Effective Secure Mobile Profile Creation Using Virtualization

Dr. T. R.Saravanan[1], Dr. G. Nagarajan[2], Dr .R. I. Minu[3]

[1]Assistant Professor, Dept. of CSE, SRM Institute of science and Technology, Kattankulathur, TamilNadu, , India

[2] Professor, Department of Computer Science and Engineering,Sathyabama Institute of Science and Technology,Chennai,India

[3]Associate Professor, Department of Computer Science and Engineering,SRM Institute of Science and Technology,Chennai,India

[1]saravanantrcse@gmail.com,[2]nagarajanme@yahoo.co.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Smartphones allow end users to perform several tasks while being on the move. As a consequence, end users require their personal smartphones to be connected to their work IT infrastructure. In the smartphone domain, the Android OS is by far the most popular platform with major market share. More and more companies nowadays provide mobile versions of their desktop applications. As a consequence, end users require their personal smartphones to be connected to their work IT infrastructure. In the smartphone domain, the Android OS is by far the most popular platform with major market share. More and more companies nowadays provide mobile versions of their desktop applications. Company confidential data should be stored in a separated space of the mobile storage. Due to Improper maintenance of location and activity manager the data there are data sharing, data leakage and data loss between different user profiles. In proposed work each profile details can be stored externally. The External Storage makes the directory for the each profile which can be used to store the information of the profiles which outperforms all the issues in all Existing technologies

Keywords: *Virtualization, Profile rules ,Location update*

1. Introduction

Cell phones permit end clients to play out a few errands while being moving. As an outcome, end clients require their own cell phones to be associated with their work IT framework. In the cell phone space, the Android OS is by a long shot the most famous stage with 82 percent piece of the overall industry. An ever increasing number of organizations these days give portable forms of their work area applications. A few gadget makers are in any event, following this pattern by creating cell phones ready to deal with two supporter distinguishing proof modules (SIMs) simultaneously. Organization secret information should be put away in an isolated space of the portable stockpiling. Much additionally stressing is the quantity of genuine applications gathering and spilling information that are not carefully essential for the capacities the applications promote to clients. This postures genuine security worries to touchy corporate information, particularly when the standard security systems offered by the stage are not adequate to shield he clients from such assaults.

By methods for virtualization[2] it is conceivable to actualize on the cell phones. Despite the fact that virtualization is very powerful when sent in undeniable gadgets (PC and Servers), it is still too asset requesting for installed frameworks, for example, cell phones. Google android is a Linux-based portable stage created, and the greater part of the android applications are customized in Java and accumulated into a custom byte-code that is controlled by the Dalvik virtual machine. Android applications are assembled consolidating by any of the accompanying: Activities, Services, Broadcast Receivers and Content suppliers. Android joins two degrees of authorization, Linux piece level and Application system level.

When associate degree unauthenticated action is performed by the user suggests that, the protection profile won't be accessible. The administrator can handle the placement management details. Once the Outer-Corporate location[9] is known by the admin, then the permission of access are done supported the executive definition to your company profile.Corporate knowledge and apps can be separated from personal knowledge and apps at intervals one device and notification sends to the admin whereas shift to the company profile. It primarily concentrates on the isolation between the applications running on the sensible phones. It provides associate degree abstraction for separating knowledge and apps dedicated to totally different contexts that square measure put in in a very single device.

2. Related work:

Yury Zhauniarovich[1[proposed a MOSES strategy based system for enforcing software isolation of applications and data on the android platform . In MOSES, it is conceivable to characterize particular Security Profiles inside a solitary cell phone. Every security profile is related with a bunch of strategies that control the admittance to applications and information. Profiles are not predefined or hardcoded, they can be indicated and applied at any time. One of the primary attributes of MOSES is the dynamic changing starting with one security profile then onto the next. Risk of leakage and sensitive information transfer can be highly reduced.

C.Gilber[3] proposed an Android leaks mechanism to avoid data leakage when mobile applications have access to this growing amount of sensitive information, they may leak it carelessly or maliciously. Android operating system provides a permissions-based security model that restricts an application‟s access to the user‟s private data. However, it is not clear to the user how sensitive data is used once the application is installed. To combat this problem, we present AndroidLeaks, a static analysis framework for automatically finding potential leaks of sensitive information in Android applications on a massive scale. AndroidLeaks drastically reduces the number of applications and the number of traces that a security auditor has to verify manually.

Jipeng Zhou and Zhengjun Lu [5] proposed a Secure Distributed Location Service (SDLS) conspire for MANETs where area of every hub was enrolled along a line and the area question was along a section in the lattice organization, public key framework checked a hub with self-marked endorsement during area administration action to accomplish an elevated level of security.

