

LOCATION BASED APP-ENFORCEMENT LOCK BASED ON GPS

A.AnithaAlice, M.Anupriya, Annie Nesa Chandra.L, Dr.L.Jaba Sheela

Student, Computer Science and Engineering, Panimalar Engineering College, Tamilnadu, India.

Student, Computer Science and Engineering, Panimalar Engineering College, Tamilnadu, India.

Student, Computer Science and Engineering, Panimalar Engineering College, Tamilnadu, India.

Professor, Computer Science and Engineering, Panimalar Engineering College, Tamilnadu, India.

ABSTRACT

Location Based Access Control (LBAC) is vital for preserving and maintaining confidential data where permission is provided only in the presence of a specified location. The main aim of Location Based Access Control is to provide the exact information to the right people at the right time provided only at the right place. The applications of Location Based Access Control includes secured access of information in banks where theft of confidential information can occur and in hospitals, institutions and in companies. It makes use of Global Positioning System (GPS) for finding the exact location. Location Based Access Control requires some infrastructure elements like Android mobile phone, communication network, Global Positioning System (GPS). This paper emphasizes on Android application "APP-ENFORCEMENT LOCK" which can find the exact location of the user using Global Positioning System (GPS) and in case of a restricted zone, then the applications to be blocked by the admin will be blocked and other applications can be accessed by the user. We have implemented the paper in the form of Android application and presented the results.

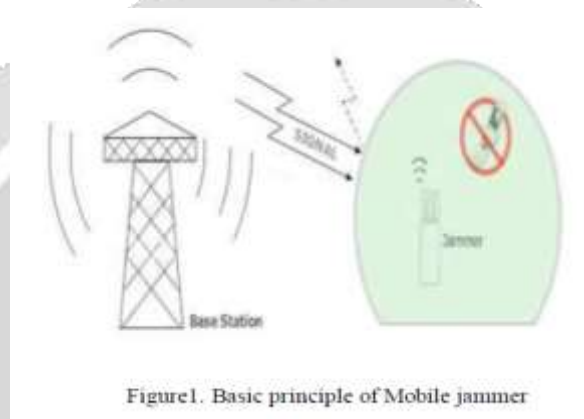
Keyword: - Location based access control (LBAC), Global Positioning System (GPS), Android, Context Based Access Control (CBAC), IOS (Iphone operating system)..

1. INTRODUCTION

Android, the Technology leader in the mobile phone era, has led a new successful way for the developers to develop new applications. Android a linux based Operating System (OS) is an open source operating system where any developer who is interested in developing a mobile application, can develop an application, that is third party development of application is allowed. Our paper focusses on security application which makes use of Android mobile due to its wide availability. Global Positioning System (GPS) is a navigation system which provides location information like latitude and longitude. In Location Based Access Control (LBAC), GPS plays a major role where the location obtained by the Global Positioning System (GPS) decides the privilege of application, (i.e) whether to allow or to block. Thus Global Positioning System (GPS) becomes the key component of Location based access control (LBAC) which differentiates the location. Mobile phones enables the users flexible to carry and due to the ease of mobility of the mobile phone, Mobile phones serves as the best platform for implementation. Thus turning our smart phone to smart location detector, which detects the access to the application. It can also be deployed in religious places where the usage of mobile phones is restricted by blocking the ringtone application once the user enters the place, thus the visitors are prevented from using mobile phone in the religious places.

2. EXISTING SYSTEM

The existing system are the Mobile Jammer and Android mobile phones. In mobile jammer ,it disables all the signals of the mobile phone in the area in which it is incorporated but disabling the signals result in complete isolation of services from the user which makes the user unaware of emergency situation. The jammer lacks in these areas, so the new system should be enacted such that only the unnecessary specified services should be disabled ,so that the user can use only the necessary services. The Android mobile phones use Permission Based Access Control (PBAC) in which the user accepts or permits the application to access the device's information ,contacts ,pictures etc at the time of installation. Declining the permission will prevents the user from installing the app. Android security is robust but at the same time the drawback is that the user will become the security decision maker. So ,Android does not provide any middle ground validation(allowing some permission and rejecting others).whereas IOS (Iphone Operating System)denies the access under all such circumstances which makes it highly robust and secured.



