IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 30-32

An Android Application For Protecting Personal Information Using Fingerprint Encryption

Rinisha Burriwar , Sayli Dhotre
Professor: - Snigdha Bangal, Supriya Mandhare
Department: - Information Technology of Atharva College of Engineering (Malad West), Maharashtra, India.

Abstract: *In developing countries like India there is strong focus on data security. New encryption algorithms and softwares are built every year. The maintenance of these encryption systems is many times overlooked. Whenever private information gets leaked, many people and organizations face huge loss. Hence, we are developing a note taking software that will secure the personal information of user efficiently by using finger print encryption for individual note. Here, we are going to use the highly efficient algorithm, i.e., the AES algorithm, to encrypt the information and fingerprint hash values and provide security to the user's sensitive information.*

Keywords: *data security, fingerprint encryption, android notes*

I. Introduction

There is an exponential increase in mobile thefts every year. Most of the newer technologies tend to ignore the most basic utility application, i.e., the notes taking or the Memo application, let alone be securing them with better encryption techniques. Hence, there is a need to create a software that will encrypt the user's personal information by user's biometric key which is, the user's fingerprint and decrypting it with the same. Here, we need to work with the user's fingerprint and with a highly capable algorithm. The security of the application will be such that even if the mobile gets stolen, the thief will not be able to access the private and sensitive information. Even if he somehow manages to access the data , the data will be in an encrypted form and the key to that data will only be known to the owner of the mobile.

The main objectives of our software are to encrypt user's individual notes, to provide security to user's sensitive information when his/her mobile is lost, to improve the data efficiency, to overcome the increasing security attacks.

Application and Scope of the system:

Confidentiality in Storage:- The information is only encrypted when it is in storage, not when in use by the user.

Authentication of Identity:-Authenticating the identity of individual user to the system has been a problem for a very long time. The selection of keys has proven to be a cause of cryptosystem failure. Hence we use the user's fingerprint as a key, thereby providing maximum security to the private data.

II. Problem Statement

The notes application must be such that there must be a choice for the user for encrypting the data in his way of ease whether it be pin or a fingerprint and must have a no nonsense straightforward and yet an attractive and easy to access UI.

The current scenario in the notes application is diverse, with technology growing rapidly in the tiniest aspects of our lives. There are the basic notes application like the in-built notes application in our devices or the application developed for the sole purpose of taking lecture notes digitally without using a book and a pen[1].

There are also some note taking applications where voice technology like audio navigation and audio searching is used for example, the My Notepad[2].

But , there are some aspects in this area of application which are still untouched. One of those aspects is security. The only encryption method available in this domain is the basic key encryption. This kind of encryption is easier for hackers to decrypt and view the data with ease.

Hence, we are developing a software that uses fingerprint encryption and also provides security to notes individually.Moreover, the user has a choice to choose his way of encryption be it finger print or a basic pin.

III. Proposed System

The prevalent use of mobile devices has been majorly changing our living style. Along with great ease and efficiency, there are new challenges in protecting sensitive and/or private data carried in these devices. The most challenging part is while the software should be made complex enough for hackers to struggle decrypting the data, the cryptographic function should be efficient for authenticated users and easy enough to use. This paper proposes an efficient data encryption and storage scheme to address this challenge. Here, we are going to use the AES algorithm and salt for extra security.

Key management is an important problem in traditional symmetric cryptography. Maintaining privacy of cryptographic key determines the security of cryptography. Biometric is the alternate to maintain the privacy of key by protecting it with users biometric from unauthorized access. A string of binary number as cryptographic key is extracted from fingerprint template and this key is used to encrypt a message. During decryption process, the user is able to generate that cryptographic key from a fresh fingerprint instance to decrypt the encrypted data.

