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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Enhancement Technique Use for Security of Digital Data in Mobile Devices

Nitesh Patil, Akshay Kulthe, Kiran Nagarkar , Rupesh Shinde

Dept. of Information Technology, Marathwada Mitra Mandal's College of Engineering, Pune, India.

ABSTRACT: In this paper, we are presenting a proposed system for Information Security Based private data of mobile devices. So our system is use for security of personal information of users. System processes user's data as encrypted format and store on the hosted server. As per users need, he can request his data through the android application and he can authenticate himself to machine and then need to authenticate his device through the OTP service and after this stage, key is generated to decrypt the data. Which is send on the alternate mobile number which will help user to get his data secure, even he lost his mobile device. As data is in encrypted format so no need to worry about the data, because here we provide users a perfect data security application

KEYWORDS*:* AES, Decryption, Data, Encryption, OTP.

I. INTRODUCTION

Mobile devices have become popular in the community for the ease it provides to the user, it's not only a way of communication but a technology which can help to store, transfer data. Important aspect which we cannot neglect is m-commerce which is now getting a hike in business. All of these benefits have raised the chances of theft to the devices and the data stored in it. Security has become great concern to the users as well as business which make use of such devices. The Self-Encryption (SE) Scheme for Data Security in Mobile Devices introduce in this paper, whether it is possible to implement a lightweight encryption algorithm which provides data confidentiality by exploiting the availability of a secure connection with a central server. The server is used to store a small amount of data, required to decrypt the confidential information. In case of loss of the device, the access to the company server is temporarily revoked. Proposed system store user's data on server in encrypted format as even theft cannot access the mobile device data.

II. IMPLEMENTATION DETAILS

The system application is developed or implemented in the
Android studio which is integrated development environment (IDE) for Google's android operating system. built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. For using this toolkit developer must need minimum knowledge of JAVA. The design of the application is done through the XML(Xtensible Markup Language). Which related with the JAVA file which is logic behind the every action done through the user-interface.

III. MATHEMATICAL MODEL

Let us consider S as a system for storing mobile device file on server
S= {……
INPUT:
Identify the inputs
F= {f_1, f_2, f_3 ……, f_n| 'F' as set of functions to execute commands.}
I= {i_1, i_2, i_3…|'I' sets of inputs to the function set }

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets,}

S= {I, F, O}

I = {File uploaded by user, i.e. File }

O = {Output of desired query, i.e. Encrypted file stored on cloud}

F = {Functions implemented to get the output, i.e AES Algorithm}

e = End of the program.

Φ = Failures and Success conditions.

Failures:

1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

Success:

user gets file within time after entering key within time.

Algorithm:

This algorithm we used for encrypt the file while storing on server.

Introduction:

AES(advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algorithm is weakness in DES. The 56 bit decryption key is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used128-bit block with128-bit keys.

Input:

128_bit /192 bit/256 bit input(0,1)

secret key(128_bit)+plain text(128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

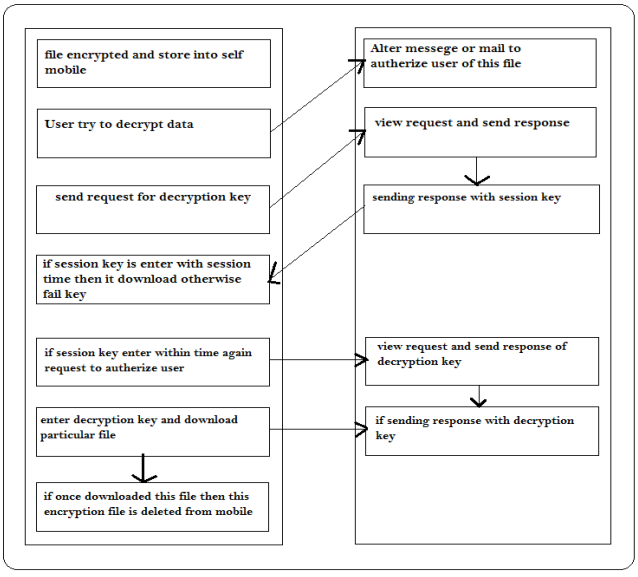
XOR state block (i/p)

Final round:10,12,14

Each round consists:sub byte, shift byte, mix columns, add round key.

Output: cipher text(128 bit)

V. SYSTEM ARCHITECHTURE



:

fig 1. System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Proposes a novel data encryption and storage scheme to address this challenge. Treating the data as a binary bit stream, our self-encryption (SE) scheme generates a key stream by randomly extracting bits from the stream. The proposed system user store his mobile data file on server that will be in encrypted format. When user want to download the file that time user have to enter OTP if OTP matches then user will get decryption key on second mobile no. of user if user enters that key and key matched ,While entering key user have to enter that key within time that time only file will decrypt.

Advantages:

1. An unauthorized user try to access data with key then he/she first send request for key to decrypt data.
2. Session key is used for more security purpose.
3. Data stored on server, so user can get data anytime, anywhere.
4. If mobile lost, key and OTP will send on another mobile device.

VI. CONCLUSIONS AND FUTURE WORK

We present a novel scheme for storing mobile data securely on server. If in case mobile device is lost user will get secure data on another mobile number of user. User will get OTP and decryption key on second mobile number of user. User have to enter key within session time. Here data stored on webserver is in encrypted format. So no one can recognize that stored data on server.

REFERENCES

[1] J. Al-Muhtadi, D. Mickunas, and R. Campbell, "A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices," *IEEE Wireless Communications*, April 2002.
[2] C. Galdi, A. Del Sorbo, and G. Persiano, "Distributed Certified Information Access for Mobile Devices," *Workshop in Information Security Theory and Practices* (WISTP'07), Crete, Greece, May 8-11, 2007.
[3] Y. Jiang, C. Lin, M. Shi, and X. Shen, "Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 9, Sep. 2006.
[4] V. Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," *StorageSS'05*,Fairfax, Virginia, USA, Nov. 11, 2005.
[5] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Surveys*, Vol. 35, Issue 3, Sept. 2003.
[6] A. J. Nicholson, M. D. Corner, and B. D. Noble, "Mobile Device Security Using Transient Authentication," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1489-1502, Nov., 2006. and Security Aspects
[7] E. Zenner, Why IV Setup for Stream Ciphers is Difficult, in Proceedings of Dagstuhl Seminar on Symmetric Cryptography, Jan. 2007.
[8] P. E. Sevinc, M. Strasser, and D. Basin, Securing the Distribution and Storage of Secrets with Trusted Platform Modules, Workshop in Information Security Theory and Practices (WISTP07), Crete, Greece, May 8-2011.