Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.344 – 350

RESEARCH ARTICLE

An Android Based Medicine Reminder System Using External Storage

Prabhukannan.G[1], Liza M. Kunjachen[2], Dr. J. Jegadeesan[3]

[1]M Tech Student, Department of Computer Science and Engineering, SRM University, India

[2]Asst. Prof (O.G)/ Dept. of Information Technology, SRM University, India

[3]HOD, Department of Computer Science and Engineering, SRM University, India

[1] prabhukannan.rg@gmail.com; [2] Lizamk2006@yahoo.co.in

Abstract*— *In Modern healthcare most of the errors have been identified in Out-patient medication administration. These medication errors are caused due to under or over doses and forgot to take medicines at proper time. Because of these types of errors recovery from the diseases are getting delayed and the patient is suffering for more time. In this paper we introduce an Android based application for the patients. This application will remind the user to take proper medicines in proper quantity at proper time. Because of the android application portability could result in theft, so data security requirements need to be incorporated in the design process. In "Med Reminder" application, information on the device is encrypted and stored in the database, it is difficult to obtain illegitimately while still making confidential data easy to access. In this application, the data in databases residing on external secure digital card (SD card) of android devices are encrypted. In this paper, we discuss the technologies and methods used in android database encryption/decryption implementation and medicine in-take schedule to set reminder.

Keywords*— *Android; Medicine; Reminder; External Storage; Encryption

I. Introduction

The patient may be suffered from any kind of disease. In order to recover from the disease it is necessary to take proper medicine at proper time. It is necessary to take the proper quantity of medicine for the proper recovery from the disease .The patient may be Teacher, Student, Business man, Aged person. The patient may be busy in their daily schedule. Because of their busy schedule sometimes they may forget to take proper medicine in the time. Caretaker can remind the patient if they are near and in contact at the particular time. If the patient is far away from away from the caretaker it is difficult to remind them to take medicine in the particular time.

Currently there are many applications available in the smartphone for the sophisticated life [1]. Reminder facility in the mobile phone is one of the most commonly used applications which are used to remember each and every small thing. Majority of the Medication errors occurred due to one of the following reasons:

a) Lack of knowledge about proper use of medicines [2].
b) Because of the patient's busy schedule Medicine in-take becomes Improper.
c) Complicated in-take schedules Because of the large number of medicines taken by the patient.
d) Lack of knowledge about keeping records of the medicine in-take schedules [3].

In this paper we are introducing an Android application for the patients which will remind their user to take proper medicines at proper time by automatically setting the reminders in the mobile.

Because of the android application availability through internet, data theft also increases. So its need assurance that data are securely stored and safe from damaging compromise. Based on our observation, encryption is the only practical way to protect sensitive data given the ease with which devices can be rooted and security mechanisms defeated.

Android provides two primary methods for data encryption: whole device encryption or file encryption. This option encrypts all data saved to internal, private storage. Data stored in the private encrypted area can only be decrypted by the OS. Second way data can be encrypted on android regardless of where that data may reside (i.e., public secure digital [SD] card memory). This solution requires third party solutions or algorithms.

This type of data encryption implemented in this application.

"Med Reminder" can perform three primary functions:

1. Issue medicine in-take reminders - "Med Reminder" will issue an alert repetitively until it is cancelled by the user. Scheduling of in-take alerts is performed by real-time scheduling algorithms that can comply with the timing constraints specified by medication directions.

2. Maintain medicine in-take records - “Med Reminder" will record the time at which its user cancels an in-take alert and regard it as the time that specific medicine(s) was taken. The medicine in-take records can be stored on board, synchronize with the database.

