A Survey on Privacy Issues in Smartphone Health Care Systems

Reena Prasad M. Tech. Scholar[#], [*]Dr. Tripti Arjariya

CSE Department, Bhabha Engineering and Research Institute, Bhopal (M. P.) India

[#]reenapsd@gmail.com

[*]tripti.beri@gmail.com

***Abstract*— With the increase of the popularity of Smartphone, enhancement in the Smartphone health care system is growing day by day. In era of digital communication doctors also using Smartphone to diagnose the disease of the patient's. It required privacy among patients' and doctor. Nevertheless, transferring the digital medical records through mobile devices brings on serious threats to patients' privacy. Mostly medical records are in form of images and already Smartphone endures from privacy issues. In this paper we focus on awareness about privacy issue related to Smartphone and their health care systems. We have also move towards survey of privacy issue of Smartphone health care systems and privacy preserving techniques. Therefore we have to plane to enhance security of the image storage in Smartphone through adopting the enhanced techniques.**

Keywords: Digital Omnivores, Smartphone Health Care, Privacy Issues, End User Privacy, Data Storage in Smartphone

I. INTRODUCTION

The first smart phones came onto the market in 1990s, yet in this era, Smartphone adoption among Users and Healthcare providers has increased substantially and mobile access to the internet is ongoing. According to the survey report, "2013 Mobile Trends Report" [1], 90% of healthcare providers are using Smartphone. Almost half of all respondents are "digital omnivores", defined as clinicians who utilize a Smartphone, tablet and laptop/desktop computer routinely in a professional capacity.

Smartphone renders the medical treatment of patient to be very flexible and comfort. A treatment system to treat patients remotely from the patient's home or their work place is to be comes under M-healthcare or Mobile-healthcare or Smartphone-healthcare. Although, finding the right balance between privacy and convenience will be challenging. HRI consumer survey of 2014 attain that data security is more important rather than the convenient access for 65% of respondents.

Smartphone works on different Operating System (OS). Among them, android is the fastest growing mobile OS in the recent years. The open source nature of the android makes it more attractive for the mobile companies. As it is open in nature so changes in it can be done according to the requirement. It provides a vast platform for the developers to explore the android operating system capabilities. Various developers provide applications to the user through android market, internet etc. If proper security measures are not applied by the developer then it may put the application at risk. Other than the application user's data is also at risk. To understand the behavior of the application, first of all android architecture need to be explored.

The Organization of the paper is as follows. In section II, types of data storage in Smartphone have been discussed. In section III, privacy issue of related to Smartphone have been explored. Section IV described the privacy issues related to Smartphone health care systems. Section V covered the background and literature survey related to the different privacy preserving schemes for Smartphone healthcare systems. Section VI summarized and concludes the survey.

II. DATA STORAGE IN SMARTPHONE

Smartphone stores the data at different locations. If the information store in these applications are accessible by some other application than it is potential for attacker to perform the attack on user's privacy. To overcome the privacy issues there is a need to understand the basic working of android applications, data storage process, and the privacy issues occur with respect to permissions. Data stored by these applications can be useful for forensic point of view also. In android applications data can be stored in 5 locations that is internal memory of the phone, SD card and to the server.

Shared Preferences: It is an android class that provides a basic storage framework to store private primitive data in key-value pairs. Primitive data such as Booleans, Floats, Ints, Longs, and Strings, persists across user sessions (even if android application has been killed). It is basically preferred to save relatively small collection of key-values.

Internal Storage: Application can directly store the private data in phone's internal memory. By default data stored in internal memory is treated as private to application. That is no other application can access that data. This data removed automatically at the time of un-installation of that application.

External Storage: An android mobile comes with an external storage medium. Application can even store there data in these external storage. But the data stored in this will

be available to all the other application also. User can modify or delete this data via connecting android mobile with the computer.

SQLite Database: Applications can use SQLite database to store structured data. The data stored in this is private to the application; no other application can access that data.