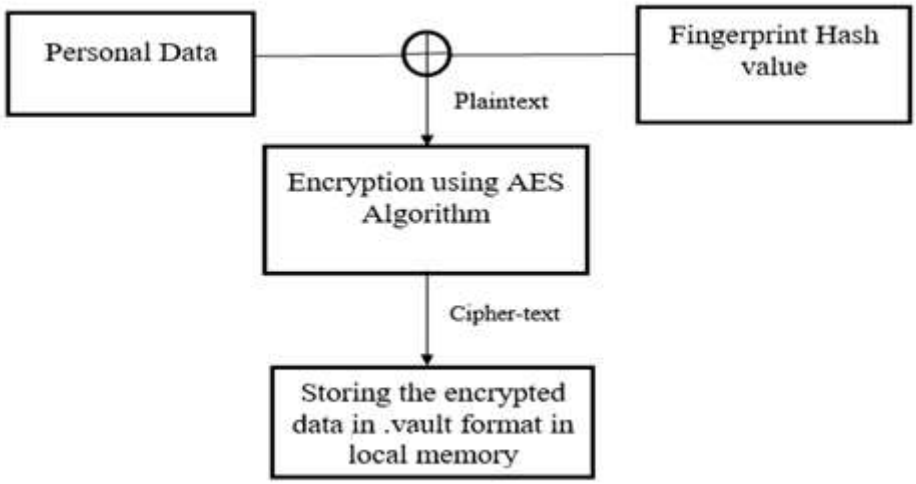

Fig.1: BLOCK DIAGRAM FOR ENCRYPTION

The encryption method will take place as follows:

The user will start with creating a memo for storing his/her personal data i.e., the plain text. The system then,asks for user's fingerprint. The fingerprint will not be stored directly in the system. The fingerprint's hash value will be then combined with salt and the personal plain text will be encrypted using AES algorithm. This encrypted data will then be stored in local memory in the .vault format.

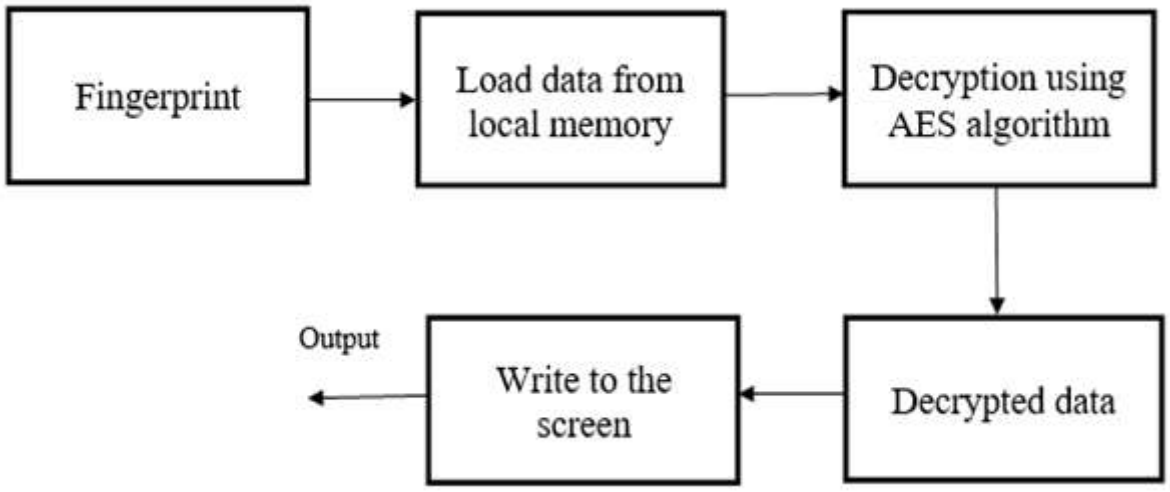

Fig.2: BLOCK DIAGRAM FOR DECRYPTION

The decryption process will take place as follows:

The user will try to access the stored and encrypted data in the system whenever he needs it. The system will then ask for a fresh instance of the user's fingerprint which will be compared for authenticity with the stored fingerprint value. After successful decryption, the data will be made available to the user to view and modify.

IV. Conclusion

The need for personal data privacy is increasing day by day due to increasing number of hackers and breaching activities. So our application provides a unique way of encrypting data by using fingerprint encryption which is more feasible and secure. After implementing the system its advantages will be incomparable to the present contemporary systems available in the market. The most admirable feature found is its user friendliness in terms of application to the user but its highly beneficial outputs which cannot be ignored. There is always a space for improvement in any software, however efficient and capable the system may be. The system is flexible enough for future modifications.

References

[1]. 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.Education and Learning Support System Using Proposed Note-Taking Application. M.Numazawa, K.Ai , M.Noto.

[2]. International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March- 2015.Android Application Development & Its Security.S.Mukerjee, Prof. J.Prakash , D. Kumar.