IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 6, June 2017

Providing Secured Transmission Of Data From Mobile To Cloud Using Permission Customized Technique

[1] Ashok Jayam, [2]Roobini Sampath, [3]Senthil Kumar.T
[1] [2] [3]SRM University (B.Tech CSE)

Abstract: ***Smart phone is the most pivot electronic device which is being used in the present generation. The smart phone is not capable of preventing over collection of data which is the most hazardous task in protecting the personal information without the knowledge of mobile administrator. Over collection of data results in accessing the user information without prior permission of mobile administrator. In this paper we have presented a technique to prevent the over collection of data in smart phone using cloud environment and by the use of the cloud environment there will be drastic increase in storage space in smart phone provided with remote access to prevent access of data in the smart phone in the case of mobile theft.***

Key Words: - ***Smart phone, Remote access, Security and Mobile cloud Provider (MCP)***

I. INTRODUCTION

Now -a -days smart phones play a vital role in the life of people .Due to its more usability the situation has turned in a way that we can't do any task without mobiles .As they gained such a prominent role due to the comfort provided by them many smart apps were being released which transformed the everyday life of a human being. The more smart apps were being released in the market the more problematic the life is getting turned. It is because the smart phones were not capable of protecting the data present inside the device. The app administrator can easily access the personal data present in the mobile phone without notice of the mobile administrator. There is no choice to refuse the data which is being taken more than requirement .In other words while downloading the app it will be up to the mobile administrator whether he/she should keep their photo in it where the app administrator can't insist us to keep the photo in order to download the app and the situation is that we will be forced to keep the photo inside the app where we are not sure about it. So we can prevent this by using the cloud environment where the cloud administrator will analyse the particular credentials which are necessary for running the app and permit only those conditions will be visible in the agreement screen. The other drawback with over collection of data is the location details of the user. If we are playing game it is not necessary for user location which can be prevented from danger. App – administrator can read and write changes in the contact while accessing the information which can be prevented by cloud admin .As many are storing data in smart phones it can be the major loss for the mobile administrator. But now we provided remote access so that in case of theft we can disable the apps from others phone and secure them. If you do so then the person who has your phone can't be able to access it thereby mobile your information will be secured.

The two major contributions of this paper are:

- By providing remote access to the smart phone the mobile administrator can be fearless about the data present in the mobile phone even after theft.
- The security of the data can be done effectively and no chance of terms beyond requirement will be specified in the licence so there won't be any sort of fear in saving the data in smart phone .As data was being saved in cloud the security and space in mobile phone increases drastically .As space in mobile phone increases speed increase, as speed increases efficiency of mobile increases. As efficiency increases life span of mobile increase.

II. RELATED WORK:-

In this section, we will discuss the current solutions of increasing security and providing remote access to the smart phone. As we know, there are four stages present in increasing the security in smart phones. They play a vital role and give good result finally. First we should find out a way to create a platform between the cloud and smart phone. By using struts web framework we can connect the server and the smart phone which thereby lays a platform to import the apps present in the connected smart phone. After creating the connection we are supposed to initiate the first stage of the security process. The first stage of security process is User Registration and data updating on server.

- Data updation:-

The smart phone application provided by the mobile cloud provider (MCP) monitor the other service applications and collect the data stored by the various application in the various locations in the device memory storage. Initially user should register their mobile with the cloud and creating an authorized account there selves through smart phone application. This account maintains the credentials of users' can access their cloud data as Google drive wherever using their account credentials.

The application receives the entire data using the receiver services and it can update the respective account on cloud. The MCP provides security for data retrieved from the user's smart phones. Cloud provider generates the key for individual user account and send to the user's phone in secure manner. Thereafter users can access their phone data wherever through cloud storage. The entire smart device storage data can be accessed through the cloud which can be configuring and accessing by respective users. Only one single registration is valid for every device. Thus how the data present in the smart phone will get connected to the server. Now the second stage of security process should be done.