Network Connection: This can be used by web based services to store and retrieved data from web with network servers.

III. Privacy Issues in Android

Online privacy has always been a concern for internet users. A new survey by David Moth [14] shows that 89% British internet users admitted to being worried about online privacy. Main source of the privacy leakage in android is the installed applications. User may install the application in android device from the Google Play or unknown source also. Mainly user considers the popularity and features of the application to take a decision for installing the application. Google Play has more than one million applications and over 50 billion application downloads [12, 13].

A. Privacy Leak due to User Awareness-

Privacy preservation is most difficult task due to the attitude of client towards awareness of information disclosure through the use applications in Smartphone. Even though frequent awareness programs and research about the information leakage and disclosure a lot of end users are not fully aware. Even though few end users are aware however they are admissible to information leakage in favor of free available services.

B. Privacy Leak due to Application Permission-

Mobile applications are a privacy nightmare. Few android applications are frequently connected to the Internet and upload personal information such as photo gallery, medical records or personal documents, to a remote server without user's consent. These applications require a list of permissions that control accessing of sensitive information or use of restricted functions.

C. Privacy Leak due to the online advertising-

Advertisements on Web are mostly dynamic in nature. These may change frequently when the browser renders the HTML of the web page. The web site contains an ad tag (typically an <iframe> or <script> tag) whose *'src'* field is set to the ad server. User will be redirected to if they click the advertisement. It gives an opportunity to ad providers to execute snippets on Smartphone with identical permissions as the parent application has. It also uses library and allowing the ad providers to infiltrate data from Smartphone.

D. Privacy Leak due to the mobile messengers

Mobile messengers such as *'WhatsApp'* for android mobiles are also popular for social networking, connecting and sharing information. Smartphone users, having the mobile number of victim, may easily steal their image through just saving and accessing the WhatsApp profile DP of victim.

IV. Privacy Issues in Smartphone Healthcare

According to Privacy International: "Privacy is an essential right accorded to each person, the right to determine who can gain access to sensitive data and under what conditions" [2]. Smartphone communication allows colleagues doctors to have a live connection and make clinical decisions wherever they are. They can review images of medical records such as electro cardiographs, Instant Heart Rate, Stress Check, Lose it, Zocdoc etc. It resolves the issue of insufficient medical professionals especially in developing countries as well as the problem of the rising costs due to aging populations. Protection and privacy of health data against unauthorized use or disclosure, when using mobile healthcare devices, is very serious and important issue [3]. Data privacy in Smartphone has leaked due to the following reasons.

Data storage over cloud- Usually, the user would like use cloud services more frequently in the mobile operating system, which is caused by two main reasons: first, the mobile device has smaller storage; second, the mobile system updates more frequently. This fact explains the importance of this pattern. As shown in Table IV, this pattern reports the system shall always perform data encryption before uploading the data to cloud servers and use secure tokens for authentication. Meanwhile, the user must be noticed with the content of the cloud-based backup and is able to remove unwanted data from cloud servers any time through her mobile device.

Mobility- Mobile devices are easy to be stolen or damaged due to their portability and use. In addition, sensitive data is often prone to unauthorized use or divulgation because of the diversity of mobile applications and the utilization of mobile devices in different contexts such as checking and sending emails, internet browsing, social networking etc.

V. Backgroung and Literature

Smartphone healthcare systems have improved the patient's quality of care. The main contribution of this paper is to survey the major privacy issues in Smartphone healthcare systems. National Committee on Vital and Health Statistics (NCVHS) is the statutory public advisory body to the Secretary of Health and Human Services (HHS) on health information policy (HIP). Established in 1949 to offer guidelines and support on issues of health data related to privacy, confidentiality, data access, standards end so on.