Karim El Defrawy and Gene Tsudik [6] defined the ALARM system to help mysterious area based directing in different dubious MANETS. Unknown Location-Aided Routing in Suspicious MANETs(ALARM) depends on gathering marks for building one-time nom de plumes recognize hubs at distinct areas. Alert system works with any gathering mark plot and uses any area based sending convention to course information between hubs.

William Enck[4] proposed an Android security model and endeavors to expose the unpredictability of secure application advancement. Android Leaks inspected these applications in 30 hours, which demonstrates that it is equipped for scaling to the undeniably huge arrangement of accessible applications. Android Leaks discovered 57,299 potential security spills in 7,414 Android applications, out of which we have physically confirmed that 2,342 applications release private information including telephone data, GPS area, WiFi information, and sound recorded with the microphone.

Exisiting Work

The point is tackling all the security related issues in this manner wiping out information sharing, information spillage and information misfortune between various client profiles. In the current works, the work and private profiles are coordinated into a solitary climate where there is probability of information sharing or information misfortune between the two. To keep away from these impediments, a reflection for isolating information and applications devoted to various settings that are introduced in a solitary gadget. The made sure about information and applications can be isolated from the individual information and applications inside a solitary cell phone. The Security Profile Manager holds the data connecting a Security Profile with at least one Contexts. Cell phones permit end clients to play out a few undertakings while being moving. In existing framework[11,12], No Communication introduction, henceforth the framework won't comprehend the information which must be perceived with non-upkeep of areas. To defeat this difficulties we go for proposed fill in as given in next segment

3. Proposed Work

A. Overview

To make Security Profiles on the smart phones, an alternate structure has been continued in this proposed framework. It predominantly focuses on the separation between the applications running on the advanced mobile phones. Organizations are happy to help representative claimed cell phones due to the expansion in efficiency of their employees especially during this COVID 19 lock down. One of the fundamental attributes of the proposed framework is the dynamic changing starting with one security profile then onto the next. The proposed framework will give an answer that could be actualized by methods for virtualization technologies.

The proposed framework will be more disengaged than the current framework and it forestalls the information in any remaining applications to segregation. Framework design documents will be investigated in the proposed system. When an unauthenticated activity is performed by the client implies, the security profile won't be reachable. The administrator will handle the location management details. When the Outer-Corporate location is distinguished by the administrator, at that point the authorization of access will be done dependent on the authoritative definition to your corporate profile. System configuration files will be analyzed in the proposed system. The system can vary the data from different storage areas. Security Profile Name attribute represents the Security Profile name where the policy is valid. The policy can be allowed, denied and allowed with rules. The user GUI will be more interactive, so that the user can easily define the rules by themselves[13,14].

B.Security Profile Creation framework

There are numerous difficulties in existing framework. As Pandemic situation is available work at home has been increased and corporate data security has become an important aspect. Data leakage in any form should be avoided. In the existing work there is improper maintenance of location and activity manager[10]. No Communication initialization, hence the system will not understand the data which has to be understood. The following Fig.1 illustrates the security profile creation framework

Employee hand set of a company has two profiles such as private and corporate profile. Private profile has his own private information, data and corporate profile has his official information and data's including the internet access to official information. A separate memory is allocated with security mechanism to avoid official data leakage in while working at home. Corporate rules and policies are linked to corporate profile. Location management is a mechanism to dynamic switch of profile to corporate and personal profile.