- Data customization :-

Security preliminary process have implemented by the mobile cloud provider. Initially cloud provider must predefine the permission of data accessing for the each android applications. Based on the predefining permission mechanism the android application can access permitted and essential data of user's phone through the cloud. MCP should assigning permission individually for each of the application installed in user's android devices. And the person who knows these security constraints about the android application's permission and data over collection can customize their account on cloud and can assign permissions for each of the application. Now the data over-collection can be prevented mainly and the credentials which are required only will be appeared in the license terms and it will be beneficial for the mobile cloud. Now it can be accessed even in the absence of mobile phone and the device will be safe. As the data was saved in the cloud there will be drastic space left in the smart phone which will increase the speed and efficiency of the device.

- Customization of data in cloud by user:-

Data privilege given by our mechanism is the online cloud drive for user's private data. Users can access their phone updates from the cloud. Using these privilege users can trace their phone while phone theft. Users can customize their phone's permissions on cloud hence we provide the data security. . Highly secured and recommended cryptography can apply to the data security on future enhancement. Thus the data present in the smart phone be secured and can be disabled using the cloud environment which is the idle feature in the present app.

- Application permission access:-

permission analysing and assigning permission of each application. Based on the customization of access permission can provide data to application eventually. Our mechanism insists the application can having the device hardware accessing permission only. And rest of the data collection permission will be redirect to the respective cloud account of each user's.

- Architecture:-

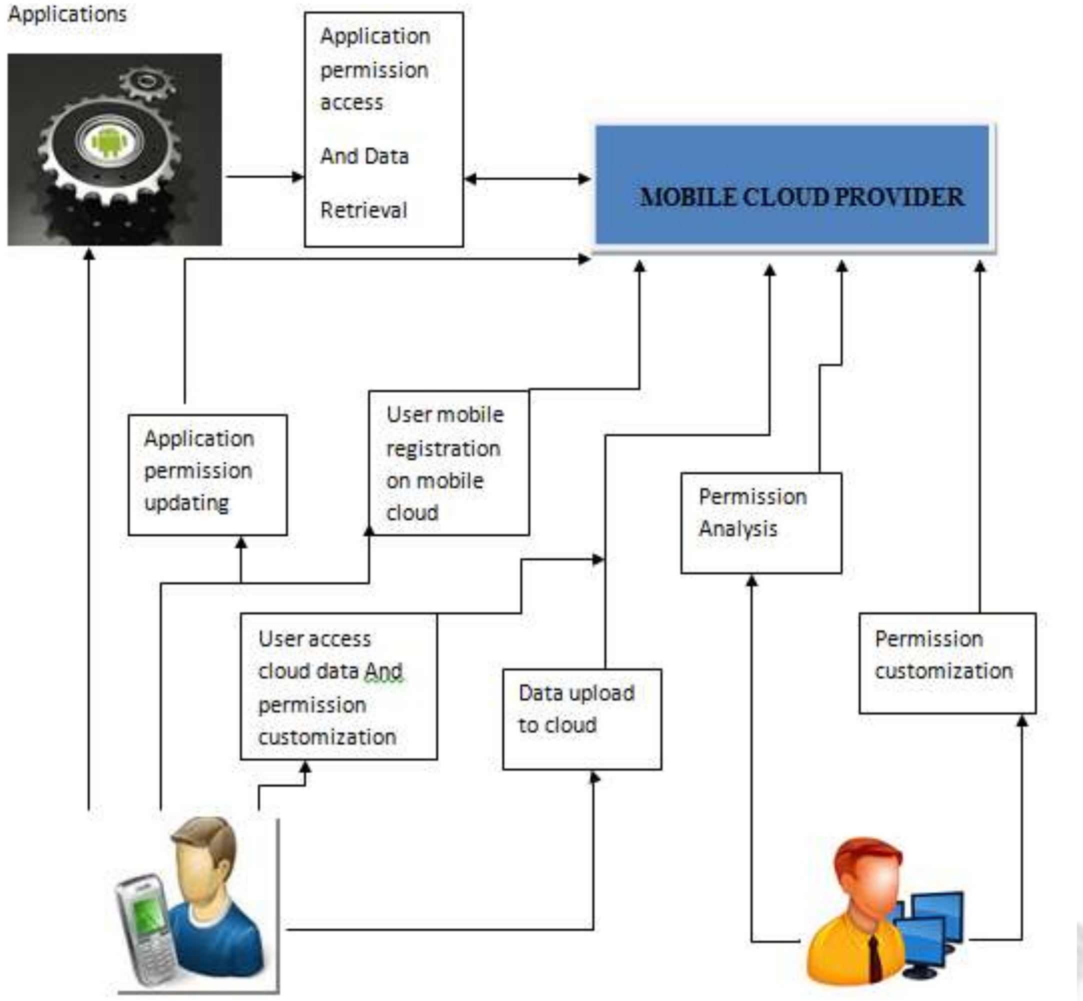
As shown above first the data present in the mobile phone will be uploaded in cloud called Mobile Cloud Provider which is done as soon as the user registration process was completed. After that the Mobile cloud provider will analyse application permission access for Data Retrieval and the application will ask the data which was permitted by the cloud and was managed by cloud administrator. In case of phone theft the user can login with the user id and password provided by cloud and can customize the apps present in his phone and the customized permissions will be stored in cloud. If this is done the data present in the phone cannot be viewed by the person who theft the phone. In this way remote access of smart phone will be accomplished.

