Privacy protection for preventing data over- Gathering Of user private information

Alin Mercybha P.J,Gnana deepika J.P, Aneka P, Rahini A
Department of Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai
***Corresponding author: E-Mail: alin@velhightech.com**

ABSTRACT

In present situation, all the data that will be stored in electronic devices. An android device is the mostly used to store the information and secure the data. However, the current devices lack behind in security and the privacy issues, when the data will get over-gathered. The objective of the project is to propose the way to protect the data over collection from the user's smart phone where as smart phone carries the whole details of the particular user such as username password from various accounts, user images, personal information's etc.

KEY WORDS: Android device, cyber security and privacy, data over-gathering.

1. INTRODUCTION

Cybersecurity aims at ensuring protection to the user personal information in a secured manner. Nowadays people use the electronic devices instead of traditional equipment. To use the system more efficiently, almost all these electronic devices need to be better enough to acknowledge different users and capable of storing and sharing data.

As shown in Fig.1, a techworld consists of various technologies, such as android, hotspot, Bluetooth, server service, Wi-Fi etc. Art systems form the backbone of the city's efficiency, liveability, and sustainability. In a techworld, people doesn't need to manage various kinds of cards, such as credit card, driving licensee card, and aadhar card. They can be acknowledged automatically by smart systems. To use various kinds of technologies, users must update their personal information to the systems. They must store their banking information and passwords for online shopping. To receive packages they must update their address. Consequently, user data are the core of a techworld, because they comprise all users' information, which is precious in the Big Data. In-spite of users suffering from privacy leakage they are enjoying the accessibility brought by the tech-world. In a tech-world various kinds of traditional systems has converted into smart systems, and coordinate their features into smartphones. Consequently, a mobile phone is the most often used electronic devices in tech-world, because of its accessibility. Using smartphones, users can access to the Internet via everywhere Wi-Fi, applying courses online, pay online bill, registering online, and getting medical prescription by tele-health. This smartphone will store user's data, but also collects data. These data also includes user's account numbers and pass-words, pin, emails and house addresses, videos, and other types of secured and private information. On the whole the security and the privacy becomes an important issue meanwhile, during these days, privacy and anti-virus apps have been developed, such as clean master, privacy app lock.

Figure.1. System model

In non-iOS systems other than in iOS systems, the researches show that there is malware in operating systems. It will prevent theft or damage to the hardware, software and to the information on them. The locked development makes no access to other permissions in the iOS app. To understand the data over-gathering, we initially analyses how these system works and the danger they brings to end users. We take location, photos, Videos, IMEI and IP address as cases and some apps are over-collecting users' data without observe them. Operating system and permissions are two aspects of data over-collection we store user data into smartphones and use them anyplace and any-time. However, some precise data may be stored into the smartphones such as password, contacts, some photos with confidential, and some other personal information. Storing user data into smartphones give potential privacy to users. We present mobile server framework, in that user information stored in server. Because of this, user data can be managed and provide encryption/decryption.

Figure.2. Mobile server framework

Related Work: In this section, we discuss how data over-collection problem can be solved by using various solutions. Active and passive methods are two approaches for defensive. Passive methods are monitoring and detecting, while Active methods are prophylaxis pertain. Data over-collection problem in current solution are passive measures. The communication became relatively simple because of the various facilities and the enhancement that is added in today's system. By examining the existing system we came to know that it lags behind in the field of privacy and security.

In a typical Tech-world, the security and privacy problem include several aspects, including privacy service, key management, precise data, and authorization. In current situation, most often used approaches for security and privacy in tech-world are precede from distributed systems. These approaches provides safe, secure, and consistent synthesis of distributed resource. For example, smart grid is an example using these techniques. In tech-world all these approaches are not enough, mainly for smart devices. Data processing becomes more complicated, which makes hard for data encryption, because of different data formats and protocol communication. Furthermore, Tech-world citizen put their data into devices for better ease. This kind of activity give different sources of harm to security and privacy problem. For example, virus in mobile and application permission, and servers hacking are common harmful activity in Tech-world

Controlling and detecting approaches in Mobile: Privacy leaks can be detected by egelectal. With the use of Static analysis, sensitive data can be detected in IOS.IOS application can be checked by PIOS by three steps. Firstly, find code path from starting point to sink by reconstruct flow graph. Second, find path in graph for interacting with network. Third, perform data flow path for sensitive information similar goal can be shared with pios, each discovered Taint Droid track. Strategy is real time analysis through three steps. First Step, Variable level tracking. Second, message level tracking can be used. Third, use file level tracking

Approaches for User-Aware: Enck (2011), Proposed an approach Kiri where they extract automatically the security way of Android apps. This security is evaluated against logic ways, before installing an application. Users has only permission for install the app if features are provided.