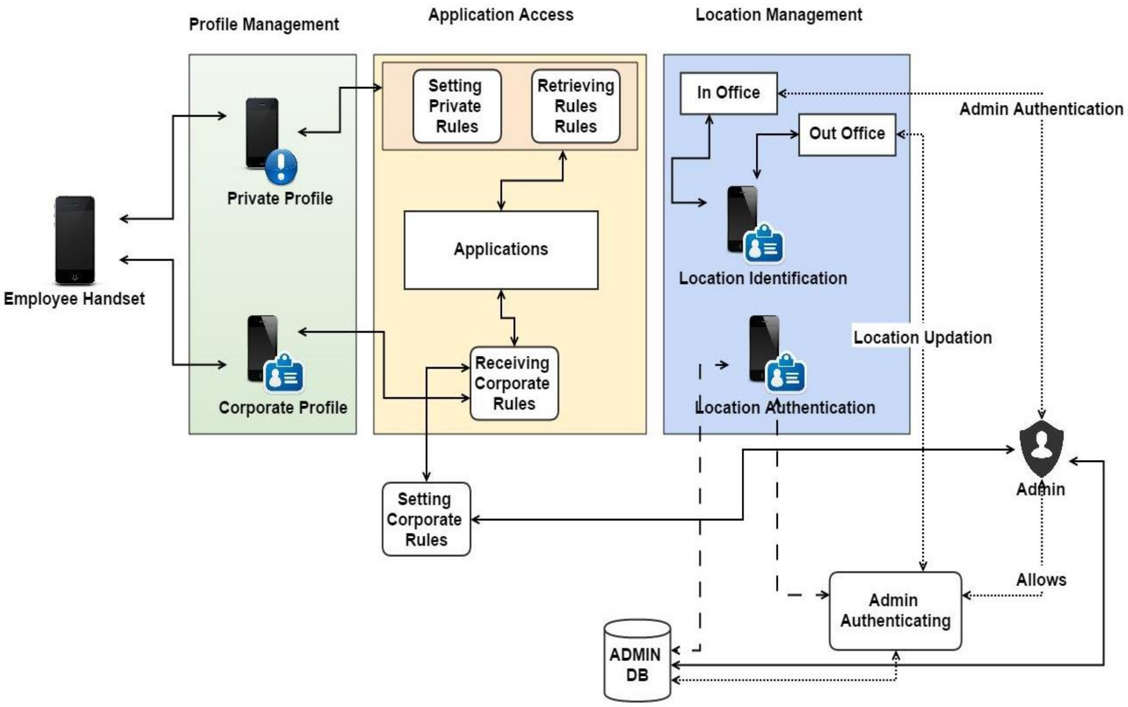


Fig.1. Security Profile Creation Framework

Corporate rules and policies are linked to corporate profile. Location management is a mechanism to dynamic switch of profile to corporate and personal profile. Authentication are performed while storing and retrieving data including location updates.

C.*User Identification*

The profile access corporate region will be enrolled to the client IMEI. Here, the portable IMEI number will be taken as a special part. The client ID stage is the significant period of the profile the board recognizing a client is a legitimate one or not. The client should be as of now enlisted by methods for his IMEI to get to the profiles powerfully. At first the worker will be permitted to choose the profile subsequent to getting enlisted to settle on his own decision. At that point during the determination of profile the relating profile rules will be characterized accordingly. User ID and access control have become a popularity include on cell phones in light of the fact that those gadgets are uncontrollably utilized by workers in enterprises and government organizations for business and store expanding measure of touchy information. The following Fig.2 illustrates security profile user identification

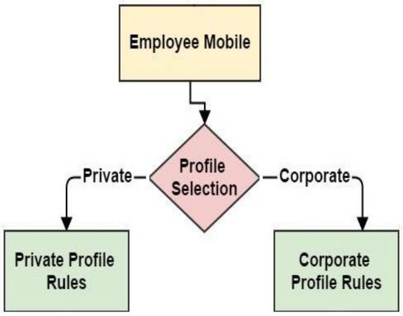


Fig.2. Security Profile User Identification

Here a client recognizable proof structure that empowers persistent and verifiable client ID administration for smartphone.Different from customary dynamic client confirmation and access control, which use accessibility of numerous sensors on the present cell phones and inactively use sensor contributions as wellsprings of client validation. It extricates sensor methodology subordinate client ID highlights from caught sensor information and performs client recognizable proof at background.This ID conjures dynamic client validation when there is a mounting proof that the telephone client has changed. Also, this framework utilizes a novel virtualization based framework engineering to forestall disruption of the foundation client recognizable proof instrument by moving it into an advantaged virtual area.

D. *Dynamic Profiles Management*

The profiles will be investigated and introduced on the gadget. The profile will be powerfully switchover dependent on the worker choice.

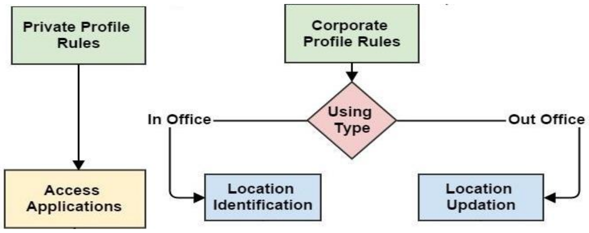


Fig.3. Dynamic Profile Management

The executive will keep up the application access subtleties. The profiles can be progressively handle the information. The following Fig.3 illustrates the dynamic profile management.In the Corporate profile there will be an area chief which advises and refreshes the client areas to the framework chairman. This area director utilizes GPS to find the client gadget, consequently it goes about as a GPS beacon to the system. Dynamic power the executives for different components of cell phones can be improved by considering the use history of the telephone. Cell phones contrast from embedded frameworks since human clients straightforwardly connect with them. In this work, we exhibit how unique power management can be improved by considering utilization history of the telephone client.

We utilize the cell phone screen and backlight as a model, and propose an energy the executives strategy that utilizes the historical backdrop of client cooperations as from the earlier to accomplish shockingly better energy saving. Current cell phones turn off the screen backdrop illumination after a fixed span that is configurable by the telephone client. We show how the ideal estimation of this stretch can be gotten from the user‟s previous history of cooperations with the phone. Large screens have become a true prerequisite fortoday‟s cell phones. Huge and splendid screens account fora huge segment of the energy interest on the telephones batteries.

