ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

Context Based Remote Access Control System Using Mobile Device for Educational Campus

Prof. Chaudhari A B[1], Gitanjali Yadav[2]

Assistant Professor, IT Dept, Govt. College of Engineering, Karad, Satara, Maharashtra, India[1]

BE IT Student, IT Dept, Govt. College of Engineering. Karad, Satara, Maharashtra, India[2]

Abstract: Now a day's everyone uses different mobile application. Also user can't control the activities perform by applications. Because of that security and privacy can't be maintain. So we face many critical issues. Context Based Remote Access Control System (CBRAC) is an android mobile application which is used to control data leakage as well as malicious activities. It is used to handle the sensitive data and privacy related issues of smartphone users. Through CBRAC user can set different policies according to their individual context and user requirement. This system is also beneficial for pre-defined area like colleges, educational institutes, hospitals etc. Network administrator can apply these different policy set for such pre-defined area.

Keywords: Context base remote access control system, android, security and privacy, data leakage, policies.

I. INTRODUCTION

In today's era, the number of smart phone users increasing day by day. A variety of general, personal, educational, banking, entertainment, health, safety and security purpose mobile application are available in market for mobile phones. These applications may useful in IT industries, hospital, educational institutes, and other work places for faster and simpler work.

But when user installed such type of mobile applications, important data is shared or transferred may become a critical issue [6]. The problem arises when mobile application shared private data and user mobile resources such as GPS that can be share your current location without users permission [1][3].

To prevent such activities user should have better control over mobile devices [5]. In pre-defined areas like college campus, the network administrator has to control over all user'smobile devices within campus.

A. Background:
Android operating system is derived from Linux based kernels and has enhanced support for security and privacy [8]. Android is design within a multi-layer security infrastructure, which provides developer a secure architecture to design their application [4].

B. Permission System:
An Android operating system contains permissions system which control and/or permit user and system application data and other relevant information. Each application declares permission listed in AndroidManifest.xml file at the time of installation and users have either select all permissions to continue the installation or cancel the installation [6][7].

II. EXISTING SYSTEM

Security for mobile operating system focuses on restricting application from accessing sensitive data and resources. In this misuse of data by malicious application may result in privacy leakage and also security may get compromise. In existing system extra hardware or location device are required and also user can set fake location [6]. Another problem is when application is installed in a mobile device it can either grant permission or cancel installation [2][4].

III. PROPOSED SYSTEM

We will be developing a CBRAC for android system that user set policies on their application and device resource. These policies set on application on the basis of user context [3]. We developing android application for college campus when user uses device at campus through the Wi-Fi or GPS administrator can set policies or restrict use some of the application on device [7][1].

When user exits that restricted area it can automatically re-gain their default setting. Basic need of our application is device connect to network using Wi-Fi or GPS.

A. Structure:
This system consists of an access control mechanism that includes access, collection, storage, processing and usage of context information and device policies. We will include some modules that are as:-

i. Context Provider:
It collects the location of device used by student or teacher in college campus using certain parameters (GPS, Wi-Fi) and stores it is in the database. So it is helpful when we check the constraints of any of the device that either of student or teachers in campus.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)
AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad
Vol. 4, Special Issue 4, January 2017

