ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Preserving Mobile Data Privacy through Profile Based Access Control

Sunil Singh, Pooja Singh, Sk Rizwana

Assistant Professor, Department of Computer Science and Engineering, Rajeev Gandhi University of Knowledge Technologies, Nuzvid, India

Student, Department of Computer Science, Radharaman Institute of Research and Technologies, Bhopal, India

Student, Department of Computer Science and Engineering, Rajeev Gandhi University of Knowledge Technologies, Nuzvid, India

ABSTRACT: Mobile data privacy deals with protecting the personal data in the mobile from thefts or unauthorized use. This paper proposes an idea of developing a mobile app that provides access control over mobile personal data based on the user's profile. According to the proposed application, different user's profile are created and specific to the user's profile, list of mobile's native functionality or apps are selected that will be accessible to the user on the selection of particular profile. The user's profile may be child, friend, guest, or custom profile based on the user's requirements.

KEYWORDS: Personal data, privacy, application, mobile

I. INTRODUCTION

At present, mobiles are much more powerful than they were in the past. The rapid growing technology is becoming popular with a wide range of new products and services. With emerging mobile technologies, the issue of privacy have been in the news in recent years. Protecting individual personal data is becoming a major challenge for the mobile developers, because, we are extensively using mobile phone for browsing, online shopping, banking, socializing, gaming etc. Due to this, our mobile phones contains important and valuable data, like, phone numbers, images, video, bank and other online account information etc. If these data are compromised, it may cause, embarrassment or sometimes even great loss, to mobile user. So, "Mobile Data Privacy" has become one of the major concern for mobile device and app developers.

Roughly speaking, personal data means any kind of information that can personally identify an individual. The obvious examples are somebody's name, address, national identification number, date of birth or photographs. It is something that is mostly seen to be stored in Mobiles. Mobiles are the most frequently shared devices. Even with pin-protected devices, user can readily unblock their phones and hand them to other users. There is much risk of confidential data being compromised and misused.

A. Motivation:

1. When social networking applications become more and more popular, the importance of privacy attracts more attention. User privacy refers to, the issue like, whether user's private information can be protected from unauthorized access. To address this issue many methods such as strong authentication, account control etc. should be added into the applications.
2. Data in form of files are more vulnerable than database records, since files are independent from each other, in most of times and hard to track. They can be easily transferred from one device to other.
3. The mobile user always wants to protect their personal data from unauthorized access. In many cases where user have to give his mobile to others, then there is a possibility that user's personal data may be compromised. To check this there should be an access control over user's personal data in mobile.

These are some issues that motivate us to do research on mobile data privacy.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

B. Research Objective

The research was commissioned to identify the problems that are existing in the field of mobile data privacy. **'The need of access control for unprotected mobile data'** is one of the problems in mobile data privacy. We are addressing this problem so that mobile data privacy can be improved. In addition, the development of an effective and consistent access control method will help user to become familiar with ways to manage the mobile personal data.

C. Problem Statement

We lock our phones with pass codes and sometimes protect them from malware with a security solution, so why don't we lock up the individual apps that houses some of our most personal and sensitive data?

From photos to emails to credit card numbers, our mobile apps hold invaluable data that is often left unprotected, especially given that some of the most commonly used apps on the different platform don't necessarily require a log-in each time they are launched. So if some other person get the mobile phone, he may misuse it. To address the problem, we are suggesting a mobile application that provides access control on the personal data in mobile of the user.

II. LITERATURE REVIEW

Privacy issues caused by mobile sharing can uplift a great threat to organizations as well as personal life. The following are the issues that focus on personal data privacy:

According to a survey conducted by the Ponemon Institutes, in an organization, the employees use approximately 23,000 mobile devices and 37 percent of them contain confidential or sensitive content. The data may be in form of documents, mail, excel etc. Most of the cases data loss is due to the sharing of mobiles with others and lack of governance. In general, an organization faces nearly $3.44 million per year due to lost or stolen data through mobiles [1]. In most of the firms many employees keep the confidential data related to their respective company in their mobiles and may protect them with a single pin or pattern but from past few years there have been many cases where the data is mishandled and sometimes used against the company. There may be a chance that because of the carelessness of the employee or sharing the phone with their friends, the data would have been compromised or stolen. Consequently resulting a huge loss for the company to recover from the breach.In some cases when we are in our own personal space, strangers may want to use the mobile for important purpose like an emergency message or call, so when we lend them the device they might misuse or alter the documents or even steal it.

When we consider our personal data at our personal spaces, the phones are not just used to store documents but also put pictures, lists, do online shopping, and almost everything. It is the latest trend, which is replacing the laptops and tabs. We can share the mobile with our family and friends but what if they alter the data or delete it. In 2009, Microsoft conducted a survey [2], which showed that almost every age group has suggested that the standard of mobile security should be increased. For example, if the mobile is shared with the children they may access the mails or may delete the pictures unknowingly. In contrast, when the mobile is shared with a stranger, he may use the personal data to threatthe owner. Therefore, in such cases, it is seen that owner are not comfortable in mobile sharing and permissiveness varies with respect to the owner's relationship to the other users.