3. It can securely save the medicine In-take data in external storage [5] by using AES algorithm.

II. Related Work

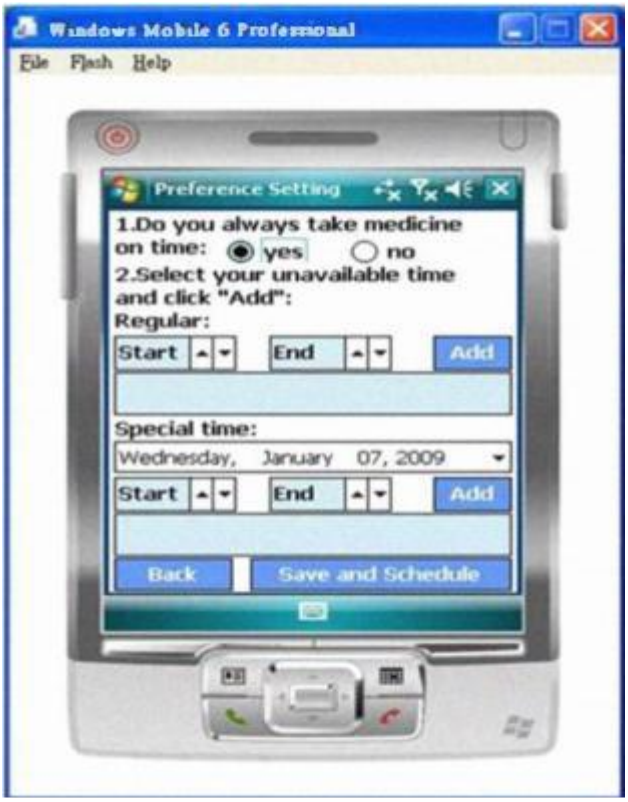
Wedjat - This application is developed by Zao J.K., Mei-Ying Wang, Peihsuan Tsai, and Liu J.W.S, to help patients to avoid medicine administration errors which are mentioned above

Wedjat can perform three major functions:

a) It can issue medicine in-take reminders

b) It can provide medicine identification and in-take directions

c) It can maintain medicine in-take records



1.Do you always take medicine on time: ● yes ○ no

2.Select your unavailable time and click "Add":

Regular:

Special time:

Wednesday, January 07, 2009

Fig. 1 Wedjat – Smart Phone Application

III. ANALYSIS

A. *Findings in the existing system:*

- Stores all the data in the file system and provides the in-take reminder.
- Stores all the data in Original plain text format.
- Stores all the data in internal storage initially.
- Remind only the Patient about the medicine in-take.

B. *Existing system has some major drawbacks which motivate us to develop new system. Those drawbacks are as follows:*

- Occupies more storage space in internal storage.
- Stores the data in unformatted file format, it is difficult to maintain the data while the data becomes huge.
- User needs perform special mechanism to store the data externally.
- Stores the data in plain text, it is easily readable by the online attacker.
- There is no facility to add Caretaker details.
- There is no facility to send reminder to the Caretaker.
- There is no facility to provide any indication about end of medicines and doctor's next appointment.

IV. PROPOSED SYSTEM

Android [5] is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers, Developed by Google in conjunction with the Open Handset Alliance. The proposed system is an application for the Android platform mobiles will remind their user about the medicine in-take schedule. This reminder will be set in the mobile with the help of the Calendar application [6].The proposed system will be developed for Android mobiles only because the market share of Android is more than other operating systems [7].

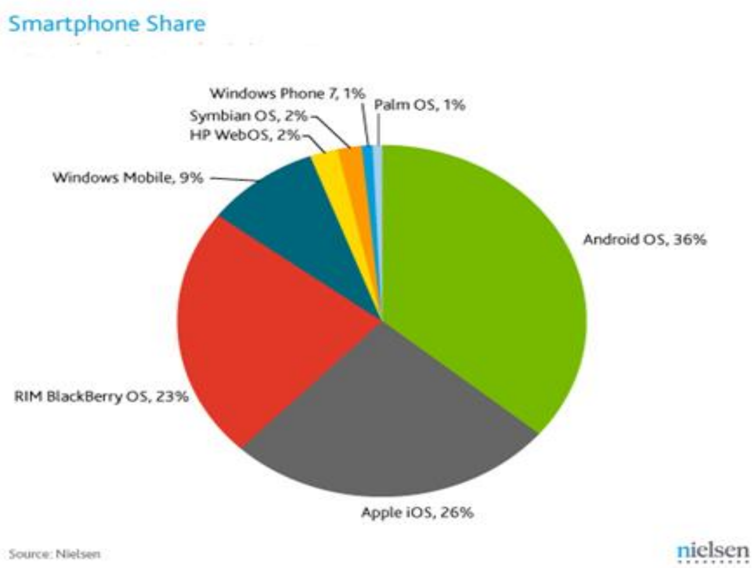


Fig. 2 Mobile OS Usage Analysis

A. *Need of New System*

The existing systems are very useful; they are providing very nice facilities to the user about their medication reminding & scheduler. But as we see in analysis section, the existing systems were developed with lots of major observed drawbacks which need to overcome by developing new system.

