ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

ENHANCED USER DEFINED AUTOMATED ACCESS CONTROL MECHANISM FOR ANDROID MOBILE DEVICE

Vidhya M
PG-Scholar in Communication Systems
VELS University
Chennai, INDIA
vidhyachithu@rediff.com

***Abstract*—Android allows applications to communicate with the hardware devices (e.g. Camera, SD card, etc.) using its permission mechanism. While installing an Android application to android devices the application will ask a list of access permissions to permit installation. Since that user can only accept those permissions or else cancel the installation. At many case users can accept that even though a user doesn't like to accept the permissions. Once we accept the set of permission, then an application can access the shared resources at any time. So the developer can retrieve the user's sensitive data's like contact list, mail addresses, storages and so on. We developed an access control mechanism for both contexts based and non-context based. Context based will be used for grant/revoke the permission at a particular location / time. A non-context based access control mechanism will help for permanently grant/revoke the particular application permission. For both contexts based and non-context based access mechanism once user describes the permission policy, then next time which will be workingautomatically. No need to define at every time and every location. From this user can only allow their needed permission for a particular application. So that we can prevent from security attracts and theft users sensitive data.**

Keywords-- UDAC; CBAC; NCBAC; Access control mechanism; Permission.

I. INTRODUCTION

Android is one of the most famous and widely using OS in the world. Android's main feature is that the Linux kernel and open source. So that nearly 100 manufacture companies are developing android based manufacture currently android has more than 70% market share. Nearly 1300000 application percent in the official market Google play. EventuallyAndroid phone's has many resources like camera WI-Fi sensors etc.Example Samsung galaxy s5 is one of the top phone in android which have 10sensors.Every application has the set of permission list to access the mobile's resources. User should accept the whole set of permission they do not have any other option where else to cancel the installation. Ifthe useraccepts the application permission, then the application can access the device, shared resources at any time. From the permission request the developer can gather user's contact information, location information and many user's personal data's. So the developer taking this as the advantage and make armful for the users sensitive data. For example a user may go anywhere with his/her mobile. If the user has some application which can accessuser's location information means the application developer can access their location information via their application.They can track user and their data. For example angry birds area game which needs Network and location information. Actually which the permission to access the user location is not needed for the angry bird game.

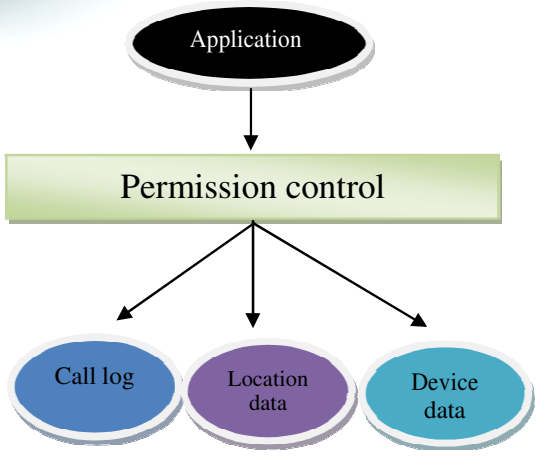
To avoid this type of problem we developed a mechanism to grant/revoke the application permission. We use two types of policy to provide an access control mechanism for permission system that is context based and non-context based.

A) Context based policy
B) Non context based policy

Fig. 1. Types of user data

To avoid this type of problem we developed a mechanismto grant/revoke the application permission. Weuse two types of policy to provide an access control mechanism for permission system that is context based and non-context based.

A) Context based policy
B) Non context based policy



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

The user should define the permission list, which should grant/deny for the first time. After defining the permissions which will be work automatic. User can define the permission by two ways that one is simply granting or revoke the permit for an application. In this type the permission is permanently granted/ revoked. The second way is that the user should define the permission by location based. A single permission may allow for multiple numbers of locations.

Another Example is that if user like to use one of the permissionsfor the application should be able access the device resources at a particular location and should not access the resources for another location.

A) Context based policy

The context is location and time. To determine location, we using WI-Fi as a primary and cellular tower, GPS. We useWI-Fi as a location component because it is better than other technique to determine the indoor location. We can identify the nearly located location by WI-Fi signal strength. In a same location, we may have, multiple number of WI-Fi access point to identify the nearby device we can use signal strength. This WI-Fi system find the nearby WI-Fi device. The list of WI-Fi is listed in our application which is already visited by a user.