Remote access:-

The smart phone with above access can be accessed from cloud as well as other mobile devices even in the absence of the mobile phone. As it was accessed from anywhere and even in the absence of phone through the id and password generated by the cloud it can be protected and secure the personal information of user.

The architecture diagram is shown below:

- Architecture diagram:-


Applications
Application permission access And Data Retrieval
MOBILE CLOUD PROVIDER
Application permission updating
User mobile registration on mobile cloud
Permission Analysis
User access cloud data And permission customization
Data upload to cloud
Permission customization

- Mobile Cloud Provider:-

  The mobile cloud provider (MCP) preserves the data present in the phone when the registration was done the data present in the phone will be imported by the cloud .

- Application permission and Data Retrieval:-

  The cloud Administrator will analyse the permissions which were required for the application and grant them. The data present in the cloud can be retrieved whenever necessary.

- Permission Customization:-

  This can be done by the cloud administrator and the mobile administrator by enabling the permissions present in the inbuilted applications so that they work accordingly.

- Permission Analysis:-

The cloud administrator will analyse the permissions required by the app and grant them thereby preventing the over-collection of data.

- Data upload to cloud:-

  The data present in the smart phone will be updated in the cloud through the cloud administrator using login credentials.
- Application permission updating:-

  After customizing the app permissions they are updated so that the application will work according to the updated permissions.
- Future Applications:-

The applications will work fastly as there will be drastic increase in memory of phone storage and the data will be secured.

- Experimental setup:-

Every app which was being downloaded by the mobile administrator into his/her mobile are able to access the personal information present in his/her phone and has the potential to make read or write changes without the notice of mobile administrator. In order to prevent this data over-collection and to prevent the phone during phone theft we are able to disable the permissions so that the app can’t be accessed. In this way we can have control on our phone even in its absence.

1. Applications permission customization:-

This algorithm is used to enable the permissions and functions of the app irrespective of its behaviour. The following are the steps present in order to make it work. First after logging in with the cloud admin we should choose app customization where the apps present in your phone will be displayed along with its features and if we disable their features the corresponding feature which we disabled won’t work. Thus we can permit the features based on our convenience. Thus the phone is being protected.

Structure:-

```
If app== modified changes then
behaviour of app will be changed and according to the customized permissions it works;
else if
no changes in customized app permissions then it works normally;
else
works normally
end if ;
end if;
```

2. Receiver data analysis:-

This algorithm is used to analyse the sensitivity of data when the data is being updated to the cloud. So the cloud is going to take responsibility for protecting the data present in the system. The structure is shown below:-

Structure:-

```
if data==more sensitivity then
More protection is allocated and confidentiality is maintained;
else if data == sensitivity
protected;
end if;
end if;
```

3. Time based updates and limitations:-

This algorithm helps in accessing the updates of application in the cloud through which the information required will be processed in the cloud and then the data present in the license terms. Thus the data over-collection is prevented and security of personal information prevails thereby providing the remote access by accessing it through cloud even in the absence of phone through the login id and password given by the cloud. The structure is shown below:-

Structure:-

```
if update== found then
Cloud analyses the requirements of applications and permit the terms in licence;
else if time== less time to expire
alarm or alert notification;
end if ;
end if;
```

- Result strategy:-

Let us take the phone which has remote access and connected with cloud which is analysing the credentials required during the time of license agreement and the phone absent with the above features then the consumption of memory in the phone increases and the speed decreases. After that security decrease and over collection of data increases.