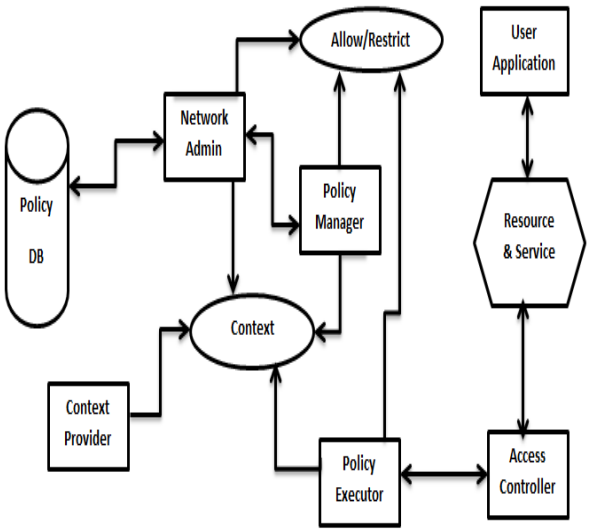

Fig. 1: Proposed Structure of system

ii. Access Controller:
Controls the authorization of application and prevents unauthorized usage of device resources or services. It enhances the security of device. It seem like an authorization system that used to stop the danger's application for user in college like using the gamming apps, social side that can be block using access controller.
iii. Policy manager:
It is used to create policies and assign to device application. It is of various types of the policy like application policy, hardware policy and Wi-Fi policy. That can be create by the policy manager it different policy for the student and teacher in college campus.
iv. Policy Executor:
It checks the configured policies set by the policy manager to either grant or deny access. It like check the constraints using stored data and received data of device that can be compared and then the appropriate policy can be apply on the device that is major work of the policy executor.
To trace the location of user using location sources such as GPS or Wi-Fi. These are stored into the database [5]. Then based on that information administrator can apply certain policies. In that the policy executor can be restrict or allow to device in campus on the context like they can restrict the social application, also can be restrict networking app that is GPS or Bluetooth, also can restrict the hardware resource like camera of mobile device. But for that the important thing is device connected with the system using Wi-Fi if system is not connected then admin can't be apply the constraint on the device. So Wi-Fi is the basic input for the system.
1. Access Network State:
In that policy administrator check that the device in the restricted zone or not if they found the device is in the restricted zone then they check the device connect with the any other device using networking application like Bluetooth and Wi-Fi. Then they disable that type of application so device is not connected with the other device.
2. Access Application State:
In that policy admin check that state of the application that install in the device just like the WhatsApp, Hike, Facebook etc. so the device restricted from the social networking application. Advantage of that is the device does not share anything with any device so it also provides the security form the data share.
3. Access Web State:
Access web state is used for the check the state of that device it used any of the web browser for surfing a data on the internet. That thing is also restricting on device so the location or any other malicious activity is not performing by the user using the device on the internet browser.
4. Access Wi-Fi State:
Wi-Fi state is the key thing in that application because without the Wi-Fi any of the networking operation is not perform. So when the device connected one to the system then they not be able to disable the device Wi-Fi using that admin is able to access the device privileges.
5. Send SMS:
That policy provides you to disable the SMS service application as well as the system SMS application so it only the calling system is available for the communication to the user.

Also we can provide other policy like the hardware policy that can be able to disable the hardware of the device like the device camera. Also we can provide the advance feature in the policy like some device that not support to android like apple I-phone using IOS system for extended version of application.

B. Technical Specification:
i. Hardware Requirement:
System - Pentium IV
Hard Disk - 40 GB
RAM - 512 MB
Monitor - VGA
Mobile - Android
ii. Software Requirement:
OS - Window XP, 7
Language - Java 1.7
Tool Kit - Android 2.3 above
IDE - Eclipse
Database - MySQL

IV. LITERATURE SURVEY

Bilal Shebaro et. al. [1] proposed that the data leakage and privacy compromised in smartphones in the android smartphone we install various applications that share our personal data [1]. That is harmful to us author thought that they also share our location and other thing like our social surfing data. That dangerous for the user prospective so author suggested that the we can modify the android operating system because that is the open source operating system any one can be modify the android OS according to their requirement so with help of the Linux operating system we can modify the android OS so that can be like

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

that user can be grant or deny the permission to any of the android application so the leakage of data, privacy and security maintain by user itself. But now days android OS give all permission to the every application if user not allows to get all permission then they can't install the application. A. S. Meenatshi et. al. [2] suggestedthat the android OS is design using the Linux kernel so if we modify the android that can be possible using Linux OS in that the Linux kernel operates each operation as process and provide the PID that is process id to each and every process that can be handle by the Linux kernel. Every Android application is composed of four essential Components: Activities, Services, Content Providers, and Broadcast Receivers. An Activity defines an application's user interface. The Service component is designed to be used for background processing. Android is designed with a multi-layered security infrastructure, which provides developers secure architecture to design their applications [4]. Each application declares the permissions listed in its AndroidManifest.xml file at the time of installation. Application developers that need access to protected Android APIs need to specify the permissions they need in the AndroidManifest.xml file which, if inaccurately assigned, can increase the risks of exposing the users' data and increase the impact of a bug or vulnerability.