3 PROPOSED SYSTEM

In order to have a better control over the device capabilities by disabling certain application-privileges when the device is present in sensitive contexts or restricted zones, the mobile phone should provide configurable policies to the respective device owners according to the location. This feature when added to Android system, can make the system robust. Context Based Access Control (CBAC) mechanism for Android system set different configuration policies at different context, thus reducing the chances for hackers who intent to steal the confidential details. Through Context Based Access Control(CBAC) mechanism, users for example can set privileges for the device when the user is using the device at work and re-gain the device privileges automatically based on the context. The proposed system incorporates high level of security and efficiency for user access of devices. Thus APP-ENFORCEMENT LOCK provides the location specific services to the user by restricting the services by determining the geographical location using the Global Positioning System (GPS).

4 .WORKING

Context Based Access Control(CBAC) consists of

- Admin Login Module
- Location Positioning methods
- Android Permission Setup

4.1 Admin Login Module

The ultimate aim of this module is to allow a user and the server to negotiate a shared secret to authenticate the login for the user. Then the admin should store the Latitude and Longitude of the location which will be validated with the value obtained from the GPS.

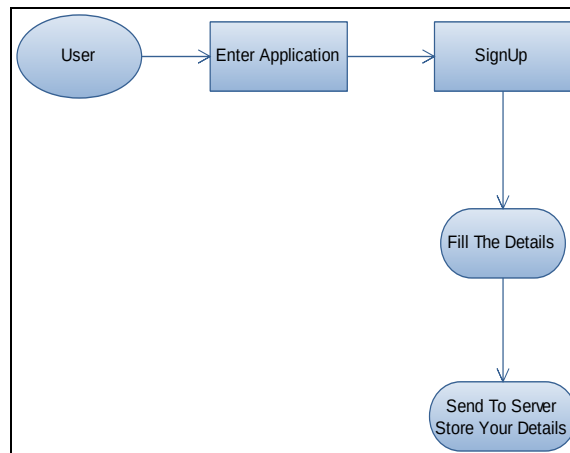


Figure 4.1.1.Admin login module

Admin module consists of login and password where the user is permitted to enter the right password. The password entered by the user is validated by the admin so that only the authenticated user is permitted to access the information.



Figure 4.1.2 start screen

In case if the correct password is not entered, then error message will be displayed to enter the valid username and password. Admin module is the first step in the Access initiation process which when entered correctly switch to next module.



Figure 4.1.3.Admin Validation Screen



Figure 4.1.4. Access Denial

4.2 Location Positioning methods

Global Positioning System is a navigation tool present in most of the devices which uses the signals from the satellite and finds the exact position of the device in terms of latitude and longitude. The Global positioning system (GPS) helps us in setting the configuration policies of the user's mobile in order to determine the location of the mobile phone. The Global positioning system (GPS) is a powerful tool which is used for many purposes like navigation, map-making, surveying, geo-tagging and even in military applications. The Global positioning system (GPS) receives the longitude and latitude values from the satellites which are revolving around the Earth. The mobile phones contain Global positioning system (GPS) receiver that uses the trilateration method in order to find the exact location of the place. Nowadays Global positioning system (GPS) has become an indispensable part of tracking which makes it highly significant. Tracking the location of the enemy warships are used in military

applications. Thus the application uses GPS Global positioning system in order to find the location details like latitude and longitude. In trilateration method, three near-by satellites are determined and a sphere is drawn around each satellite which intersects at two points possibly one point in space and other point on ground. Thus the exact location is the intersection of the point on the ground at which the three spheres intersect.