If we take the phone which has remote access and connected with cloud the security increases, consumption of memory decreases and security in absence of phone increases.

Fig -1:Statistics of phone without remote cloud service.

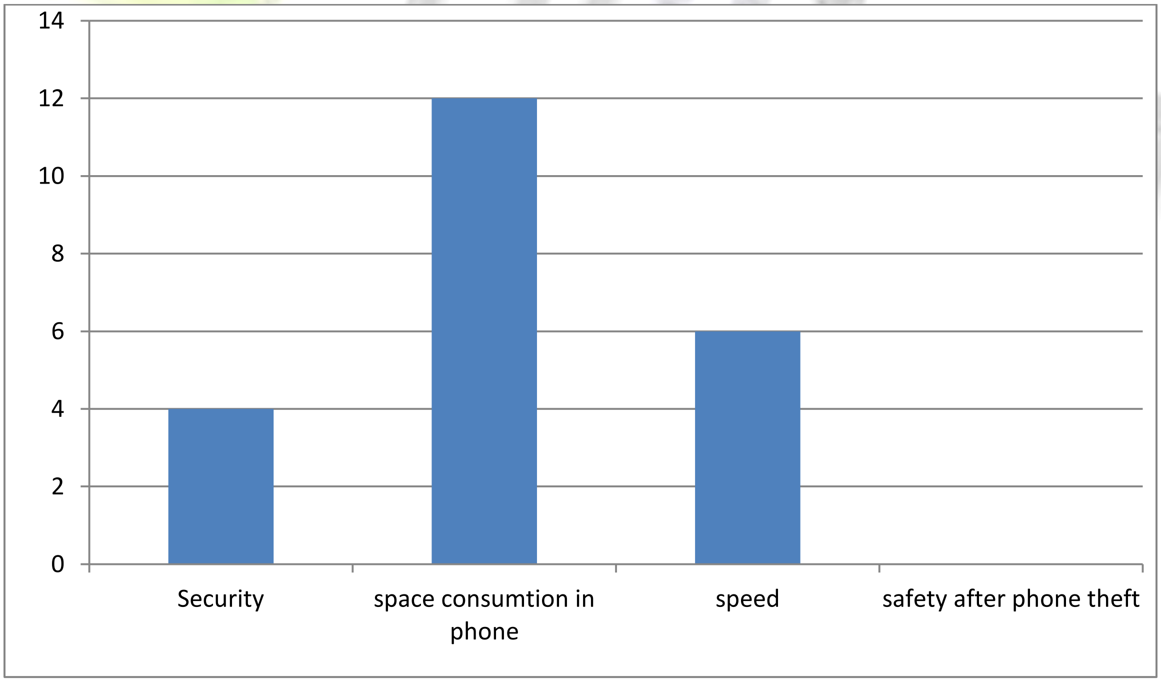


Fig -1:Statistics of phone without remote cloud service

As stated above those are the problems present with the phone without remote access and lack of cloud connection where security space consumption in phone storage speed and safety after phone theft were low .

