Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.499 – 505

LOCATION BASED ACCESS CONTROL AND THEFT MONITORING FOR ANDROID DEVICES

[1]Mr. M.Arun Marx, [2]M.Lahari Sri, [3]S.Manjusha, [4]B.Pragathi Dhakal

[1]Assistant Professor-I, Department of Information Technology, Prathyusha Engineering College, Chennai, India

[2, 3, 4] Student, Department Of Information Technology, Prathyusha Engineering College, Chennai, India

Abstract— The motivation for every location based access information system is: "To assist exact info at right place in real time with personalized setup and location sensitiveness". In this application location based access control we implemented the concepts to enable the mobile users to automatically change our profile based on our location and to identify their lost mobile by the help of advanced features and also we prevent the thief to use that mobile through this application. User can create profile and set the mode like (silent mode is off, Wi-Fi is on etc.) and our profiles will be changed automatically once user entered the location. The location will be gathered using Global Positioning System (GPS). Once the profile is created, it starts working without user interaction. This works using service which is a component that runs in the background. The service continuously gets the current sim number and check database number. If the sim number is mismatched then it will ask the user to enter the password which he/she registered earlier. The password entered does not match then the front camera opens immediately in hidden view mode and take the picture of that person and send that image with new sim number details and location to user's registered email id if internet exist else the text message sent to the registered mobile number. Once the wrong password is given a page will be booted repeatedly for every 5 seconds thus they can't even uninstall this application.

Index Terms—Location based Access Control, Theft Monitoring, and Android Devices

1. INTRODUCTION:

In this technology world everybody is using the smart phones. Smart phones is a cellular telephone with an integrated computer and has features such as operating system, web browsing and ability to run software application. Our phones profiles have to be changed for certain location. In certain places phones are meant to be silent but sometimes we forget to change the profile to silent mode which leads to trouble. The main aim of location based access is systematically change the mobile settings like (mode, Wi-Fi, Bluetooth etc). Create the profile and set the mode as (silent mode is on; Wi-Fi is off etc). We could create multiple profiles. While creating a new profile based on location, the device must present in the particular location. Once the profile is created, it starts working without user interaction and physical presence. This works using service which is a component that runs in the background without direct interaction with user. As the service has no user interface, it is not bound to the lifecycle of an activity. The location will be gathered using Global Positioning system (GPS). The GPS is a space based navigation system that provides location and time information in all-weather condition. This application needs a one-time registration like user name, password, mobile number, email id and alternate number to send the message if mobile lost. These details save in sq.-lite database. After the registration we could create multiple profiles and change the profile settings from any mobile number using message command with password. In case of having mobile missed in silent mode, we will not be able to find without ringtone sound. In this case we can change the mode to general or some other sound profiles from another mobile and find our mobile easily.

As well as there are lack of security and ways to keep that phones safe. To enable the mobile users to identify their lost mobile by the help of advanced features and also we prevent the thief to use that mobile through this application. Once we registered our details process will be running in the background using the concept called service. Using this concept every 5 minutes the sim number will be check by this application. If anyone stolen the mobile and try to change the sim, if the new sim is detected our application will check whether the newly inserted sim's number and previously registered number is same or not. If it is not, then it will ask the user to enter the password which he/she registered earlier. If the password matched then the user can able to use the mobile as usual. If the passwords doesn't match then the front camera opens immediately in hidden view mode and take the picture of the thief and send that image with new sim number details to user's registered email id if internet exist else the text message sent to the predefined mobile number. The location of the device is found using GPS. This particular application can also be hide by the user. Thus mobile theft monitoring is a useful application which helps us to track and find the device in an effective manner.

2. EXISTING SYSTEM:

In Existing System there is no application for profile changing system based on the locations. We have to change the profiles manually but if we want to change the profile based on the location is not possible. It is not possible to get the mobile information when we lost the mobile. Once we lost the mobile we have to complaint on particular police stations but it's not possible to get back that mobile or any information about the lost mobile. User cannot track the thief location or their sim details

DISADVANTAGES:

- We have to change the profile manually.
- Difficult to recover the missed mobile
- We cannot get any information about the lost mobile.
- We cannot get location information about the lost mobile.
- Third person can use the mobile.

3. PROPOSED SYSTEM:

The main aim of Proposed System is systematically change the mobile settings like (Mode, Mobile data, GPS, Wi-Fi, etc). The feature of the application is finding the missed mobile which is in silent mode through message with password.

Easily find out the missed mobile and get the theft mobile number. Once sim changed it asks for password if we doesn't give a correct password then front camera opens in hidden view mode and take the picture of the thief and send that image with new sim number and location details to user's registered email id if internet exist else the text message sent to the registered mobile number.