To save energy cell phones turn off their screens when they are inactive. On all current cell phones a static timeout esteem is utilized to choose when to kill the screen; most regularly the client can design this break as a component of the phone settings. In this part we contend why finding the ideal worth of the screen rest break is certifiably not a minor choice.

E. Application Management

This focuses on application management, it provides a lower degree of control over the device, but a higher level of control over applications. The application access information for every profile are given during the time of installation. Mobile application management differs from mobile device management. Mobile device management solutions manage the down to device firmware and configuration settings and can include management of all applications and application data. App wrapping was initially a favored method of applying policy to applications as part of mobile application management solutions.

App wrapping sets up a dynamic library and adds to an existing binary that controls certain aspects of an application. For instance, at startup, you can change an app so that it requires authentication using a local passkey. Or you could intercept a communication so that it would be forced to use your company's virtual private network or prevent that communication from reaching a particular application that holds sensitive data. When an employee brings a personal device into an enterprise setting, mobile application management enables the corporate IT staff to download required applications, control access to business data, and remove locally cached business data from the device if it is lost, or when its owner no longer works with the company. Enterprise mobile application management has been driven by the widespread adoption and use of mobile applications in business settings. Most mobile devices out there in client land run some variant of Google's Android working framework. However, that doesn't mean the OS is ideal for the undertaking. At the point when it originally came out, the Android working framework was without a lot of big business highlights and the gadgets were outfitted towards shoppers.

F. Location Management

The location of the employee will be recognized and refreshed to the authoritative information base. In view of the areas, the administrator will acknowledge the solicitation from the worker. It's the motivation behind the area director to send the client solicitation to the framework chairman, to refresh the employee area to be either in-office or out-office areas. The area of the association is at first set up in the profile status which undoubtedly checks for the area of the client presence. The following Fig.4 illustrates the location management

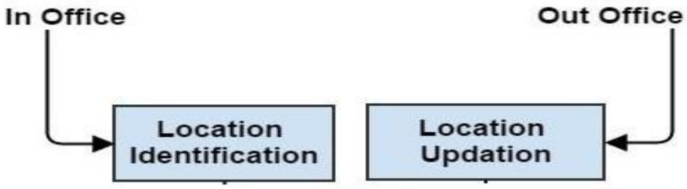


Fig.4. Location Management

There will be an area administrator which exists in the android structure, utilizes the gadget GPS to follow the client gadget by methods for empowering the far off admittance to the client. The area supervisor makes employments of area tracker to follow the focused on gadget. Select gadget the board benefits and design gadget enrolment settings. Send enrolment demands over the air utilizing SMS, email, or a custom uniform asset finder. Confirm against Active Directory, once pass code. Make and appropriate tweaked worthy use arrangements and EULAs. Register corporate and representative bring your own gadgets.

Apply or alter default gadget strategy settings. Find gadgets getting to big business frameworks. Influence existing Active Directory/LDAP and Certificate Authorities. Each association needs to see and control the cell phones entering their venture, regardless of whether they are given by the organization or part of a Bring Your Own Device (BYOD) program. MaaS360 cell phone the board (MDM) is the quickest, most thorough approach.

G. Administrative Operations

The corporate profile utilization will be broke down from the administrative perspective. The consequence of the investigation will be appeared as a report. Unauthenticated application[7] access will be stayed away from. Here the director utilizes the area supervisor to refresh the users in-office and out-office notification in the server database. Here the manager holds control of the whole framework.

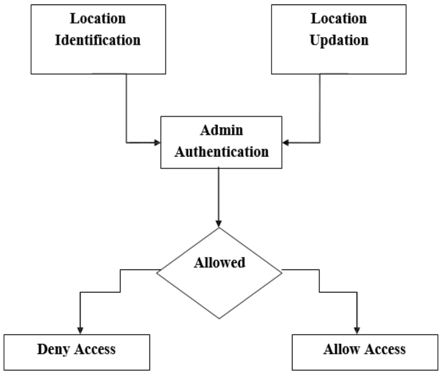


Fig.5. Administrative Operations

The above Fig.5 illustrates the operations performed in administrative operations.There will be an area chief used to refresh areas to the overseer. In the corporate profile the manager offers validation to the worker permitting him to get to or deny the corporate applications. If there should be an occurrence of out-office presence of the worker the client will be permitted or confined, which is conceded by the head for secure access.

F. Administrative Notifications

The notifications from the employee or the client will be accounted for to the more significant position authority or an administration. The director deals with all the notices and updations which remembers both for office and out-office client verifications.