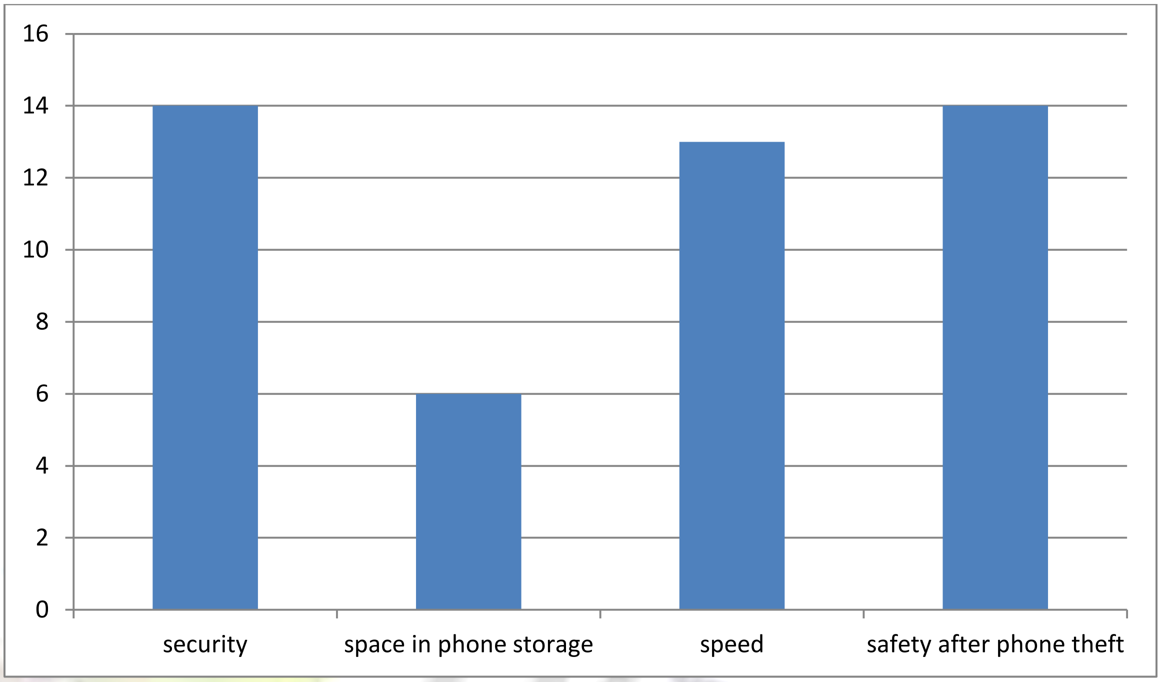
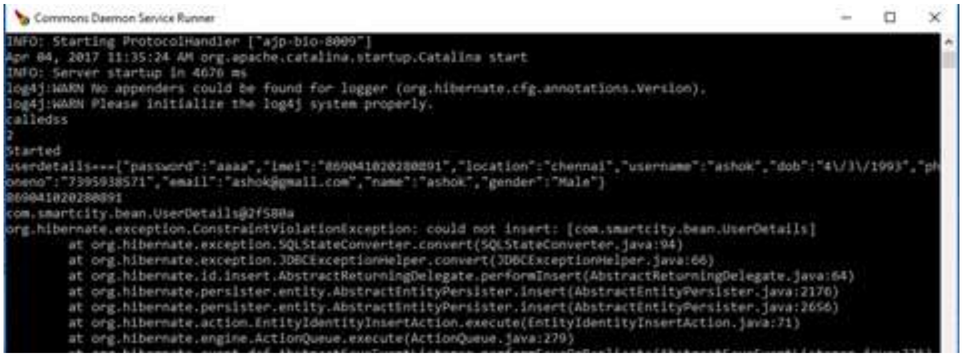


Fig -2: phone with remote access and with cloud connection

Thus the phone with remote access and with cloud connection differed from normal smart phone where security speed and safety after phone theft were more and space consumption was less.