The existing systems are not providing any notification about doctor’s next appointment, also the end of dose/medicine.

The existing systems have no facility to store the records in external storage. The existing systems have no facility to store the records securely [8].The existing systems have no facility to send alerts to patient's care taker.

So there is a need of developing such system which will try to overcome all the drawbacks of the existing systems.

So we are taking the initiative for developing such full-fledged system which we are proposing will securely store the Data in external storage. Our system will also automatically give notification about doctor's next appointment and send alerts to patient's care taker and also provide the facility to store the records in external storage securely.

V. System Overview

The input includes

- Medication Name.
- Medicine in-take Duration.
- Times of the day to take drugs.
- Number of Dosages to take.
- Caretaker contacts.

After obtaining the inputs, mobile application securely saves the data in external storage. Output includes medicine in take records and medicine reminders. After system produced an in-take reminder, it prepares the time schedule it sets of the alert at proper in take time. If the patient forgets to take their medicines then our system reminds them about medicine in-take time and sends the alert to patient's Care taker.

All Inputs are encrypted and stored in SQLite database, which will be stored in external SD card. Then the output generated by decrypt the encrypted data from SQLite database. For this encryption/decryption process AES algorithm is used.

During encryption/decryption "Med Reminder" uses the IMEI-IMSI number for key generation. Key is generated during encryption /decryption process. It generates the same key dynamically at every time. It reduces the possibility of Key theft during online access.

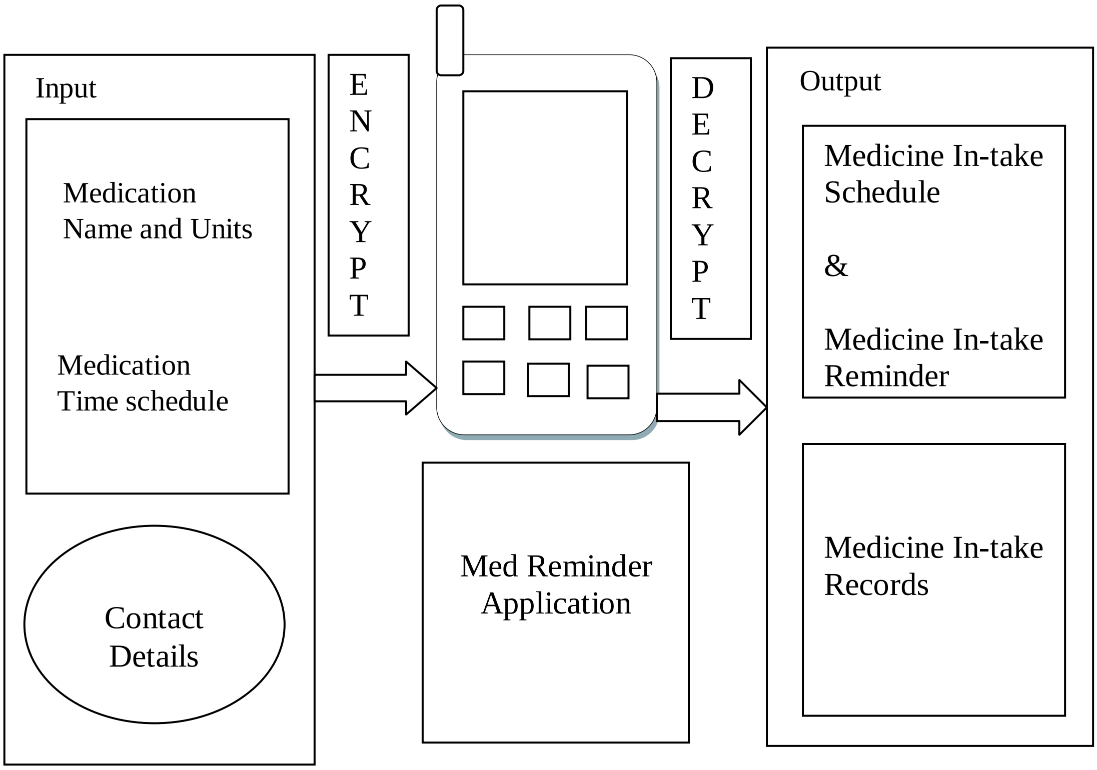


Fig. 3 input and output data flows of the proposed system.