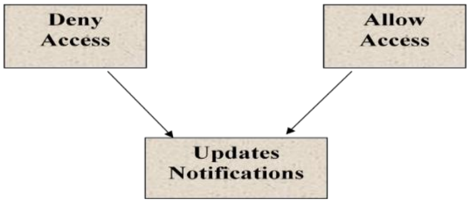


Fig.6. Administrative Notifications

The above Fig.6 illustrates administrative notifications. The Advanced for a wide range of PDAs accessible on the lookout, the Applications Manager Mobile Client gives a helpful technique to follow basic applications, perform activities, get cautions and recognize issues rapidly and effectively from any area. The updates are done consistently occasionally at whatever point the information base gets invigorated. The chairman client can likewise be made to another case by the client.

Mobile Admin allows clients to perform tasks, for example, opening AD accounts, observing workers and organization gadgets, running reinforcement occupations, and overseeing virtual conditions without surging back home or to the workplace. Mobile Admin provides direct joining with Solar Winds Orion items permitting framework and organization chairmen to deal with their Solar Winds applications and conditions. With Mobile Admin‟s portable Active Directory highlights, framework executives can oversee AD protests from a cell phone. Versatile Admin additionally incorporates coordination with Novell Netware for secure administration of clients and gatherings. With Mobile Admin's versatile virtualization the board combinations, framework. Administrators can assume full responsibility for their virtual surroundings directly from their mobile device.

IV. PERFORMANCE EVALUATION

A. Overview

We evaluated performance of proposed work with Eclipse Juno 4.2.0 in the developer end and Android Mobile with Minimum API-14 at the client end. Smartphone is needed to get data. User permission is needed to install application. All installed application will be investigated. The profile creation will be taken care of by various proprietors. Corporate Profile can be vary from the private profile. After corporate principles have been characterized two security profiles will be made at the time application installation. The profile data will not be shared with the other data. Isolation is kept up between the security profiles. Based on the authorization, The profile can be activated with the location identification. Profile administrator, which is one of the audience will be told when the profile activity is contrasted. Client authorization is needed to install application. Location manager takes care of all location updations.

B. Dynamic Profile Management

The utilizations of the private profile can be adjusted whenever without any intervention of administrator. The private applications includes no limitation since there is no manager to confine admittance to its applications.

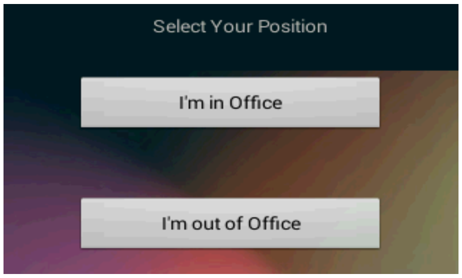
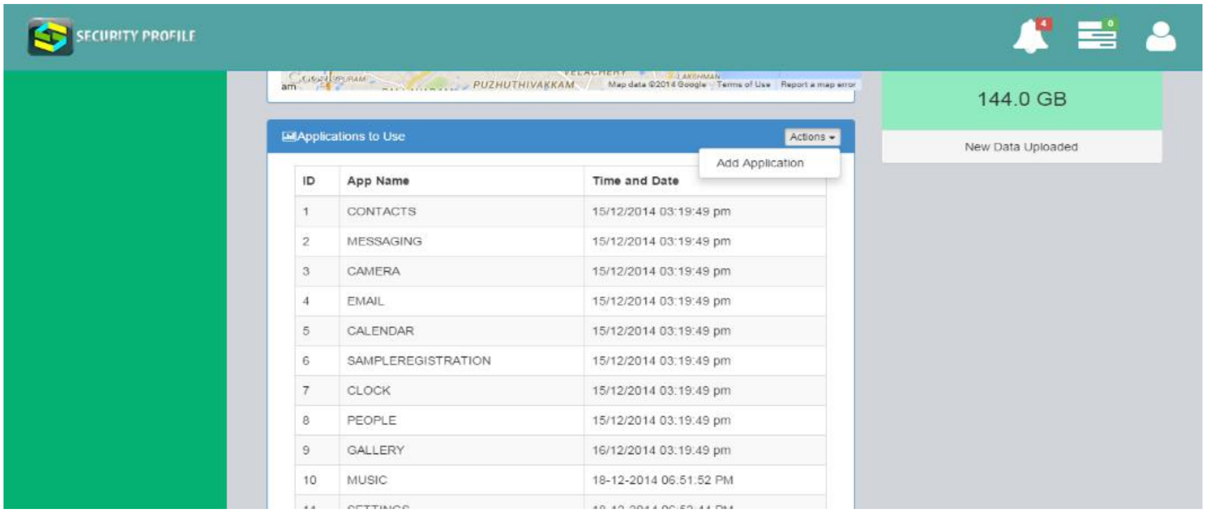


Fig.7. Corporate Position Management

The above Fig.7 clearly illustrates about the corporate position management which empowers the client to get to the utilizations of the corporate profile either in office or out of office. The area chief holds the client location. The Corporate profile holds the connection to area supervisor which recognizes and tells the client areas. The area supervisor sends warnings to the manager.