- Screenshots:-

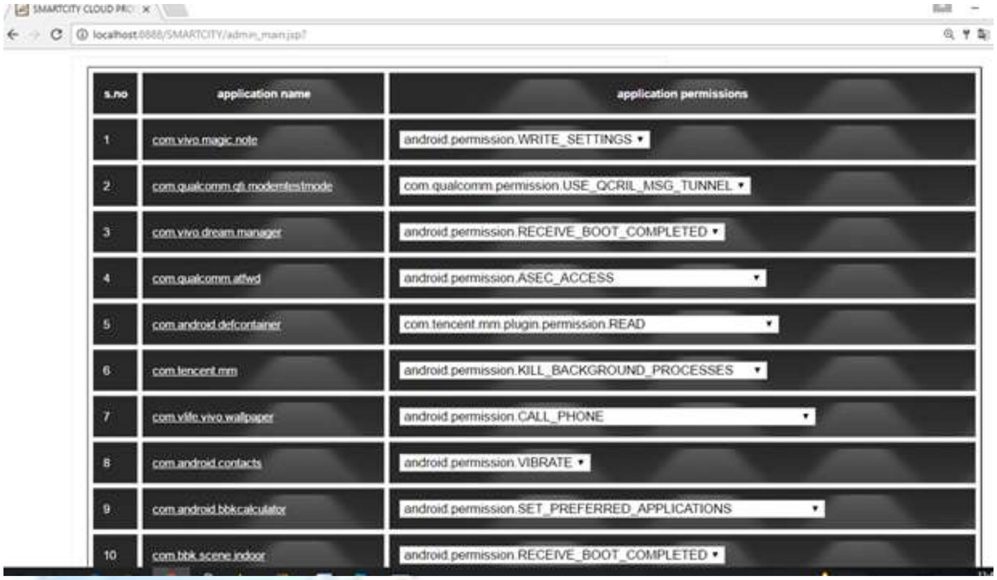
  The below figure shows the data which is updated in the server. As shown in the figure as soon as the user registers the details will be updated in the cloud.



```
INFO: Starting ProtocolHandler ["ajp-bio-8009"]
Apr 04, 2017 11:35:24 AM org.apache.catalina.startup.Catalina start
INFO: Server startup in 4676 ms
log4j:WARN No appenders could be found for logger (org.hibernate.cfg.annotations.Version).
log4j:WARN Please initialize the log4j system properly.
calledss
2
Started
userdetails+++{"password":"aaaa","imei":"869041020280891","location":"chennai","username":"ashok","dob":"4\/3\/1993","ph
oneno":"7395938571","email":"ashok@gmail.com","name":"ashok","gender":"Male"}
869041020280891
com.smartcity.bean.UserDetails@2f580a
org.hibernate.exception.ConstraintViolationException: could not insert: [com.smartcity.bean.UserDetails]
        at org.hibernate.exception.SQLStateConverter.convert(SQLStateConverter.java:94)
        at org.hibernate.exception.JDBCExceptionHelper.convert(JDBCExceptionHelper.java:66)
        at org.hibernate.id.insert.AbstractReturningDelegate.performInsert(AbstractReturningDelegate.java:64)
        at org.hibernate.persister.entity.AbstractEntityPersister.insert(AbstractEntityPersister.java:2176)
        at org.hibernate.persister.entity.AbstractEntityPersister.insert(AbstractEntityPersister.java:2656)
        at org.hibernate.action.EntityIdentityInsertAction.execute(EntityIdentityInsertAction.java:71)
        at org.hibernate.engine.ActionQueue.execute(ActionQueue.java:279)
```

Fig -3. Data updation

- Along with the user data the applications present in the smart phone will be imported in the cloud from which the cloud administrator can custamize the permissions required by the app.

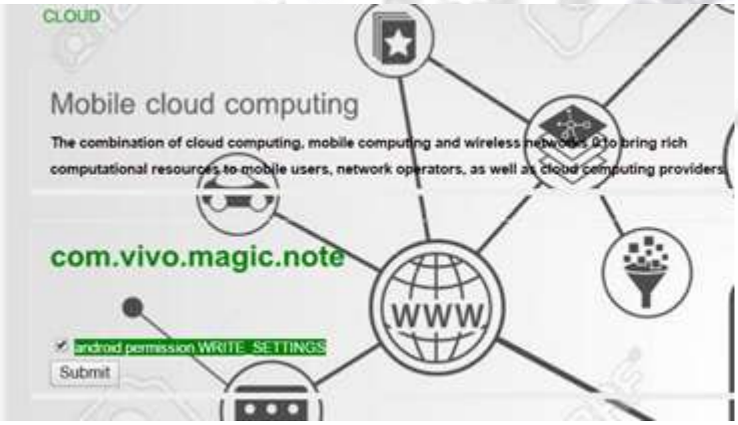


SMARTCITY CLOUD PR
localhost:8888/SMARTCITY/admin_main.jsp?