User-ware security control approach was proposed by Xiao et al to check how private information is used behind applications, static information can be used and classifier them as safe way or unsafe based on a tracked information .private data can obscured before access tracking, Then the choosing information with the help of platforms to give default settings that expose users' private data only for safe manner, thereby preserving security and reducing the burden for users deciding. These two methods to reduce the burden operation for users ,whether to allow permissions to access those apps that include security requirements .However, with the development of different approaches, Application developers will make more methods to program and to achieve the goal for user data collection, user data cannot be protected in passive approaches

Mobile Server Computing Offload: Related to mobile server computing, some researches can be proposed. Analyzed how computational offloading is suited among mobile devices. And also discover a framework to give runtime support for application execution. This frame-work support sharing among multiple user not only single user.

Figure.3. Home page

To achieve better utilization of server resources and to save mobile bandwidth is the main aim of these researches. Mobile server computing approaches focus on mobile applications execution using server, in our framework, not only for application execution but also the storing data in server.

Background: The most widely used android devices are the smart phone. Nevertheless, Present devices are not competent for the purpose of storing secured data. Current smart phone operating systems only provide partial permissions for any application to access personal information and providing details of how much is actually used and understands the pre-required information during installing it. The user can choose to uninstall the particular app even if it will bring some hidden security issues. We will be discussing the data over-gathering issues and then analyses these current status and risks.

Detecting Location: Location is most widely used data in the smart phone, wherever we are the GPS can be easily used to track the location and also directing to our destination, thus it is mostly used as maps .They also help in suggesting the shops nearby or the restaurant .This is done by allowing permission to the user or by setting the privacy and permission that is accessed by this app. The iOS software will be proving the facility to the user using which they can know their most frequent visits, whereas the features may not be available in the previous versions of iOS.

Accessing Photos: Album is also widely used in smartphones. Users take pictures not only for memory, but also for convenience such as taking photos of the slides instead of writing them down and print screening the route found by Maps. As a result, smartphones with large storage capacity hold increasing amount of pictures including life photos and information pictures. Since this is the most widely used application it needs to be protected by using the security issues. In fact, users use these apps to deal with just several or parts of photos, not all of them.

Accessing Contacts: To contact with others more convenient, users are willing to create new contacts, replenish existing contacts with e-mail address, new phone number, and remarks .The functionality of address book does provide users convenience for communication and work. However, accessing users' address books from apps brings serious potential security danger. The address book includes user names, physical address, phone numbers, email addresses, and other notes.

Accessing Calendar: Calendar apps are used in aim of organizing users' schedule, tracking events and reminding users of impending events. User stores the names and phone numbers for meeting attendees, meeting date, and time and attachments within the remark section. Both iOS and Android have their calendar apps attached in the operating system, and it is impossible to uninstall them unless jailbreak. Hence using this app we can access the calender and the features that the user wants to access.

The Architecture Design: It is impossible to enforce app developers not to share users' data with advertisement networks and other third party organizations, and it is unreasonable to expect that all smartphone users can understand permissions clearly and protect their privacy carefully. In fact the security problem is created by ourselves, and to solve it we have to change our patterns of thought, not to deal with aftermath but to eradicate it. We present a mobile-server framework, shown in Fig. 7. In this framework, all users' data is stored in the server, and smartphones only deal with some basic users' data are collected everywhere, such as paying bills by credit cards, registering into websites with apartment addresses, taking online courses using real name, and receiving tele health with personal information. All data are facing the potential hazard of being over-collected, especially in smartphones operations of apps, such as managing the apps and showing the result of them.

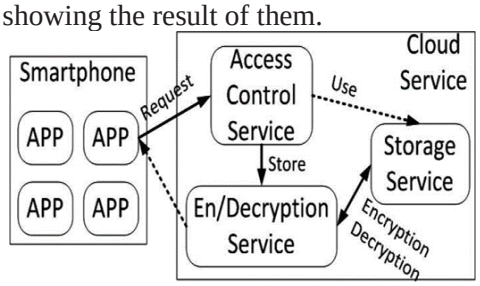

Figure.4. Access point specification

Smartphone users can be totally free of managing their data and have larger volume to install more apps by putting data into the server and letting the server service to manage data and security. Although the security of a server service is not perfect nowadays, server service providers are much more professional than app developers and users. Using server service, the operation of encryption and decryption of data can be finished in Server, and apps work as Data. The architecture of the mobile server will deal with the server. The server will be holding the entire data of the user personal information and will be performing all the requests that the user needs and process accordingly. Once the smart phone requests for the access control, it will be having all the permission to access the user personal data and also store the user data in the encrypted form.

System Models: In this, data are the most important for users to keep their privacy not exposed. Furthermore, smartphones, as the pivot of a tech- world, not only offer convenience but also undertake the responsibility of protect users' private data. However current smartphones are not competent for the job of protecting users' privacy. To

analyze and solve this problem, we define some terms used in our research. (Data Over-Collection). Collecting data more than enough on original function while within the permission scope. The data over-collection behaviors happens everywhere. For example, I take a picture and want to share it with my friends via some SNS app in my smartphone. For sharing this photo to my friends, I have to agree the per-mission request from this app. After authorize the access permission to this SNS app, all my photos are available to this app, but I only want this app to access one specific photo. As a result, this app may collect data more than enough on my original requirement while within the per-mission scope which I authorize. Users' data are collected everywhere, such as paying bills by credit cards, registering into websites with apartment addresses, taking online courses using real name, and receiving tele health with personal information. All data are facing the potential hazard of being over-collected, especially in smartphones

Data detection and updating on server: The tech-world application provided by the mobile server 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 server and creating an authorized account there selves through tech world application. This account maintains the credentials of users' can access their server data as Google drive wherever using their account credentials.