ADVANTAGES:

- Profile will be changed based on the locations.
- Easily find out the silent missed mobiles.
- User can get information about the mobile when we lost.
- User can get the Location Details of the particular mobile when sim changed.
- Third person cannot use mobile because of the app which we installed open automatically for every 5 seconds.

4. ARCHITECTURE:

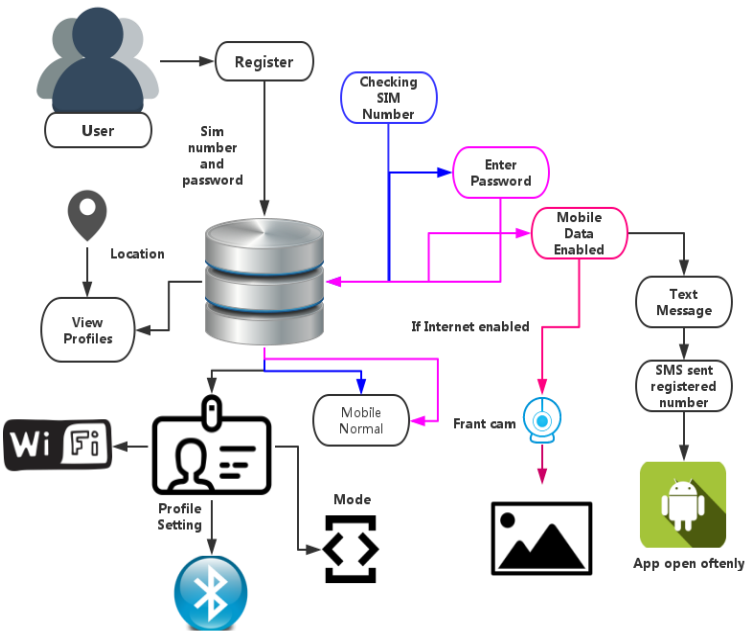

Fig 4.1 Architecture Diagram

5. MODULE DESCRIPTION:

5.1 ONETIME REGISTERATION:

In this module, the user needs to be registered with our application once app installed with his/her the details. The user gives the user name, password, mobile number, mail and the alternative mobile number.

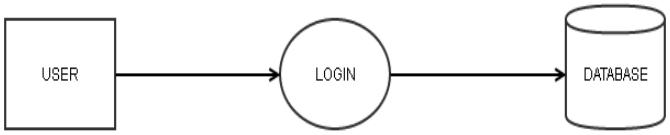

Fig 5.1 one time registration

5.2 CREATE THE PROFILE:

In this module, after signing up into the application the user profile is created and it is stored in the local database. The service runs in the background after completion of user sign up. User can change the profile mode based on the locate.

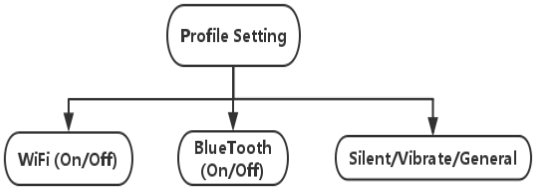

Fig 5.2 create the profile

5.3 AUTOMATIC PROFILECHANGER:

After getting that particular user's current location and the profile mode to that location it automatically updates the profile mode of the mobile. This profile change is based on location.

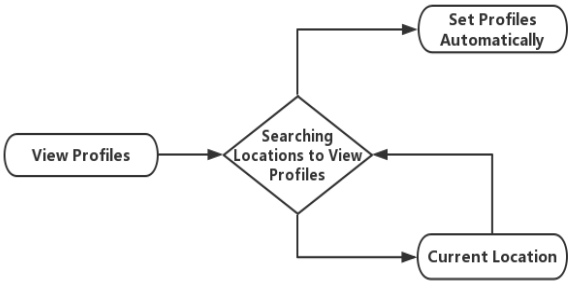

Fig 5.3 automatic profile changer

5.4 USER VALIDATION MODULE:

In this module our application will check the current sim number with the registered sim number. If it's matches means system shall allow the user. If it is not matches means it asks for the password which is user registered one.

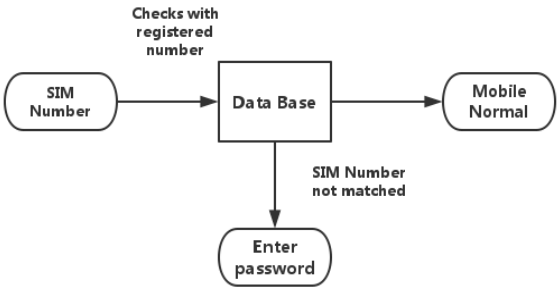

Fig 5.4sim validation module

5.5 DETAILS CAPTURING MODULE:

If the password also doesn't match means our app will check the internet and open the front camera then take the picture in hidden view mode so that thief cannot recognize the photo was taken against to him. Internet also not present means the newly inserted mobile number and details are to be send to registered mobile number.