C. Application Management

Application management which helps in adding and eliminating the client applications from a profile. The default applications for a profile are incorporated at profile creation.



ID	App Name	Time and Date
1	CONTACTS	15/12/2014 03:19:49 pm
2	MESSAGING	15/12/2014 03:19:49 pm
3	CAMERA	15/12/2014 03:19:49 pm
4	EMAIL	15/12/2014 03:19:49 pm
5	CALENDAR	15/12/2014 03:19:49 pm
6	SAMPLEREGISTRATION	15/12/2014 03:19:49 pm
7	CLOCK	15/12/2014 03:19:49 pm
8	PEOPLE	15/12/2014 03:19:49 pm
9	GALLERY	16/12/2014 03:19:49 pm
10	MUSIC	18-12-2014 06:51:52 PM

Fig.8. Application Management

The admittance to the client profile applications should likewise be possible by the system administrator to limit the undesirable access. The mobile has corporate applications and isolated applications from corporate profile for secure access The following Fig.8 illustrates the application managementEmpowering and incapacitating the security limitations can be acted in the administrator page of the worker. The administrator deals with all the available applications to be gotten to by the client to go through secure access. The following Fig.9 clearly gives a diagrammatic view of the corporate applications enabled in a corporate profile of a employee smart phone

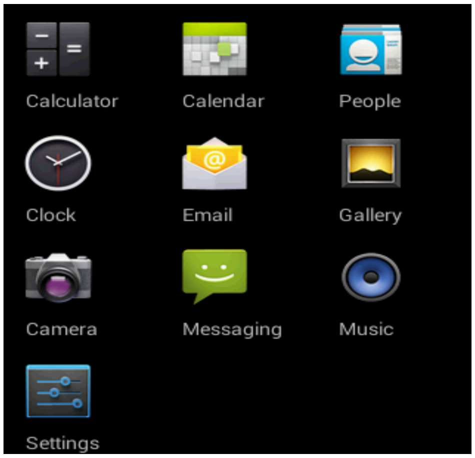


Fig.9. Corporate Applications

The following F.g10. illustrates the point by point confined arrangement of private profile applications to execute separation from corporate profile applications. All the uses of the corporate profile are given by the administrator yet for the private profile the applications can be added or eliminated by the client itself with no limitations.

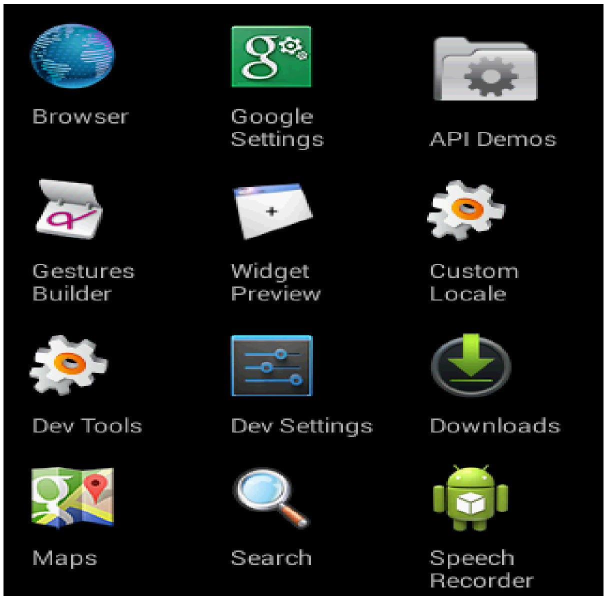
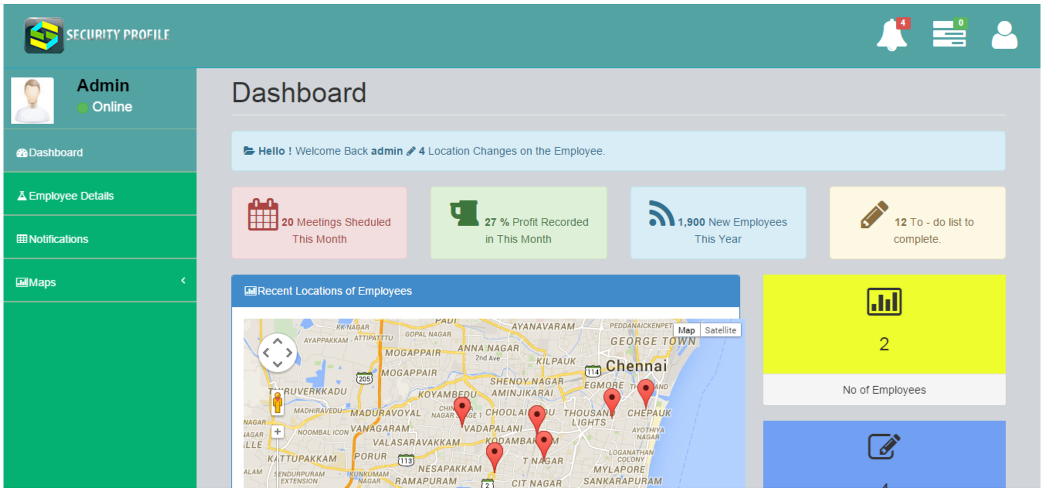