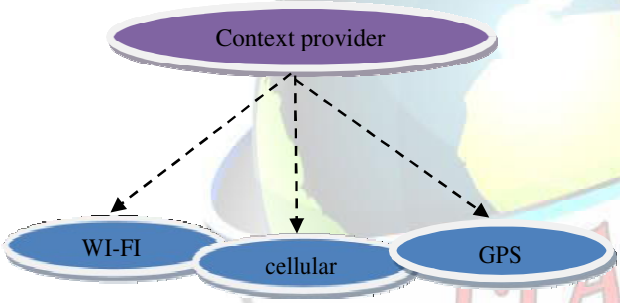


Fig. 2. Type of context

There are a number of visitsWI-Fi present in the device where the user visited the area. While user going to define the permission at that time he/she may grant or revoke the permission to number of visited WI-Fi which already presented on the device. If the userdefinesonce, then no need to define for every time for the same visited location the mechanism will be work automatically. But user should define access privileges for every non visited or new location.We developed Wi-Fi map for gathering accurate information. From the Wi-Fi map we can see where the Wi-Fi is actually located with graphical interface.

Another context is time based, from this user should define starting (ST) and ending time (ET) for disable or enable the particular application permission. More over once user define their permission policy which will be work automatically for next time. For Example if the particular permission from one of the application should access the shared resources at morning and night session should not. For this type of pillage access we using time context.

B) Non context based policy

Non context based policy is used for permanently grant or revoke the permission for the particular application. This technique very used when the user does not like the particular permission to disable / enable permanently. User no need to define the same access privileges to all context. Which is most effective and time reduced method. User can also use this policy for changing access privileges to different context by manually. This method is user friendly and no need of external sensors or hardware support.

In android we can install the application in two ways the first one is directly installed application to device from Google play which is a official app store of android. and another one is to install from ".apk "file.

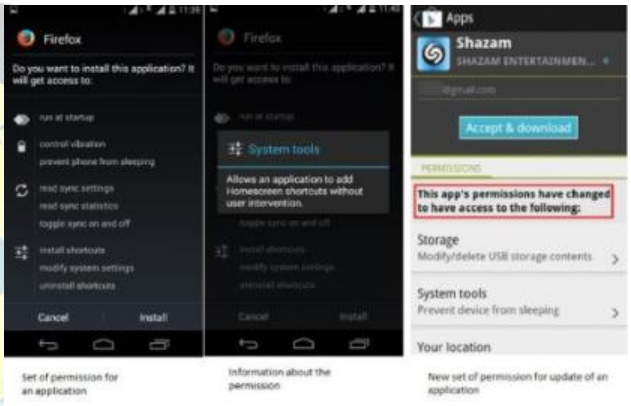


Fig. 3. Application installing from".apk" file.

We can install the application from both ways. There is more than 13lacks application available in Google play.Fromthat user should select which application they need. While installing application from Googleplay which ask access permission from user to access the device resources. on that time if user not compromise with application permission then he/she cannot reject the particular permission which user does not like. There is one only option to user is accept the list of permission or otherwise cancel the installation by pressing back button.In the similar way while installing application from sd card or any other storage device which asking several permission. User should accept the permission or else press the cancel button to cancel theinstallation. Once user accept the list of permission for particular application then which can access the device shared resources at any time after install the application. The application only can access the device shared resources which the application have already got permission from user.

There is another chance to get extra permission from user is that when the user going to update the particular application. Basically the application update is provide for fixing the bug and providing additional future to theirapplication. User can update their application in two different way that is manual

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

and automatic update. Automatic update is easy and dangerous to user, because a automatic update can update itself when the particular application have the new version without user knowledge. The risk present in automatic update is that the developer can give extra permission to their application when the application going update automatically then the permission's also accepted automatically. In manual update should manually update their application on that time the access permission will be shown to user they should accept or cancel the installation. After accept all the new permission from update the new permission will accept the device resources at any time.

II. EXISTING SYSTEM

Context-based policies are also a necessity for politicians and law enforcement agents who would need to disable camera, microphone, and location services from their devices during confidential meetings while retaining these resources back in non-confidential locations.

In this paper finding indoor location is not much efficient. Because they not use the Wi-Fi based location service. Or any other technique for indoor location.