Figure.5. Data detection and updating on server

The application receives the entire data using the receiver services and it can update the respective account on server. The MCP provides security for data retrieved from the users' smart phones. Server 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 server storage. The entire smart device storage data can be accessed through the server which can be configuring and accessing by respective users. Once the data is detected we can easily update them on the server and based on our privacy we can set who can actually access the data

Security preliminary process on server service: Security preliminary process have implemented by the mobile server provider. Initially server 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 server. 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 server and can assign permissions for each of the application. The security will be totally enhanced by doing this the user will be needed to authenticate the data that require privacy.

Figure.6. Security preliminary process on server service

Data privilege on server mobile environment: Data privilege given by our mechanism is the online server drive for user's private data. Users can access their phone updates from the server. Using these privilege users can trace their phone while phone theft. Users can customize their phone's permissions on server hence we provide the data security. We proposed dynamic permission mapping algorithm to provide the customized application permission environment for data over collection as well as for phone application security. Highly secured and recommended cryptography can apply to the data security on future enhancement. Only once the data is successfully updated on the server, we will be able to gather the required set of information based on the user requirements. Hence only after the updation on the server we can perform the security related activities.

Application permission analysing on server: We proposed 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 server account of each user's. Hence once the permission is provided by the user we will be able to update or set the security for the application. Hence this application permission we will be able to analyse and detect the permission that should be given by us. Only the user who accesses the data

will be having the permission to access the particular data. Hence this is the final modal using which the data will secured in the cloud environment.

Figure.7. Application permission analyzing on server

2. EXPERIMENTS

To implement prevention of data over-collection in tech-world, we use four smartphones and one simulative server to build a simple mobile-server environment. Then we measure the performance and viability of our framework through following experiments. Using this we will be able to provide a secured data and we can store it in mobile cloud server. Hence this experiment is a look forward application development for the purpose of storing and retrieving the data from the server. Our server environment will be acting as a base for storing the data in the secured format.

Experimental setup: First, we set two structure: one in original environment and another in mobile server environment. Then we choose some apps from App Store and Google Play to value their security about unique device identifier (UDID), GPS location, photos, contacts, user-name and password. Finally, to trigger this prototype, we require computer which assumed as the server and mobile device as the experimental objects. We transmit the user data such as photos, mails, contacts, username and password from the smartphone to the server, and delete all these data from the device.

3. RESULTS

The main advantage of our project is to save storage space in users' smart phones. Users' native data includes photos, music, movies, videos except app data and system used data comprise 50 percent of smart phone's storage space. Such that most of the device's storage spaces are freed to install more apps. Thus we will be decreasing the risks that we generate while accessing the data and to reduce the danger that is caused by it. Thus we can secure our data in this kind of database and updating on the server such that we will be able to update it whenever possible.
We estimate the security risks of the apps in original and Mobile server environment and set four degrees to calculate the security risks of these apps as follows: Data can't be collected: 100; Data can't be transmitted: 70; Transmit data to app developers: 40; Transmit data to third parties: 10.

4. CONCLUSION

The most severe issue in smartphone is prevention of data over-collection. Unlike other issues, data over-collection is different and difficult to be solve, because they depend on authorization permission by the users. In-order to prevent data over-collection and to increase operation pressure to the user, we have presented an suitable approach. Every installed application send request to the server for accessing the user data, and the server access permissions to apps installed. Meanwhile the encryption/decryption service are used for encryption and decryption operations which saves data resource of device which deals with these complex calculations. Finally, experimental result validates the feasibility and advantages of our framework. Hence this will be providing the most secured form to safeguard out data and also promoting easy accessibility. The security will be totally enhanced by doing this the user will be needed to authenticate the data that require privacy.

REFERENCES

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

Egele M, Kruegel C, Kirda E and Vigna G, PiOS, Detecting pri-vacy leaks in iOS applications, in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp, 2011, 1–15.

Enck W, Gilbert P, Chun B.G, Cox L.P, Jung J, McDa-niel P and Sheth A.N, Taintdroid, An information-flow track-ing system for realtime privacy monitoring on smartphones, in Proc. USENIX 9th Conf. Oper. Syst. Design Implementation, 2010, 1–6.

Enck W, Octeau D, McDaniel P and Chaudhuri S, A study of Android application security, in Proc. 20th USENIX Conf. Secu-rity, 2011, 21.

Yibin Li, Wendyun Dai, Student Member, Zhong Ming, and Meikang Qiu, Senior Member, Privacy Protection for Preventing Data Over-Collection in smart city, Manuscript received, 2015.