VI. External Storage SD Card

Most of the Mobile phones have lesser internal storage. It can hold only lesser data. By using External SD card [9] application can store more data. Especially for larger files, external storage is the best option to save the file because internal storage space can be very limited depending on the device of your user.

Using External Storage is a great way to expand the amount of storage of the application use locally on the device.

A. SQLite in External Storage

SQLite [10] supports standard relational database features like SQL syntax, transactions and prepared statements. In addition it requires only little memory at runtime (approx. 250 KByte). SQLite is a software library that implements a self-contained, server less, zero-configuration, transactional SQL database engine. SQLite is the most widely deployed SQL database engine in the world.

SQLite supports the data types TEXT (similar to String in Java), INTEGER (similar to long in Java) and REAL (similar to double in Java). All other types must be converted into one of these fields before saving them in the database. SQLite itself does not validate if the types written to the columns are actually of the defined type, e.g. writing an integer into a string column and vice versa.

SQLite is available on every Android device. Using a SQLite database in Android does not require any database setup or administration. The SQL statements for creating and updating the database must only be defined and the database is automatically managed for users by the Android platform. SQLite database is kept in a single file somewhere in the /data/ directory. Data are kept in Plain text format. This means that it will always be possible for someone to extract that data by rooting the phone obtaining the .db SQLite file and opening it with a text editor.

So the data will be encrypted, before enter into the database and store that database file in external SD card.

B. Security

Generally data present in the external storage are less secure because of its public access. Attackers can get the information present in external SD card without the knowledge of user.

Attack may happen in the following manner.

1) User may visit malicious web page during surfing over the internet.

2) Attacker can get the information present in the database through client side script. This type of attack is called indirect attack.

3) Attacker can get the data present in the external SD card while the card is used with other devices also. This type of attack is called direct attack.

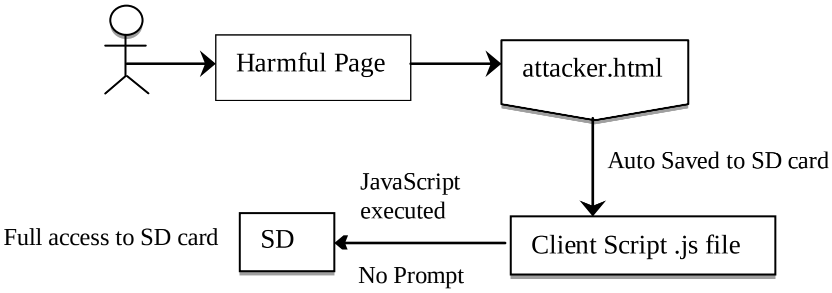


Fig. 4 Data access indirectly by client script

So it is necessary to store the values in encrypted format in SQLite Database.

"Med Reminder" application uses AES algorithm in order to perform encryption.

"Med reminder" application stored within the internal memory (Built-in memory) of the device.

Internal memory is more secure than the external memory.

"Med Reminder" application generates the random key and it is stored within the application.

This key is used for encryption. Encryption is performed at the time of storing the data in external SD card. So encrypted data only access through application, not able to some other means.