So, from the above facts it is seen that today's mobile security measures are weak and do not adequately meet the user's security and privacy concerns when it comes to the personal data.

III. SYSTEM STUDY

Existing System:

The word 'lock' is relevant in every aspect of our modern lives. We lock our houses, cars, bikes, computers, and even our luggage when we got to the airport. There are lockers at schools, amusement parks, and sometimes even at the workplace. And also we lock up the individual apps in our mobile that house some of our most personal and sensitive data using the application.Mobile App lockers will allow users to protect their apps from misuse by locking the apps with the PIN that may be tied to a mobile security account.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

***Drawbacks of Existing System*:**

a) When user wants to open the app, user has to enter the password. It may be sometimes inconvenient for the user, to enter password every time.
b) The existing apps lock mostly the other apps. They are not able to lock native functionality i.e. voice calling, internet, camera etc.
c) Every time user has to search and select all the applications which he want to protect from others.

IV. PROPOSED SYSTEMS

We are proposing a profile based application that will allow users to protect their personal data from misuse. The app contains different types of user's profiles, such as, child, friend, guest etc. and specifies the list of native mobile functionality and applications that can be accessed in the profile. We can add or delete list of contents of the user profile whenever required.

The user can protect their personal data by selecting the profile according to the person to whom the mobile is to be given to. The person will be able to access only that functionality which are unblocked by user by selecting corresponding profile. Therefore, with the help of this application we can prevent unauthorized access of user's personal data.

Advantages of Proposed System:

a. User need not to enter the password every time when he open the app.
b. User will be allowed to block any functionality of the mobile phone, like, camera, voice calling, internet access etc.
c. User can add, delete and save the functionality to be blocked for a particular profile and activate whenever is required.

Feasibility Study

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited therefore expenditures must be justified. Developing an Android Application is cost effective because android is an open source project. Anyone can download an ADT bundle through internet and develop an app. Thus the developed system will be within the budget and this can be achieved because most of the technologies used are widely available. This application is technically feasible because user can run this app in any version of android.

V. METHODOLOGY

Development methodology is 'a way of organizing the work of software development'. One of the basic, most popular methodology for mobile application development is "agile methodology".

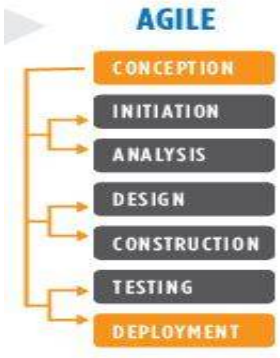

Figure1: Steps in Agile methodology

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Agile is an iterative, team-based approach for development. This approach emphasizes the rapid delivery of an application in complete functional components. Rather than creating tasks and schedules, all time is "time-boxed" into phases called "sprints." Each sprint has a defined duration (usually in weeks) with a running list of deliverables, planned one sprint in advance. If all planned work for the sprint cannot be completed, work is reprioritized and the information is used for future sprint planning. As work is completed during each sprint, it is continuously reviewed and evaluated.

VI. SIMULATION AND RESULTS

The application contains different user's profiles. When user selects a particular profile, all the installed applications and services in the mobile are listed out. Initially everything is in blocked state. The user can select the application or the services from the populated list, that he want to unblock for the current profile. While giving mobile to others, the user will select the required profile so that only desired applications are given access to. For ex.

a) Child requires access to only games and gallery. So, if parents want to give their mobile to child, then they can keep their kids locked out of the apps that would allow them to access internet, voice calling, Bluetooth-Wifi etc. which is not required for them.
b) If an unknown person is requesting for user's mobile to make a call then user selects guest profile, so that the person can use only the calling facility and remaining applications in the mobile are blocked.
c) When user wants to give mobile to a friend, he wants to protect the personal information like photos, emails and credit card numbers which is invaluable information. In addition, some of the most commonly used apps that do not necessarily require a login each time they are launched, like, Whatsup, Facebook etc. Therefore, we can protect those applications by blocking them based on profile.

Home screen:
When user opens the application, it shows the profiles with names Child, Friend, Guest etc. When user select one of the profiles all the installed applications and services in the mobile are listed out along with the checkboxes.