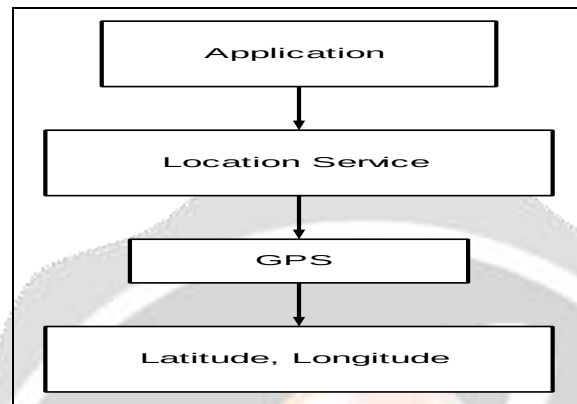


Figure 4.2.1 location detection flowchart



Figure 4.2.2. Displaying location from GPS

4.3 Android Permission Setup

The responsibility of Android Permission Setup is to find the privilege of the devices based on the location of the device. If the latitude and longitude values in admin's database and the value obtained from the GPS matches then the user will be allowed to access only the permitted services and the devices which has been blocked will display blocked screen. If the values doesnot match then the user can access all the services.

5. ARCHITECTURE DESIGN

The user once installed the application in the mobile phone must enter the password which will be validated by the admin and if it is valid, then the location details obtained from the Global Positioning System (GPS) will be checked

with the location details set by the admin in the database. If a match occurs, then the configuration policies set by the admin will be defined on the user's mobile phone and if the user tries to access the applications which are blocked by the admin, the user gets a blocked screen and other applications which are not blocked by the admin can be accessed by the user. This configuration policy is highly needed in order to incorporate security which the Permission Based Access Control (PBAC) system lacks. By this Context Based Access Control (CBAC), the user will be able to use the needed application according to the location. Example: The user cannot have access to use social networking applications in corporate offices or in institutions, whereas he can have access to chat or text anybody and once the user leaves the premises, the user gains the privileges to access all the applications installed in their mobile phones. In smart environments, the user must be able to differentiate the location automatically, so that it reduces the burden of the user. This Location Based Access Control (LBAC) is highly useful in smart cities where based on the location, the applications are restricted and regained which makes it highly efficient and significant.