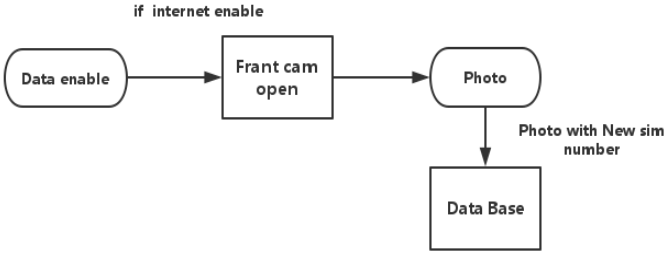

Fig 5.5 capturing hacker details

5.6 PREVENTING USER TO USE THE MOBILE:

If our application identified as the mobile was stolen by someone, then it'll let our application to open often for every 5 seconds. So thief cannot even uninstall our app.

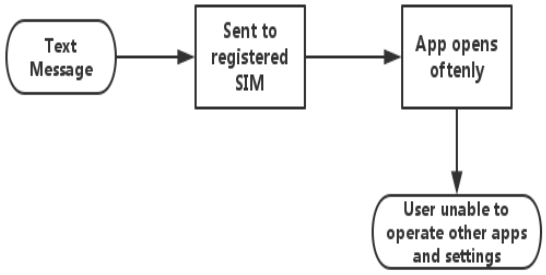

Fig 5.6 preventing hacker to use

6. CONCLUSION:

In this paper, we conclude that the user do not want to depend on anyone, by using in this application user can create profile and updating profile based on the location. While creating a new profile, the device must present in the particular location. We realized our application based on secure internet service and finding hacker details which is one of the most problems in hacking. Developing one of the new methods for secure the account and finding hacker details. In case of user missing their mobile hacker cannot the phone because it ask for a password when new sim card is plugged in. user can get image of the hacked user and the information of the hacker sim details and location details.

7. FUTURE ENHANCEMENT:

After going through the surveying, it can be gathered that there is a huge scope of application development in mobile domain. The proposed system can be further enhanced by making the following features in the application that enabling the application through which we can have backup of our phone data and also send the hacker details to the cops who are all nearby to the hacker location or send message to the nearby police stations to catch the hackers immediately.

REFERENCES:

[1]A. Kushwaha and V. Kushwaha, "Location based services using android mobile operating system," International Journal of Advances in Engineering and Technology, vol. 1, no. 1, pp. 14–20, 2011.
[2] S. Kumar, M. A. Qadeer, and A. Gupta, "Location based services using android," in Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications, ser. IMSAA'09, 2009, pp. 335–339.
[3] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in Proceedings of the 20th USENIX conference on Security, ser. SEC'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 21–21
[4] D. Kulkarni, "Context-aware role-based access control in pervasive computing systems," in SACMAT08 Proceedings of the 13th ACM Symposium on Access control Models and Technologies, 2008.
[5]W. Enck, M. Ongtang, and P. McDaniel," Understanding android security," Security Privacy, IEEE, vol. 7, no. 1, pp. 50–57, 2009.
[6] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies," in 22nd USENIX Security Symposium (USENIX Security'13). USENIX, Aug. 2013.

[7] M. Moyer and M. Abamad, "Generalized role-based access control," in Distributed Computing Systems, 2001. 21st International Conference on., 2001, pp. 391–398.
[8]W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in Proceedings of the 20th USENIX conference on Security, ser. SEC'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 21–21.
[9] J. Ligatti, B. Rickey, and N. Saigal, "Lopsil: A location-based policy-specification language."
[10]G. Zhang and M. Parashar, "Dynamic context-aware access control for grid applications," in Grid Computing, 2003. Proceedings. Fourth International Workshop on, 2003, pp. 101–108.
[11]C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati,and P. Samarati, "Supporting location-based conditions in access control policies," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security, ser. ASIACCS'06. New York, NY, USA: ACM, 2006, pp. 212–222.
[12]G. Edjlali, A. Acharya, and V. Chaudhary, "History-based access control for mobile code," in Proceedings of the 5th ACM conference on Computer and communications security, ser. CCS '98. New York, NY, USA: ACM, 1998, pp. 38–48.
[13] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad,and G. D. Abowd, "Securing context-aware applications using environment roles," in Proceedings of the sixth ACM symposium on Access control models and technologies, ser. SACMAT '01. New York, NY, USA: ACM, 2001, pp. 10–20.