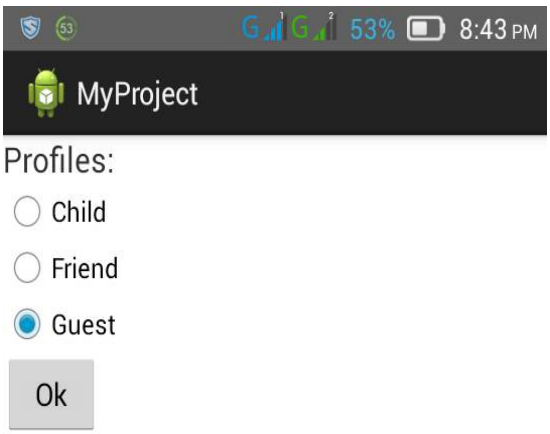

Figure 2: Home screen showing Child, Friend and Guest profile

App Screen:
Initially all checkboxes are checked and user can uncheck the particulars for which he wants to allow access to others for current profile.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

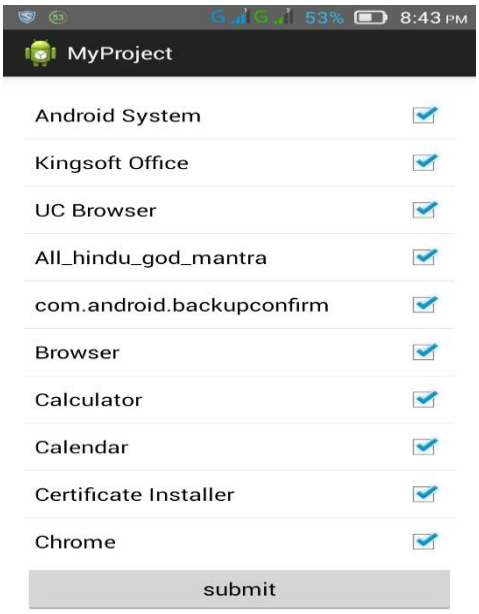

Figure 3: The screen with all the installed applications in the mobile.

Result

The application prototype was installed in 20 different mobile devices for the performance test and it was working well in the devices. We were able to restrict the unauthorized access to mobile content with this application

Advantages and disadvantages

Advantages:

a) We are able to block application based on the user's requirements.
b) User can give the mobile to anyone without worrying about the personal data in the mobile. The application controls unauthorized access of private data in the mobile.
c) The application is easily accessible to all the user's as it is developed in android.
d) We can block even native functionality of mobile by this application.
e) This application does not require internet connection.

Disadvantages:

One more application need to be installed in the mobile phones. We need to select the application individually from the available list to block it. Device may be sometimes a bit slow because of access privilege verification.

VII. CONCLUSION

Developments regarding mobile data privacy is crucial today, due to the huge opportunities offered by developments such as social networks, "Big Data" , cloud computing and IOT. The apps may secure our personal data but due to Bring your own device (BYOD) there are more chances of leakage of ones data in a company. Even if it is in industries or personals lives data privacy is as equal as the right to freedom .Since issues of data privacy in mobiles are increasingly becoming targets of threats like data breaches and data stealing. Though there are many problems in mobile data privacy, we have addressed one of the problems that is 'the need of access control for unprotected mobile data'. This problem is addressed by developing an android application that preserves mobile data privacy through profile based access control. The development can be extended to other mobile operating system, like iOS etc.

REFERENCES

[1] www.ponemon.org/-The Cost of Insecure Mobile Devices in the Workplace.pdf
[2] Amy K. Karlson, A.J. Bernheim Brush, Stuart Schechter Microsoft Research One Microsoft- Can I Borrow Your Phone? Way Understanding Concerns When Sharing Mobile Phones

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

[3] http://www.lexology.com/library/detail.aspx?g=d55b66e9-5ea2-4768-bb1a-5d843d54d813
[4] https://homes.cs.washington.edu/~syhan/papers/spsm4018s-jung.pdf
[5] http://www.dataprotection.ie/documents/guidance/Health_research.pdf
[6] https://blogs.mcafee.com/consumer/app-lock-the-security-system-for-unprotected-mobile-apps
[7] http://en.wikipedia.org/wiki/Information_privacy
[8] http://www.it.umd.edu/Publications/Data_Classification_Presentation022908.pdf
[9] http://www.gsma.com/publicpolicy/wpcontent/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf
[10] developer.android.com
[11] stackoverflow.com/questions/58116/get-application-name-from-package-name.html

BIIOGRAPHY

Sunil Singh is Assistant Professor in the Computer Science and Engineering Department, Rajiv Gandhi University of Knowledge Technology, Nuzvid AP. He received Master of Science (MS) degree in 2013 from IIIT Allahabad, India. His research interests are Information Security, Cyber forensics, Access control etc.

Pooja Singh is aBTech student in the Computer Science and Engineering Department, Radharaman Institute of Research and Technology, Bhopal MP. Her research interests are Computer Network, Mobile computing etc.

SkRizwana is aBTech student in the Computer Science and Engineering Department, Rajiv Gandhi University of Knowledge Technology, Nuzvid AP. Her research interests are Access control, Information security, Software development etc.