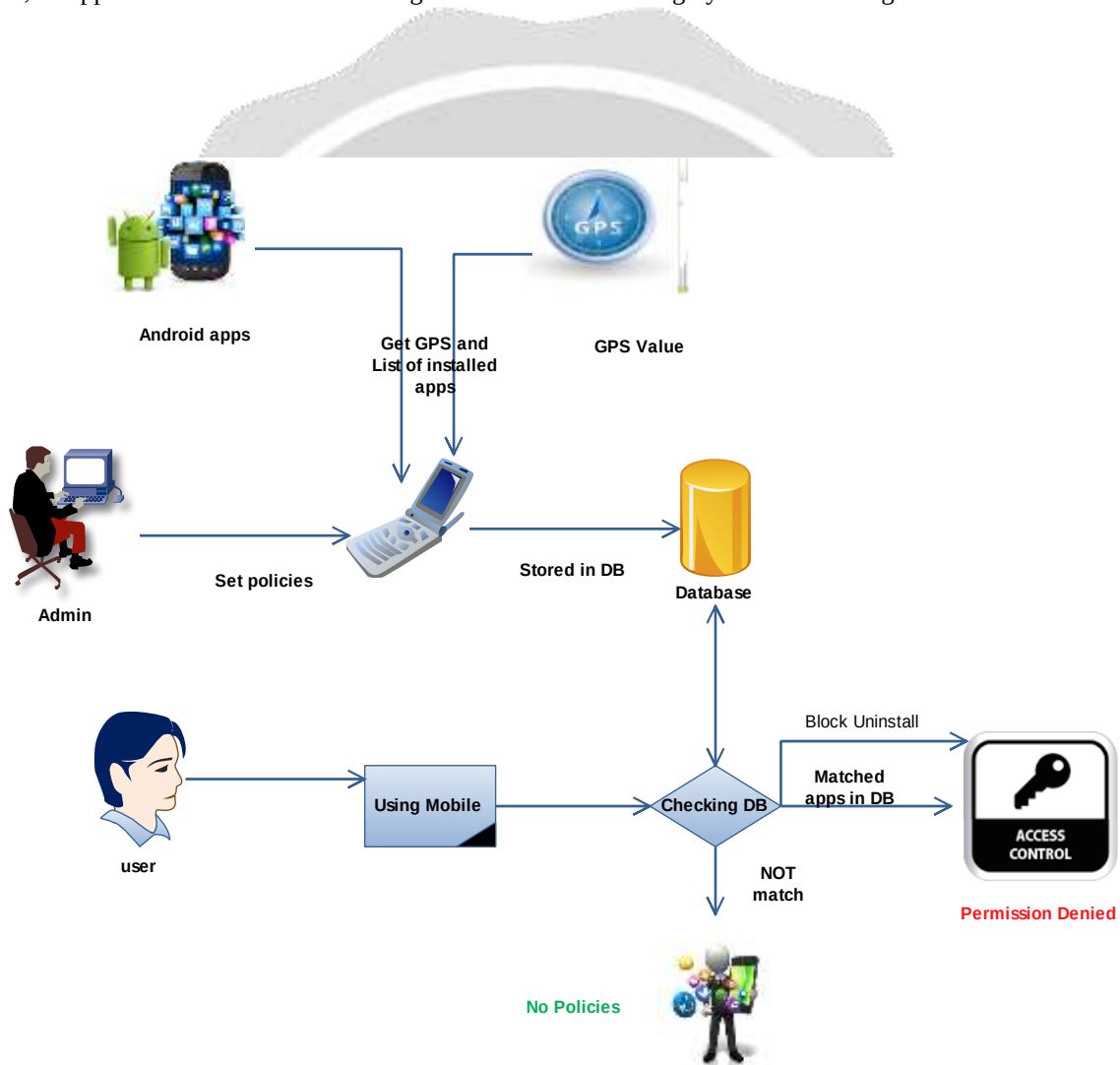


Figure 5.1.System Architecture

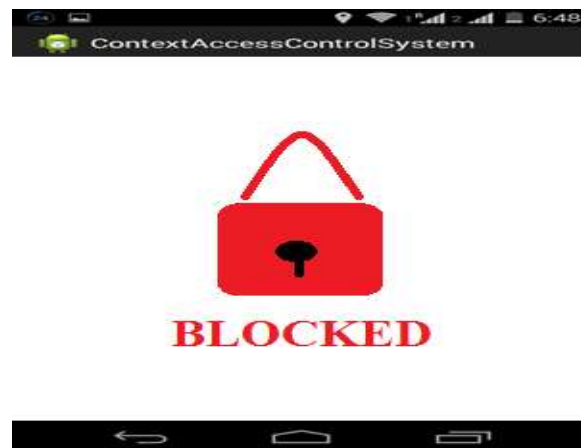


Figure 5.2 Access Blocked Screen

6.CONCLUSION

This paper has focused on Location Based Access Control(LBAC) which can be used in the places where confidential data should be maintained without any theft of data. Thus the paper has been successfully implemented as an Android application. The screenshots after implementing project has been shown. The Location Based Access Control(LBAC) which controls the access based on the location of the user is explained in this paper. Thus the confidential information is prevented from un-authorised access which is highly need in smart environment. This kind of access control helps in better maintenance of the information.

7.REFERENCES

- [1].Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, 9th USENIX Conf. Oper. Syst. Des. Implementation, 2010.
- [2]. Soundcomber: A stealthy and context-aware sound troja for smartphones, R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, 18th Annu. Netw. Distrib. Syst. Security Symp., Feb. 2011.
- [3]. Crepe: Context-related policy enforcement for android, M. Conti, V. T. N. Nguyen, and B. Crispo, 13th Int. Conf. Inf. Security, 2011.
- [4]. Location Based Services using Android Mobile Operating System, A. Kushwaha and V. Kushwaha, Int. J. Adv. Eng. Technol., vol. 1, no. 1, pp. 14–20, 2011.
- [5]. Enforcing Spatial Constraints for Mobile RBAC Systems, M. S. Kirkpatrick and E. Bertino, 15th ACM Symp. Access Control Models Technol., 2010.
- [6]. IEEE transaction on information forensics and security, vol 11, no 10, October 2016.
- [7]. Mobile phone signal jammer for GSM ,CDMA with pre-scheduled time duration using ARM7, International journal of science, enginnering and technology research (IJSETR), volume 2, issue 9, September 2013.
- [8]. www.HowStuffWork.com
- [9]. www.designerandroid.com