Fig.10. Isolated Applications from Corporate Profile

As the applications are isolated from corporate profile with separate storage for both profile makes our proposed work out performing comparing to existing techniques.

D. Location Management

Location indication by the location manager to identify the location of the user and to send the location update to the system administrator. The location manager is initialized at the time of profile creation. The administrator takes care of location updation to the server database at regular intervals. By GPS the office parameters are set for the location tracking. Here the control transfes from application activity manager to the location manager[8] which holds the location of the employee"s organization to check his availability. The following Fig.11 clearly explains about the location dash board of a employee indicating the location changes with respect to corporate profile updations.



Dashboard

Hello ! Welcome Back admin 4 Location Changes on the Employee.

20 Meetings Sheduled This Month

27 % Profit Recorded in This Month

1,900 New Employees This Year

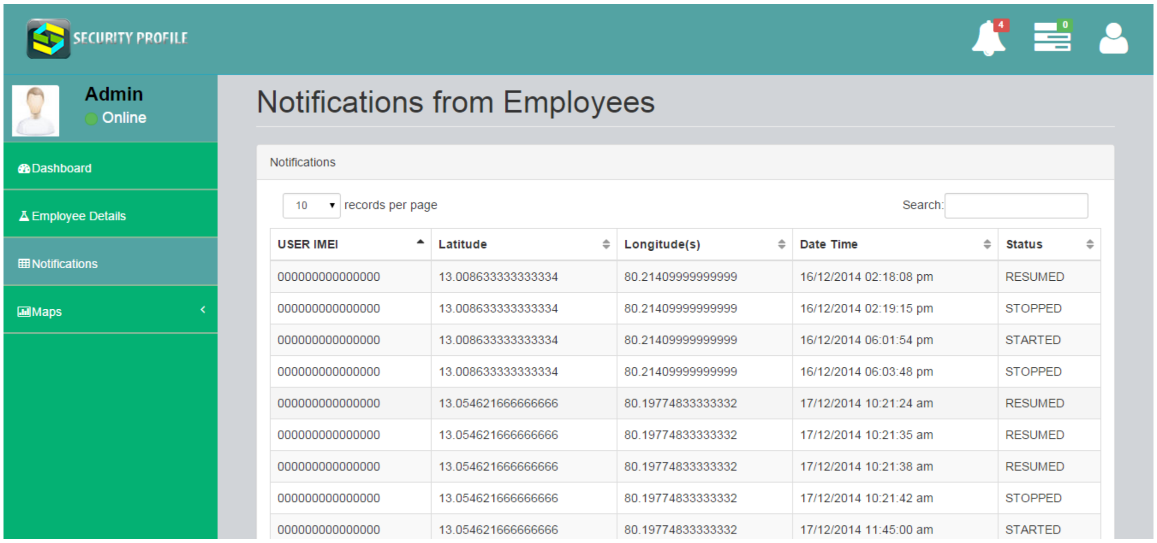
12 To - do list to complete.

2

No of Employees

Fig.11. Administrative Dashboard

On the off chance that the client is out of corporate the administrator can deny or permit the client to get to the corporate profile and in this way refreshes client locations.The corporate profile can get gotten to just if the chairman allows to validate regardless of area of the user.The manager can make a worker to be added or taken out from the client information base by his manipulations.The out-office notices are appeared in green while all in-office warnings are appeared in red. The following Fig..12 clearly indicates admin notification updations.



Notifications from Employees

Notifications

10 records per page

USER IMEI	Latitude	Longitude(s)	Date Time	Status
000000000000000	13.008633333333334	80.21409999999999	16/12/2014 02:18:08 pm	RESUMED
000000000000000	13.008633333333334	80.21409999999999	16/12/2014 02:19:15 pm	STOPPED
000000000000000	13.008633333333334	80.21409999999999	16/12/2014 06:01:54 pm	STARTED
000000000000000	13.008633333333334	80.21409999999999	16/12/2014 06:03:48 pm	STOPPED
000000000000000	13.054621666666666	80.19774833333332	17/12/2014 10:21:24 am	RESUMED
000000000000000	13.054621666666666	80.19774833333332	17/12/2014 10:21:35 am	RESUMED
000000000000000	13.054621666666666	80.19774833333332	17/12/2014 10:21:38 am	RESUMED
000000000000000	13.054621666666666	80.19774833333332	17/12/2014 10:21:42 am	STOPPED
000000000000000	13.054621666666666	80.19774833333332	17/12/2014 11:45:00 am	STARTED

Fig.11. Admin Notification Updation

The administrator can allow a user to enter into the profile if he grants access to the user.The administrator can be allowed to view all the details about the in-office login informations like date,time,status thus giving a detailed information about the location updations.

