then web service send a notification to user's phone.

Access Result: If user is identified as being accessing the web portal from company, then full access is granted. Else if from home then partial access is granted. Access is denied from all unregistered locations.

- All communications are signed and encrypted using RSA PKCS. It makes use of the concept of public key encryption. RSA PKCS include signing (Private key) and verification (Public Key), encoding and decoding, encryption (Public key) and decryption (Private key).These three steps make the communication more secure.

3.3 Implementation

3.3.1 Web

Login by using username and password through web portal. An OTP will then be displayed on portal after authentication. User will then be instructed to proceed via mobile.

3.3.2 Mobile

Enter username and password. On successful login user is asked to enter OTP displayed on portal in mobile API. Meanwhile in background, information such as IP address, BSSID of Wi-Fi, latitude and longitude is retrieved and placed in object of Shared Preference.

1. IP address:

Public IP address of the device(mobile phone) is obtained by including link http://ip-api.com/json in HttpGet() as shown in Fig.3

```
HttpGet httpget = new HttpGet("http://ip-api.com/json");
```

Fig. 3.

The value returned will be JSON. Example :{"status":"success","country":"India","countryCode":"IN","region":"13","regionName":"Kerala","city":"Thrissur","zip":"","lat":"10.5167","lon":"76.2167","timezone":"Asia/Kolkata","isp":"BSNL","org":"BSNL","as":"AS9829 National Internet Backbone","query":"117.216.85.89"}.

2. WiFi BSSID:

BSSID of WiFi in mobile phone is obtained with the help of WiFi Manager system by invoking the command *getSystemService(WIFI_SERVICE)* as shown in Fig.4.

```
WifiManager
wifiManager=(WifiManager)getSystemService(WIFI_SERVICE);
WifiInfo wifiInfo = wifiManager.getConnectionInfo();
 wifibssid=wifiInfo.getBSSID();
```

Fig. 4.

3. Latitude and Longitude:

```
gps = new GPSTracker();
if(gps.canGetLocation()){
double latitude = gps.getLatitude();
double longitude= gps.getLongitude();
lat_str=String.valueOf(latitude);
lon_str=String.valueOf(longitude);
}
```

Fig.5.

On submitting OTP all information retrieved gets signed and encrypted using RSA PKCS algorithm and passed to web service for further process.

3.3.3 Web Service

Verify username and password passed from mobile phone. After decrypting, the received parameters are verified. If parameters are properly received then an authorization successful notification is send to mobile.

3.3.4 Web

After successful authorization from mobile phone public IP address of the device running web portal is obtained by using curl as shown in Fig.5.

```
$url="http://ip-api.com/json";

$ch = curl_init();

curl_setopt($ch, CURLOPT_URL, $url);

curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);

$result = curl_exec($ch);

curl_close($ch);

$comp_ip=$result;
```

Fig. 6.

On clicking OK button of the web portal interface obtained after login, verification occurs. If no parameters are received from mobile , user is instructed to reauthenticate from mobile via web portal. If retrieved latitude and longitude fall in the range of 2 kms from registered home location, then partial view of the software is the access result. If retrieved latitude and longitude fall in range of 5 kms from company's location provided the IP and BSSID obtained also matches the corresponding known values, then full view of the software is the access result.

Here range (say d) is introduced for ensuring location accuracy. This is done by using Haversine formula as shown in Fig.6.

```
earth_radius = 6371 km;
diffLat = deg2rad(CL – FL);
diffLon = deg2rad($CLo - $FLo);
o = sin^2($diffLat/2)  +
        cos(deg2rad(FL)*cos(deg2rad(CL)* sin^2(diffLon/2);
g = 2 * asin(sqrt(o));
d= earth_radius * g;
CL/Lo:CurrentLatitude/Longitude
FL/FLo:FixedLatitude/Longitude(Home/Company)
```

Fig. 7.

3.4 Experimental Setup

The experiment was done designing software for project management in companies. This software enable administrator to divide a project into tasks, allotting tasks to staff, monitor staffs, projects and tasks progress. Through this staff can know his assigned tasks, his co-worker in project, files related to project, upload his homework to get rewards. Based on location, GUI of the software changes limiting access. Moreover Staff get an increment if he took extra time at home to do the work assigned**.**

4 Conclusion

The new generation IT professionals are very passionate in working. People willing to work from home are increasing day by day limited by the geo-fenced software. Moreover people who took extra time at home are not getting any rewards in the present system .The proposed idea overcome such limitations. It gave way to creation of more passionate professionals.

Here public IP and BSSID are provided by trusted entities. So there is no issue of spoofing. Even GPS values obtained from IPhones cannot be spoofed. But there is an issue of spoofing GPS values in Android phones. Here security lies in the fact that staff is also a trusted entity who declare that application won't be misused. So future work is to ensure no spoofing of location in Android phones as well.

Acknowledgement

Our sincere thanks to all who helped in developing this concept that include mainly Mr. Rineez Ahmed N, CTO of Livares Technologies Private Limited and Mr. Manoj ,Software Developer of Aiko InfoTech and Mr. Jinav Shah, Software Engineer at Indus.

References

[1] Denning D and Macdoran P, "Location-based Authentication: Grounding Cyberspace for better Security ," *Computer Fraud and Security*, pp. 12–16, 1996.

[2] YounSun Gho, L. Bao, M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol," Mobiquitous, Third Annual International Conference on Mobile and Ubiquitous Systems, Networking, and Services, pp.1-7, 2006.

[3] Takamizawa, H. & Kaijiri, K., "A Web Authentication System using Location Information from Mobile Telephones," Proceedings of the IASTED International Conference Web-based Education (WBE 2009)

[4] S. von Watzdorf and F. Michahelles, "Accuracy of positioning data on smartphones," pp. 1–4,2010

[5] Robert W. Reeder and Stuart Schechter," When the Password Doesn't work: Secondary Authentication for Websites", IEEE Usability of Security,pp-43-49,2011

[6] Ananya S and Venkatalakshmi B," Location based Intelligent Mobile organizer",IEEE,pp-488-491,2011

[7] Feng Zhang,Aron Kondoro,and Sead Muttic," Location-based Authentication and Authorization Using Smart Phones," *IEEE 11th International Conference on TrustCom*, pp. 1285–1292, 2012.

[8] Shraddha D. Ghogare,Swati P.jadhav,Ankita R.Chadha and Hima C. Patil," Location Based Authentication: A New Approach towards Providing Security,"IJSRP,vol.2,no.4,2012.

[9] Salem M and Deva B, "3rd Party geolocation messaging: A Positioning Enabled Middleware for Realizing Context-Aware Polling," *IEEE International Conference(Mobilware)*, pp. 100-109, 2013.

[10] Prabhakaran K, Kumar N.R,Puniha G and Asmi S,"A novel approach of geofencing and geotagging system based sea border identification using embedded system," *International Conference ICCTET*, pp. 338–341, 2013.

[11] Cardone G, Cirri A , Coradi A and Foshini L, "Crowd sensing in Urban Areas for City-Scale Mass Gathering Management: Geofencing and Activity Recognition," *IEEE Sensors Journal* , vol. PP, no. 99, 2013.

[12] Tarnauca B, Puiu D,Nechifo S, and Comnac V, "Using Complex Event Processing for implementing a geofencing," *IEEE 11thInternational Symbosium on SISY* ,pp. 391-396, 2013.