s.no	application name	application permissions
1	com.vivo.magic.note	android.permission.WRITE_SETTINGS ▾
2	com.qualcomm.qti.modemtestmode	com.qualcomm.permission.USE_QCRIL_MSG_TUNNEL ▾
3	com.vivo.dream.manager	android.permission.RECEIVE_BOOT_COMPLETED ▾
4	com.qualcomm.atfwd	android.permission.ASEC_ACCESS ▾
5	com.android.defcontainer	com.tencent.mm.plugin.permission.READ ▾
6	com.tencent.mm	android.permission.KILL_BACKGROUND_PROCESSES ▾
7	com.vlife.vivo.wallpaper	android.permission.CALL_PHONE ▾
8	com.android.contacts	android.permission.VIBRATE ▾
9	com.android.bbkcalculator	android.permission.SET_PREFERRED_APPLICATIONS ▾
10	com.bbk.scene.indoor	android.permission.RECEIVE_BOOT_COMPLETED ▾

Fig -4:Data present in cloud

- As shown below even the mobile administrator can customize the settings of the app according to him.The below figure shows the customization technique from which the user can customize the permissions so that the data can be protected.



CLOUD

Mobile cloud computing

The combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers

com.vivo.magic.note

☑ android.permission.WRITE_SETTINGS

Submit

Fig -5:Customization of data

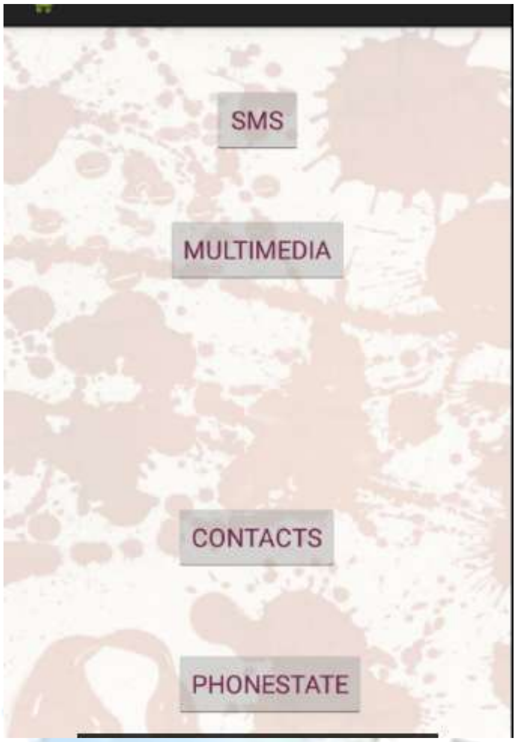
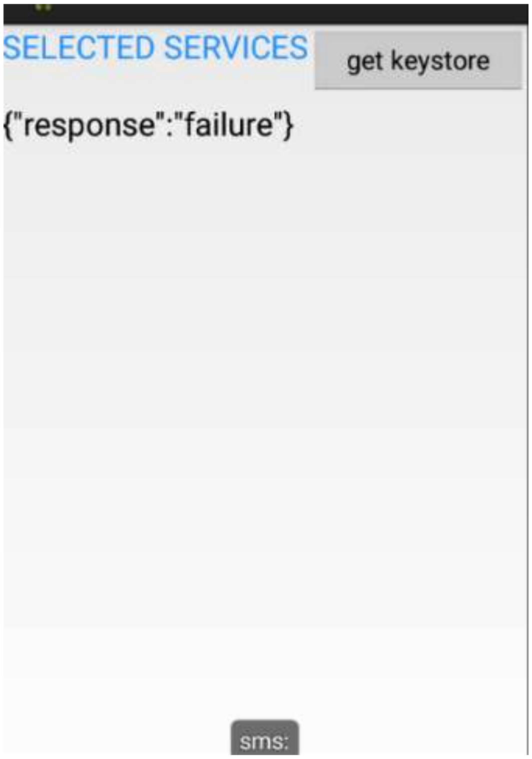


Fig -6:List of applications



```
{"response":"failure"}
```

Fig -7: Result after Customization

- The above figure shows the list of the applications from which data will be lost. By customizing the applications according to our wishes we can secure the data.It is shown in the figure 6.

- The figure 7 show how the data can be protected .We have restricted the permission to read the message so the messages which were received by the person cannot view the messages .In this way the data can be secured and cannot be viewed until it was enabled.