Which is fully based on location based access control if user want to disable any permission or service's at permanently mean we can select every visited location even though we select every permission there may be chance to visit non visited location on that time we can configure the permissions' for the new location .otherwise the set of permission will access the shared resources in the new location. So we can't permanently disable the particular permission.

III. PROPOSED SYSTEM

Our proposed system will be both location and non-location based permission control system for mobile. We also developed for time dependent permission. So we can achieve the complete permission control system. The Enhanced user defined access control mechanism for Android. The mobile device is fully user defined permission control for that user may control the permission in following three methods. For example, set restricted privileges for device applications when using the device at work, and device applications may re-gain their original privileges when the device is used at home.

a) Particular App permission denies for particular locations. (Location based)
b) App permission denies with a particular amount of time. (Time based)
c) App permission denies by permanently. (permanent access/deny)

If the device has multiple number of application those are developed by the same developer, on this condition user need to give permission access/deny for any one application other application with same developer also can access the same access/deny app permission. This is because of the android system checks only the user ID to authenticate. To control the fake application with the same user ID we are going to use package ID instead of user ID.The user ID may be same for multiple application, but the package ID will not be same for every application. So our system will be given security for fake application.

Our system has three important phase that is follow:
A) Application Manager
B) Permission Manager
C) Policy manager

IV. SYSTEM ARCHITECTURE

A) Application manager

User can have any number of application which may be third party application or it own inbuilt application. And also a single can have large number of space .but our application should fetch all type of application to our application then only user can see the list of application and their permission list. Application manager is place where the list of installed application on the devise is display in the single application.

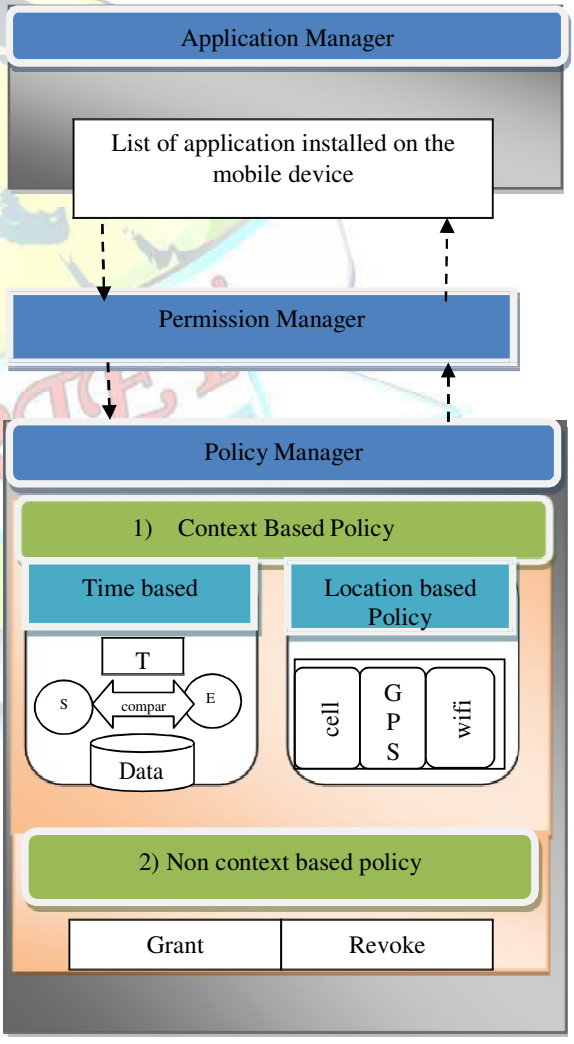


Fig. 4. System architecture

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

B) Permission Manager

Every android application has the set access permission to access the device shared resources. To show these permission to the user, we should display what all are the permission for the particular application to our application. First we dhow the installed application which user already installed on his/her device. Then the user should select the particular application then this list of permission for a respective application permission will be displayed. In this phase user can the permissions

C) Policy manager

Policies are initiated by the user who use the device if the policies are once generated then which will be work automatically. We using two type of policy like context based policy and another one is non-context based policy. For user preference they can choose any on from that policy's.

V. IMPLEMENTATION

A) Developing App Interface

Implementing user interface of an application by linear & list layout. Our UI three need parallel layer and list layer those are

1) List of installed application on the mobile device
2) List of permission which the application needed
3) Context based control
4) Non context based control

In this the "List of installed application on the mobile device "is an main layer whichAppear at front of an application. Other three layers are inside the main layer which will show when the users touch the particular application.