V. EXPERIMENTAL RESULT

1. Menu Window:

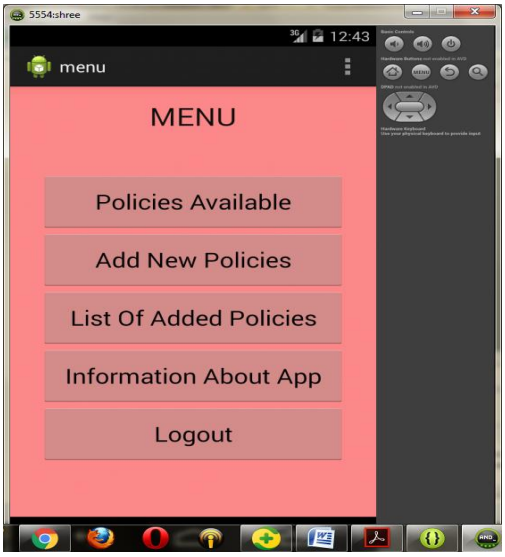

Fig. 2: Main menu

In that window provide the four tab. In first that show the available policy that can be apply by user also if the user wants to create new policy as their requirement using second tab that is add new policy. Using the third tab user can check under which policy which of the restriction is applicable. That is only provide the information not any of modification is made in that tab. In forth of the tab its provide the information regarding the application. And last tab is for the log out form the application.

2. Policy Window:

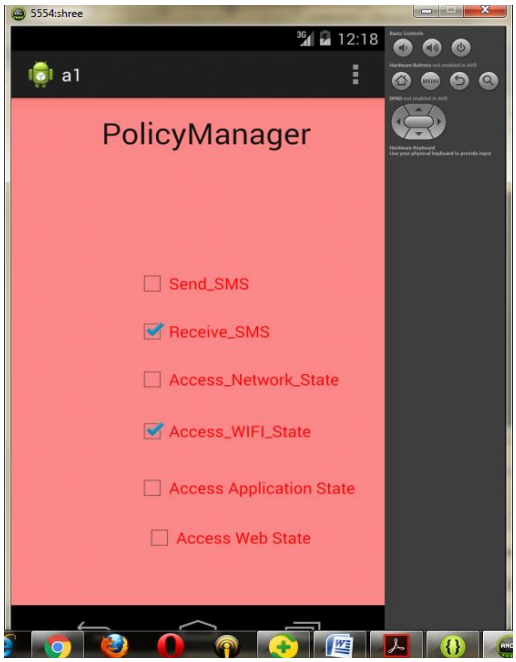

Fig. 3: Display of policy manager

VI. CONCLUSION

We will develop an android application on CBRAC for mobile devices used in college campus. This will help to restrict the malicious data and allow system to access the specific data and or resources based on user context in campus. It also set configuration policies over their application and services at different context. We will also develop the network administrator for college campus that will access to only specified application and other application may disable when user in college campus.

REFERENCES

[1] Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino, "Context-based Access Control Systems", IEEE Transaction on Dependable and Secure Computing, Volume:12, No:2 April 2015.

[2] Sumedh P. Ingale, Sunil R. Gupta, "Security in Android Based Smartphone", International Journal of Application or Innovation in Engineering & Management, Volume: 3, Issue: 3, March 2014.

[3] Ms. Nisha Rajan, Ms. Nalini Preetha R, "Managing Context Based Access Control Systems for Mobile Devices", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3, Issue: 12, 2015.

[4] A.S.Meenatshi, M. B. Prasanth Yokesh, D. Rajini Girinath, K. Amsavalli, "Android – Access Privilege: Integration of Multi Access Control System", International Journal of Innovative Research in Computer and Communication Engineering, Volume: 3 at Chennai, 2015.

[5] Dave Smith and Jeff Friesen, "Android Recipes: A Problem-Solution Approach", Second Edition, Apress Access Publication.

[6] "Android Security Overview" at: http://source.android.com/devices/tech/security/index.html

[7] Nikolay Elenkov, "Android Security Internals", First Edition, No Starch press Publication.

[8] "Android Architecture" at: https://www.tutorialspoint.com/android/android_architecture.html.