- Conclusion:-
  Privacy protection has become a threat in smart phone where the third party people were viewing the personal information present in it .So we have provided an active approach to protect the data privacy in smart phone thereby providing the remote access to protect the privacy data in smart phone with cloud connection which will prevent data – overcollection and increase the safety of data in absence of phone.Now the speed of phone increases because there is drastic difference in memory space. By using this technique we can disable the apps present in the phone during phone theft so there are no chances for data leakage.Thus the data overleakage can be prevented to maximum extent and the phone can be tracked during phone theft.Thus it is so beneficial so it will be more beneficial as smart phone is going to play a vital role in the next generation.

REFERENCES

[1] Schneider. (2014). Go green in the city [Online]. Available: http:// 2014.gogreeninthecity.com/smart-cities.html

[2] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "PiOS: Detecting privacy leaks in iOS applications," in Proc. 18th Annu. Net . Distrib. Syst. Security Symp., 2011, pp. 1–15.

[3] W Enck, P.Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in Proc. USENIX 9th Conf. Oper. Syst. Design Implementation, 2010, pp. 1–6.

[4] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of Android application security," in Proc. 20th USENIX Conf. Security, 2011, p. 21.

[5] A. Bose, X. Hu, K. G. Shin, and T. Park, "Behavioral detection of malware on mobile handsets," in Proc. ACM 6th Int. Conf. Mobile Syst., Appl., Services, 2008, pp. 225–238.

[6] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proc. ACM 1st Workshop Security Privacy Smartphones Mobile Devices, 2011, pp. 3–14.

[7] J. Cheng, S. H. Wong, H. Yang, and S. Lu, "Smartsiren: Virus detection and alert for smartphones," in Proc. ACM 5th Int. Conf. Mobile Syst., Appl. Services, 2007, pp. 258–271.

[8] Appthority. (2014). App reputation report [Online]. Available: https://www.appthority.com/app-reputation-report/report/ AppReputationReportS ummer14.pdf

[9] L. Musthaler. (2013). At least 80% of mobile apps have security and privacy issues that put enterprises at risk [Online]. Available: http://www.networkworld.com/article/2163225/ infrastructure-management/at-least-80-of-mobile-apps-havesecurity- and-privacy-issues-that-put-ente.html

[10] A. Pathak, Y. C. Hu, and M. Zhang, "Where is the energy spent inside my app?: Fine grained energy accounting on smartphones with Eprof," in Proc. ACM 7th Eur. Conf. Comput. Syst., 2012, pp. 29–42.

[11] M.qiu,W. Gao M.Chen, j w niu and L.zhang" energy efficient security algorithm for power grid wide area monitoring system"IEEE Trans .Smart Grid,vol2,no 4,.pp.715-723,Dec.2011

[12] J.Blom, D. Viswanathan,M. spasojevic, J. Go , K. Acharya and Ahonius,"nFear and the city : Role of Mobile Services in harness ing safety and security in urban use context " in proc.SIGCHI conf , Human Factors Comput.Syst,,2010,PP1841-1850

[13] A. paverd , A.Martin , and I. Brown,"Security and privary in smart grid demands response system" in Proc,2nd INT, Workshop Smart Grid Security ,2014,pp.1-15

[14] D.Damopoulous , G. Kambourakis, M.Anagnostopoulous, S.Gritzalis,and J.Park," user Privacy and modern mobile service: Are they on the same path?" personal Ubiquituos comput., vol17, no7,pp.1437-1448,2013

[15] P.Gilbert, B. G Chun, L.p.cox,and j.jung," vision: Automated security validation of mobile apps at app marked ,"in proc.acm 2nd Int .Workshop Mobile Cloud Comput .Services,2011,pp.21-26

[16] W.Enck , M.Ongtang and P.McDaniel ," Understanding Android security ,"IEEE Security Privacy , vol .7,no 1, pp.50-57, jan .2009

[17] X.Xiao, N.Tillmann,M. Fahndrich, J.De Halleux , and M.Moskal , " User- aware privacy control via extended statics – information flow analysis ," in proc ,IEEE/ACM 27th int Conf.Automated Softw.Engg, 2012,pp.80-89