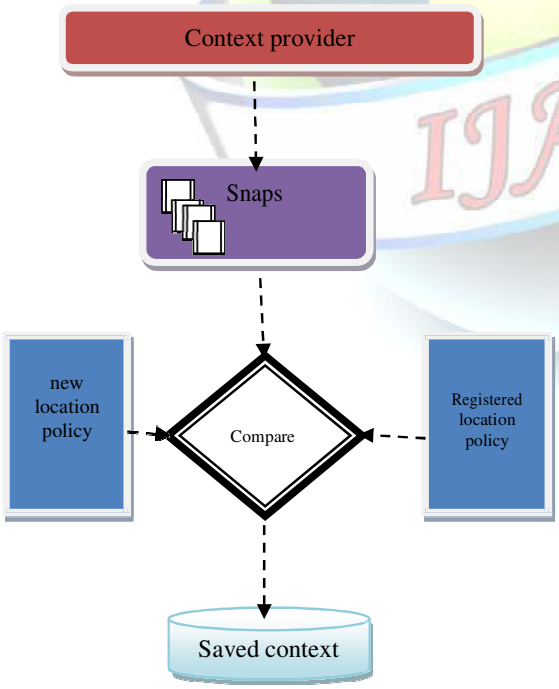


Fig. 5. Gathering new location

B) Gathering Installed Application

A user may installed many number of application. An application may have much number permission. But our application should fetch all the information about the list of application and their permissions. In this module we fetching all the predefined and third party application and list it in our application

C) Wi-Fi Map Accessing & Integration

For getting accurate indoor location we are using Wi-Fi technology for out project. This Wi-Fi system finds the nearby Wi-Fi device. The list of Wi-Fi is listed in our application which is already visited by user. While user going to define the permission on that time he/she can simply click the click box of particular location. A user can allow selecting multiple numbers of locations. This is user free. Once user define the permission access there is no need to once more which will be automatically work when the user move one location to another

D) Context based policy

The context is location and time. To determine location we using Wi-Fi as primary and cellular tower, GPS. We using Wi-Fi as location component because it is better than other technique to determine the indoor location. We can identify the nearly located location by Wi-Fi signal strength. in a same location we may have ,multiple number of Wi-Fi access point to identify the nearby device we can use signal strength. This Wi-Fi system finds the nearby Wi-Fi device. The list of Wi-Fi is listed in our application which is already visited by a user.

E) Non Location Based Policy

If user want to permanently grant/revoke a particular application permission mean they can achieve be non-context based policy. Particular permission is not needed for any location mean they no need to revoke the permission for every location. They can simply go for non-context based policy and just off/on the permission.

F) Policy Enforcement

Policies are defined by user .once the policy is denied by the user then which will we automatically enforced. Our application compare the user's current context if the current context is matched with any other context which user defined already mean which invoke automatically.

VI. PROJECTANALYSIS

And some of the application was crashing when the user revoke the particular application.For example consider the cricbuzz application which is used for live score update for cricket so which need internet connection to run the application unlikely if user if user revoke the "full internet access permission then the application will crash

The purpose ofthis experiment is to observe the Android device's battery consumption change when UDAC policies are enforced compared to when they are not.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