NCVHS define the Health information privacy as the user's right to "control the acquisition, uses, or disclosures of his or her identifiable health data" [7]. HHS published a set of privacy principles for health information technology and a model privacy notice for MHRs (Mobile Health

Records) for comment [6]. But, to date, a final model notice has not been provided.

X. Xuan et Al. [4] study the privacy patterns for mobile operating systems with consists of two phases - privacy requirements elicitation and privacy patterns recognition. Requirement of privacy has been extracted in three ways-

- Through getting the knowledge from domain experts.
- Through carried out the literature survey on public documents of existing mature systems and
- Through feedback from real users.

On the basis of requirement analysis, author proposed 7 privacy patterns that are presented with the RePa Requirements Pattern Template. All of these patterns were refined by professional business analysts that concrete the result of work.

S. Avancha et Al. [5] survey the privacy challenges involved in mobile computing and communications technologies. Despite the benefits of Smartphone, privacy is necessary concern for personal monitoring technology like healthcare systems. In this paper author first develop a theoretical framework to resolve privacy issue of mHealth, second it itemize the privacy properties required for mHealth, and third, it discuss the technologies related to privacy of mHealth systems.

S. Sadki and H. El. Bakkali discuss about the efficiency of privacy preserving mechanisms used in existing mhealth care applications. Nature and the diversity of medical records shared between different bodies (Clinics, laboratories, physicians, pharmacies etc.) increases privacy and security risks. Thus, introduce a new conceptual module to preserve privacy in mobile healthcare based on encryption, anonymity and creating the culture of privacy and security awareness.

There are some limitation and problem in storing images securely in Smartphone devices. It is important to develop high security solutions to maintain privacy in order to expand the utilization of systems in the homecare field. S. Sadki and H. El. Bakkali [3] suggested that a privacy-preserving solution in mobile healthcare allowing patient to take control of their privacy preferences and ensuring a high level of privacy protection. But in this concept patients should not store their data on their smart phones. Also proposed a future work to develop and enhance each component of Privacy Module for Smartphone healthcare to fit with current Smartphone healthcare systems.

In this paper [3], author mainly focuses on two main concepts. First is the patient awareness about privacy that is not sufficient for privacy due to the variation on brain level of every patient. Second is privacy preference that uses encryption, anonymity and access control mechanism to mitigate privacy issues. But Smartphone application required permission before installation. Application having the full privilege may access the data from device rather it is protected from access list. And through accessing the file attacker also may decrypt it easily. Anonymity is also not feasible when using own Smartphone for storing healthcare data.

S. K. Manda and B. Hanmanthu proposed a privacy-preserving opportunistic computing framework for Smartphone healthcare systems with minimal privacy disclosure of personnel health information (PHI). This technique is based on attribute access control and MD5 message digest. They have suggested as future work to perform on Smartphone-based experiments to identify and verify the effectiveness of the proposed system. This technique has not been proficient with internal attackers.

H. Lin et Al. [9] concentrate on privacy problems of cloud-assisted mobile health systems. Developed a cloud based Smartphone health monitoring system to preserve the privacy patients and PHI. Researcher adopted the private proxy re-encryption technique to develop the cloud based Smartphone healthcare system. This technique increases the computational complexity of cloud service provider.

S. Kousalya [10] reduces the complexity of encryption in cloud based mobile healthcare systems through adopting the re-encryption scheme. This technique requires contribution of four parties for remote processing such as cloud service providers, patients, semi trusted authority and mobile healthcare monitoring system.

VI. CONCLUSION

There are few inadequacies and hindrance to store medical data securely in the form of images into own Smartphone. The first issue is the inadequacy of privacy preservation techniques due to the information leakage and end user awareness. Recent privacy-preserving solution in mobile healthcare systems allows patient to take control of their privacy preferences and ensuring a high level of privacy protection. It is inadequate and second issue due to the distinct level of end user's brain and knowledge.

