



SMART MAP WITH PRIVACY PROTECTION

Mohammed Faisal.H¹,Azarudeen.A²,Manikandan.V³,M.Ahsan Shariff⁴

Student, Dept. of Information Technology, Mohamed Sathak A.J. College of Engineering, India.^{1,2,3}

faisalfais633@gmail.com¹, azarudeenbtech@gmail.com², btechm3@gmail.com³.

Asst.professor, Dept. Of Information Technology, Mohamed Sathak A.J. College of Engineering, India.⁴

ahsan.shariff@gmail.com⁴

Abstract--In smart city, all kinds of users' data are stored in electronic devices to make everything intelligent. A Smartphone is the most widely used electronic device and it is the pivot of all smart systems. However, current smart phones are not competent to manage users' sensitive data, and they are facing the privacy leakage caused by data over-collection. Data over-collection, which means smart phones apps collect users data more than its original function while within the permission scope, is rapidly becoming one of the most serious potential security hazards in smart city. In this paper, we study the current state of data over-collection and study some most frequent data over-collected cases. To prevent the data over-collection we show the smart things which is near by the user. We present a mobile-cloud framework, which is an active approach to eradicate the data over-collection. By putting all users' data into a cloud, the security of users' data can be greatly improved. We have done extensive experiments and the experimental results have demonstrated the effectiveness of our approach.

Keywords— Smart city, Smartphone, cyber security and privacy, data over-collection

I. INTRODUCTION

Smart city is meant to be and will be the next generation of urbanization. However, it brings some new challenges to be solved, such as security and privacy. The most arduous challenge about the cyber security and privacy of smart city is to ensure sensitive data secure. People living in a smart city use all kinds of electronic devices instead of traditional manual or mechanical equipments. To make the whole smart city

efficiently, almost all these electronic devices need to be smart enough to recognize different users. Consequently, they must have the ability of storing and sharing data.

II.EXISTING METHOD

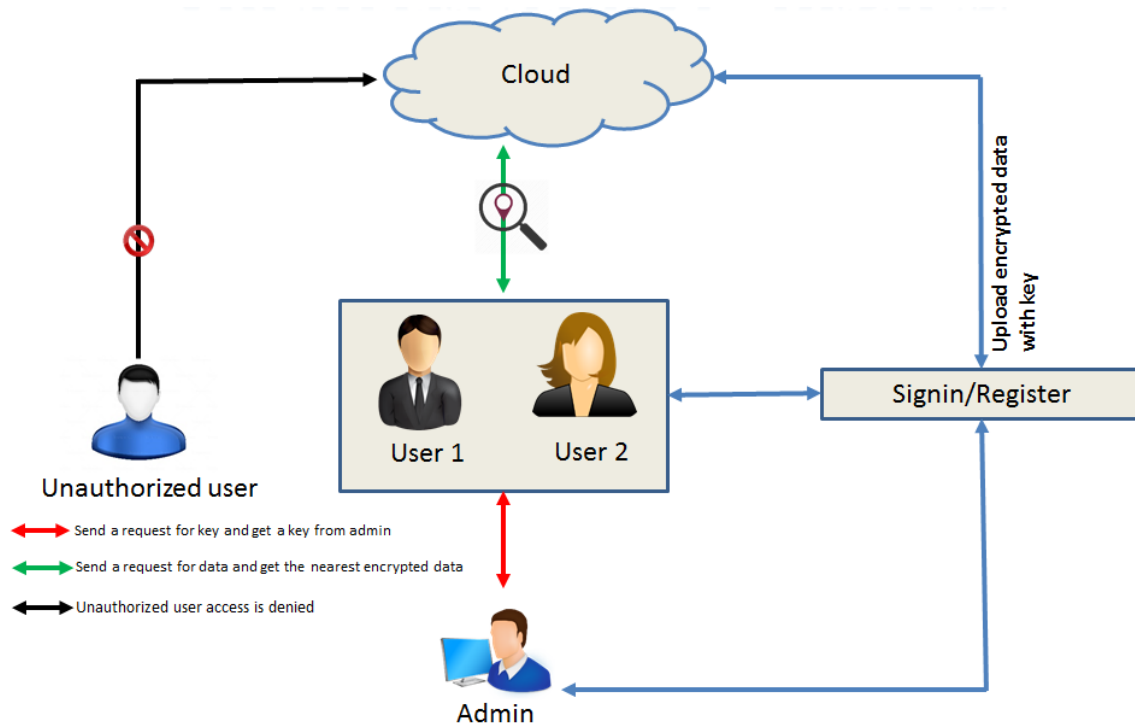
In existing concept user search the query like hospital, mall.. in the result it will show over-collection of data so it will take more time and the user data not have any privacy. It uses Search Graph Algorithm. Search in combination with a new graph-theoretic lower-bounding technique based on landmarks and the triangle inequality.