C. Encryption Using AES Algorithm

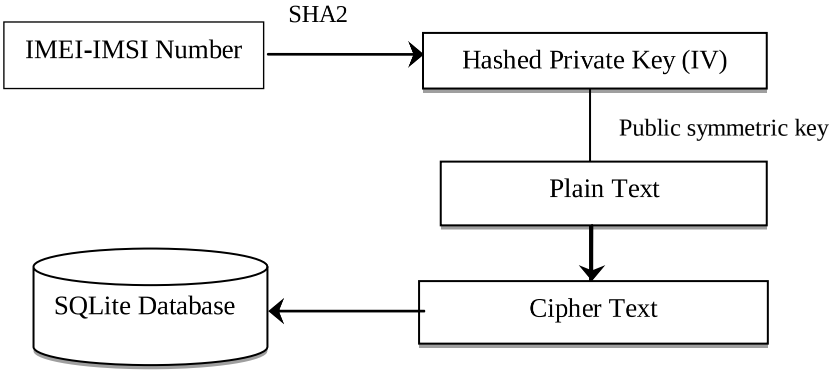


Fig. 5 Data Encryption using AES

In this application, Get IMEI - IMSI numbers as input and used as key for AES algorithm and performs encryption using 128 bit key. Our approach requires the Mobile IMEI-IMSI numbers as a private key input. Application uses the Secure Hash Algorithm (SHA2) to encode the key. Android device uses the hashed private key as the public symmetric key passphrase and plain text as inputs into the 128-bit AES encryption algorithm. The Scrambled cipher text is then stored by application in the SQLite database which is residing the external SD card for future access.

To decrypt the cipher text, the same hashed private key as key and decoded the SQLite data.

VII. CONCLUSIONS

For some phones and devices (especially the older ones) the internal storage is quite limited. Every application and its data files take precious space. In this paper an attempt has been made to implement store the data in external storage. In order to improve the security of data in external storage [11], AES algorithm has been implemented to encrypt the data in proposed system. The proposed system reminds user about their medicine in-take schedule. The system which we are implementing will also give the reminder about doctor's next appointment. It will also tell the user about the end of the medicines.

The proposed system also has the facility to add caretaker's contact details and send reminder to them. In future additional file-level encryption could be provided to encrypt whole database file.

File level encryption of database prevents manipulation of database schema.

In Med Reminder Data Stored in encrypted manner because of this we are unable to use some of the SQL's built in functionality.

For example we cannot use SQL ORDER BY clause when retrieving data from the database because of encryption of Data.

Sorting of encrypted data requires implementation of holomorphic encryption algorithms, [12] such as Crypt DB [13] that are not available in the Android platform.

REFERENCES

[1] E. Cuervo, A. Balasubramanian, D.-k. Cho, A.Wolman, S. Saroiu,R. Chandra, and P. Bahl. Maui: making smartphones last longer with code offload. In Proceedings of the 8th international conference on Mobile systems, applications, and services, MobiSys '10,pages 49–62, New York, NY, USA,2010. ACM.

[2] Wan D, "Magic Medicine Cabinet: A Situated Portal for Consumer Healthcare," Proceedings of 1st International Symposium on Handheld and Ubiquitous Computing (HUC '99), September 1999.

[3] Govemo M, Riva V, Fiorini P, Nugent C, "Medicate Tele-assistance System", 1 th International Conference on Advance Robotics. June 2003.

[4] 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 real time privacy monitoring on smartphones. In Proceedings of the 9th USENIX conference on Operating systems design and implementation, OSDI'10, pages 1–6, Berkeley, CA, USA, 2010.USENIX Association. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[5] http://en.wikipedia.org/wiki/Android_%28operating_system%29*FLEXChipSignalProcessor (MC68175/D)*, Motorola, 1996.

[6] http://developer.android.com/reference/android/provider/CalendarContract.Reminders.html

[7] http://www.devworx.in/news/android-news/android-defeats-all-others-in-South-east-asia-market-survey-122301.html.

[8] M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu, and D. S. Wallach.Quire: Lightweight provenance for smart phone operating systems. In 20th USENIX Security Symposium, San Francisco, CA,Aug. 2011.

[9] http://developer.android.com/guide/topics/data/data-storage.html.

[10] htttp://www.sqlite.org.

[11] ”Android security overview,” http://source.android.com/tech/security/index.html.

[12] Cooney M. IBM touts encryption innovation; new technology performs calculations on encrypted data without decrypting it [Internet]. Computer World; 2009. http://www.computerworld.com/s/ article/9134823/IBM_touts_encryption_ innovation.

[13] Popa RA, Redfield CMS, Zeldovich N, and Balakrishnan H. Crypt DB: protecting confidentiality with encrypted query processing. SOSP ’11, Proceedings of the 23rd ACM Symposium on Operating Systems Principles; 2011 Oct 23-26; Cascais, Portugal. New York: ACM; p. 85-100.