Usually privacy preservation techniques in health care systems employs encryption, anonymity and access control mechanism. However, Smartphone application required permission before installation. Application having the full privilege may access the data from device rather it is protected from access list. And through accessing the file attacker also may decrypt it easily. Anonymity is also not feasible when using own Smartphone for storing healthcare data.

It is important to develop high security solutions to maintain privacy in order to expand the utilization of systems in the homecare field. Hence it is required to develop and enhance each component of Privacy Module for Smartphone healthcare to fit with current Smartphone healthcare systems.

REFERENCES

[1] Epocrates Inc, "2013 Mobile Trends Report", [Online]. Available: http://www.epocrates.com/oldsite/2014MobileTrendsReport/MT14_WP_03.pdf [Accessed:]

[2] K. Renaud and D. Gálvez-Cruz, "Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach", in Information Security for South Africa (ISSA), pp. 1-8, 2010.

[3] S. Sadki and H. El. Bakkali, "Enhancing privacy on Mobile Health: An Integrated Privacy Module", in Fifth Int. Conf. on Next Generation Networks and Services (NGNS), Casablanca, Morocco, pp. 245-250, 2014.

[4] X. Xuan, Y. Wangy, and Li Shanping, "Privacy Requirements Patterns for Mobile Operating Systems", in IEEE 4th International Workshop on Requirements Patterns (RePa), Karlskrona, Sweden, pp. 39-42, 2014.

[5] S. Avancha, A. Baxi and D. Kotz, "Privacy in Mobile Technology for Personal Healthcare" ACM Computing Surveys, Vol. 45, No. 1, November 2012.

[6] HHS, "Draft Model Personal Health Record (PHR) Privacy Notice", Dec.2008, [Online]. Available: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1176&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true [Accessed:]

[7] COHN, S. P. 2006. Privacy and confidentiality in the nationwide health information network [Online]. Available: http://www.ncvhs.hhs.gov/060622lt.htm. [Accessed:]

[8] S. K. Manda and B. Hanmanthu, "Privacy preserving support for mobile health care using message digest", Int J of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol: 3, Issue: 9, September-2013.

[9] H. Lin et Al., "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring", IEEE Trans. on Information Forensics and Security, vol: 8, Issue: 6, pp. 985 – 997, March-2013.

[10] S.Kousalya, "Privacy and efficiency on health care data using private proxy reencryption scheme", Int J of Innovative Research in Computer and Communication Engineering, vol: 2, Issue: 1, pp. March-2014.

[11] M-OWASP "OWASP top 10-2013, the ten most critical web application security risks", June 2013 [Online]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10 [Accessed: 1-July-2013].

[12] Nicolas Viennot, Edward Garcia, Jason Nieh, "A Measurement Study of Google Play", in SIGMETRICS'14, Austin, Texas, USA, June 16–20, 2014.

[13] Holly Evarts, "Crucial security problem in Google Play: Thousands of secret keys found in android apps", Columbia University School of Engineering and Applied Science, 2014 [Online]. Available: http://www.sciencedaily.com/releases/2014/06/140618163920.htm [Accessed: July 2014]

[14] David Moth, "89% of British internet users are worried about online privacy: report", Jan-2014 [Online]. Available: https://econsultancy.com/blog/64209-89-of-british-internet-users-are-worried-about-online-privacy-report#i.mtjtp18l2fj6xy [Accessed: July 2014]

[15] G. A. Di Lucca, A. R. Fasolino, M. Mastoianni and P. Tramontana, "Identifying cross site scripting vulnerabilities in web application" in Proc. of the web site evolution, Sixth IEEE Int. Workshop (WSE), pp. 71-80, September, 2004. [DOI: 10.1109/WSE.2004.10013]

[16] Pooja Khandelwal, Divya Rishi Sahu, Deepak Singh Tomar "A Security Survey of Android Smartphones", in 2nd Inte. Conf. on Advance Trends in Engg. & Technology (ICATET - 2014), pp. 550-553