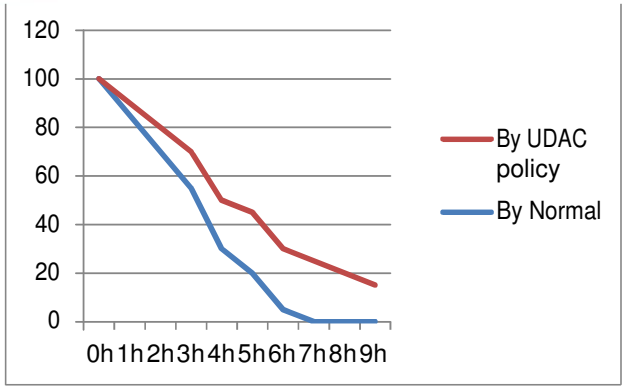


Fig. 6 .Battery drain difference

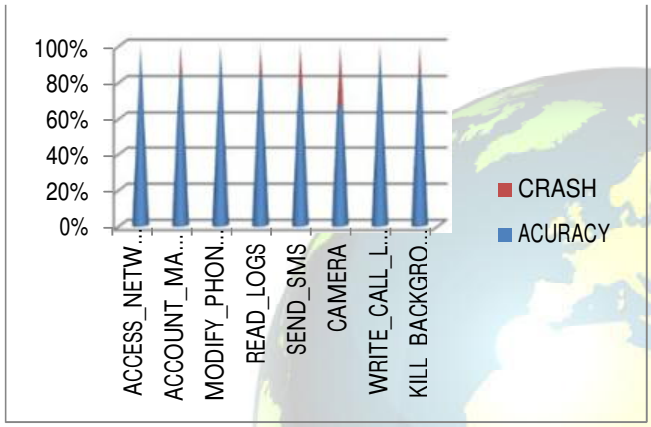


Fig. 7. Application crashing

VII. CONCLUSION

The location based access control mechanism for android device is in GRANT/DENY the particular application permission which based on location and time. Once the user defines the set of permission for an application they do not need to define once more it will be working automatically when the user move one location to another. We also developed non context based access control mechanism for GRANT/DENY the particular application permission permanently. So the user can simply GRANT/DENY (on/off) the permission or they can go for context based. We can avoid the fake application from the same user by using package ID instead of user ID. We using Wi-Fi for accessing indoor location also we used cellular and GPS.

REFERENCE

[1] Sangho Lee and Da Young. " A Novel Method to Avoid Malicious Applications on Android" International Journal of Security and Its Applications , July 2013.

[2] Wendong Xiao, Wei Ni and YueKhingToh. "Integrated Wi-Fi Fingerprinting and Inertial Sensing for Indoor Positioning" International Conference On Indoor Positioning And Indoor Navigation., August 2011

[3] Kangsoo Jung and Seog Park "Context-Aware Role Based Access ControlUsing User Relationship"International Journal of Computer Theory and Engineering, November 2013.

[4] ManavSinghal, Anupam Shukla "Implementation of Location based Services in Android using GPS and Web Services"International Journal of Computer Science Issues, , March 2012

[5] Milan Redzic, ConorBrennanand Noel E O'Connor "Indoor localisation based on fusing WLAN andimage data" International conference on indoor positioning and indoor navigation , Vol 6, NO 4, December 2011

[6] PanktiDoshi, PoojaJain,AbhishekShakwala. "Location Based Services and Integration of Google Maps in Android" International Journal of Engineeringand Computer Science, December 2014.

[7] SeemaVanjire ,UnmeshKanchan, Ganesh Shitole , PradnyeshPatil."Location Based Services on Smart Phone through the Android Application" International Journal of Advanced Research in Computer and Communication Engineering, September 2014.

[8] Amit Kushwaha ,VineetKushwaha "Location Based Services using Android Mobile Operating System" International Journal of Advances in Engineering & Technology, August 2011.

[9] Chenshu Wu, ZhengYang,YiyangZhao,Yunhao Liu "Footprints Elicit the Truth: Improving GlobalPositioning Accuracy via Local Mobility" IEEE INFOCOM April 2013.\

[10] KyungmiKim ,Hyunsook Kim " A Self Localization Scheme with Relay Nodes for Mobile Wireless Sensor Networks" Journal of Next Generation Information Technology, March 2011.

[11] Sonusharma, Manasiniakm, Nehaprabhukhanolkar&Kajalnirmal "Locations around me (ANDROID)" International Journal of Research in Engineering & Technology, 2014.

[12] G. Sujith, P.V. Vinod, M.S. Vinaya, S. Suresh Babu "Real-time vibration monitoring in Android smart phone using Location Based Service" International Journal of Innovative Research in Science, Engineering and Technology, April 2014.

[13] Kevin Benton, L. Jean Camp, VaibhavGarg "Studying the Effectiveness of Android Application Permissions Requests" Fifth International Workshop on Security and Social Networking, 2013.

[14] Muthumurugesan D, Nalini S, Vinodini R "Smart Way to Track the Location in Android Operating System" Journal of Computer Engineering, May 2013.

[15] Shu-Ping Lu, Kuei-Kai Shao, Yu-Nung Chao, uo-ShuLuo and Chi-Hua Chen "The Design and Implementation of Collaboration Service Integration Platform Based on Context-Aware Role Based Access Model" International Journal of Security and Its Applications , June 2014.