4. Conclusion and Future Enhancements

The whole proposed structure is an answer for give strategy based security holders executed totally through programming. In view of the Profile Management, The information between those profiles will be segregated. The Location the executives likewise performed through the cycle of administrator notices. To make Security Profiles on the advanced cells, an alternate structure has been continued in this proposed system.It gives an answer that could be executed by methods for virtualization advances. It will be more segregated than the current framework and it forestalls the information in any remaining applications to isolation.System design records will be investigated and when an unauthenticated activity is performed by the client implies, the security profile won't be reachable. The head will deal with the area the executives subtleties. When the Outer-Corporate area is recognized by the administrator, at that point the consent of access will be done dependent on the regulatory definition to your corporate profile. While playing out those activities, undertaking information will be more secret. As an upgrade of this cycle, The another profile or corporate profile should get to the information from the distributed storage. So the gadget stockpiling may not be conflicted. The managerial part can be ad libbed all things considered in the proposed framework. So that improved report will be produced from the regulatory part. Here the client will be permitted to switch between various profile all the while simultaneously.

References

1. YuryZhauniarovich, "MOSES : Supporting and Enforcing a Security Profiles on Smartphones", IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 3, may-june 2014.
2. K. Barr, P. Bungale, S. Deasy, V. Gyuris, P. Hung, C. Newell, H.Tuch, and B. Zoppis, "The VMware Mobile Virtualization Platform:Is That a Hypervisor in Your Pocket?" ACM SIGOPS OperatingSystems Rev., vol.44, no. 4, pp. 124-135, Dec. 2010
3. C.Gilber,"Android Leaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale", Proc.Fifth Int'l Conf.Trust and Trust worthy Computing (TRUST'12).pp.291-307.2012. William Enck,"Understanding Android Security", IEEE Security &Privacy, vol.7, no.1, pp. 50-57, January/February 2009, doi:10.1109/MSP.2009.26,Page(s):57-64.
4. Jipeng Zhou and Zhengjun Lu, "A Secure Distributed Location Service Scheme for Mobile Ad Hoc Networks", IEEE International Symposium on Computer Network and Multimedia Technology (CNMT), 2009.
5. Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, Vol.10, No.9, 2011.
6. D. Saranya, S.Prakash,K.S. Kavitha Kumari," Autonomous Forklift Vehicle with Object Recognition and Obstacle Detection," Journal of Green Engineering (JGE), vol.10, Issue no.6,pp 3238-3246,June 2020
7. K.S. KavithaKumari, K.Uma, C.Rameshkumar, M.BashaKhaja," Crime Prediction Using Machine Learning and Testing With Classification Models," International Journal of Psychosocial Rehabilitation,vol 124,issue no.6,pp.9275-9287,May 2020
8. H. R. Schmidtke, "Location-aware systems or location-based services: a survey with applications to CoViD- 19 contact tracking," Journal of Reliable Intelligent Environments, vol.6, pp.191–214, Sep 2020
9. Gang Sun; Shuai Cai, Hongfang Yu, Sabita Maharjan, Victor Chang, Xiaojiang Du, Mohsen Guizani , "Location Privacy Preservation for Mobile Users in Location-Based Services," IEEE Access , vol..7,pp. 87425 – 87438, June 2019
10. Prathiba, R., and G. Nagarajan. "A two phase energy-efficient routing protocol for underwater wireless sensor network to enhance data gathering." International Journal of Mobile Network Design and Innovation 9, no. 1 (2019): 24-36.
11. Sreeram, S., and G. Nagarajan. "EDA-PEGASIS: A Balanced Energy Aware Routing Approach for Sensor Network to Reduce Cognitive Networking Complexities in Wireless Medium." In International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy, pp. 575-584. Springer, Singapore, 2020.
12. Simpson, Serin V., and G. Nagarajan. "SEAL—Security-Aware List-Based Routing Protocol for Mobil Ad Hoc Network." In International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy, pp. 519-530. Springer, Singapore, 2020.
13. Sajith, P. J., and G. Nagarajan. "Optimized Intrusion Detection System Using Computational Intelligent Algorithm." In Advances in Electronics, Communication and Computing, pp. 633-639. Springer, Singapore, 2021.