This leads to various disadvantages as follows

- It will show all the result so it will not be smart.
- It takes more time to get a smartest one.
- There is no privacy protection to the user.

III.PROPOSED METHOD

In our system all kinds of user’s data are stored in electronic devices to make everything intelligent. But we have prevented the data over-collection and store the encrypted data to give the privacy protection to the user’s data. We are using Nearest Graph algorithm with GPS.





IV. IMPLEMENTATION

4.1 Login / Registration:

In this module we design to develop login and signup screen. Android used xml to develop classical screens in our application. The modules describe signup page contains phone number or user name, password and conform password those kind of details should be stored in database. Login screen contains phone number or username and password when the user/admin to login the app it should be retrieve the data to the database and combine based on user input if its match user name and password to allow in the app otherwise alert and show a message to the user/admin.

4.2 Database Creation:

User/Admin number or name and password have been stored after registration. Android used MySQL Database for storing and fetching user application details

4.3 Find current position:

This module to find current position of the map. We will create an Android application which will display current location in Google map using Google Map Android API V2. Google map now integrated with the Google play service, so we need to set up Google play service library for developing Google map application. Here Google map will show using latitude and longitude without network connection like using GPS system.

4.4 Add mall, bus stop, railway station, hospital etc. :

This module admin add location of mall details, floor details and the shop details .Add the hospital and doctors details , Restaurant ,Bus Stop, Railway Station and Airport. All the details and personal details like phone number and address are stored in encrypted format in database.

4.5 Searching Mall, Bus stop, Railway Station, Hospital, Restaurant etc.:

In this module to display nearby malls, hospitals, restaurant, bus-stop, railway station and airport from your current position. Google map with help of network connection or GPS system finding the malls, hospitals, restaurant, bus-stop, railway station and airport nearby you. It fully integrated in Google play services.



4.6 Find the store inside the mall:

In this module to show internal structure of mall and what kind of store and shopping shops and its name and details and doctors details of the hospital details are show to the user. Here attached advanced technology to show your current position and your targeted position between exactly to show how much of kilometre or meter.

4.7 Call or Message:

This module user can call or message to the doctor or to the mall shop owner. So user can easily get the information.

V. CONCLUSION

Data over-collection in Smartphone becomes the most severe potential privacy hazard in smart city. Unlike malwares, data over-collection is difficult to be solved, because these kinds of behaviours are within permissions authorized by users. To maximize releasing users' operation pressure and eradicating the data over-collection problem, we presented an active approach. Every app that wanted to use users' data sent its request for accessing to the cloud, and the cloud access control service could provide detailed permissions for every app to every block of users' data. Meanwhile the operations of encryption and decryption were achieved by cloud encryption/decryption service that saves computation resource of Smartphone for dealing with these complex calculations. Finally, experimental result verifies the feasibility and advantages of our framework.

VI. FUTURE WORK

The further enhancement of this allow to search malls near to you and shop list Shop details within those malls. It calculates distance & give you direction guide to the mall from your current location and also include online buying. Replacement paths algorithm can be used as an alternative. The fast replacement paths subroutine is known to fail for some directed graphs. However, the failure is easily detected, and so our k shortest paths algorithm optimistically uses the fast subroutine, and then switches to a slower but correct algorithm if a failure is detected. Using this system can provide shortest path in a better manner

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. Netw. 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. Ocateau, 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/AppReputationReportSummer14.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-have-security-and-privacy-issues-that-put-ente.html>

**BIOGRAPHY:**

Mohamed Faisal.H is currently pursuing in B.Tech Information Technology in Mohamed Sathak A.J. College of Engineering, Anna University in Chennai, India, in May 2017



Manikandan.V is currently pursuing B.Tech Information Technology in Mohamed Sathak A.J. College of Engineering, Anna University in Chennai, India, in May 2017



Azarudeen.A is currently pursuing in B.Tech Information Technology in Mohamed Sathak A.J. College of Engineering, Anna University in Chennai, India in May 2017



Ahsan Shariff M received his B.Tech in Information Technology Department from Syed Ammal Engineering College, Ramanathapuram, India in May 2007 and got M.Tech in CSE from SRM University, Chennai, India in May 2013. He is currently working as an Assistant Professor in the Department of Information Technology in Mohamed Sathak A.J. College of Engineering, Chennai.

