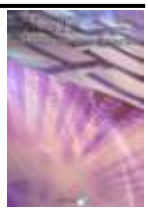

Data Encryption Using Modified AES for Android Mobile

Ahmed Tariq Sadiq[1], Faisal Hadi Faisal[2]

[1,2]Computer Science Department, University of Technology Baghdad, Iraq

drahmaed_tark@yahoo.com, myemail_welcome@yahoo.com

ISSN: 2231-8852

ABSTRACT

Smartphones are very common and deal with sensitive information. The personal information is very important and should be protected. Data is often exposed to attack because it is considered confidential data. There are many applications on smartphones that use passwords to protect data in mobile, these applications are weak because the password is easily broken. For this reason, encryption algorithm should be used to preserve data in mobile and encryption is very important for keeping confidential data. There are many encryption algorithms to ensure the security of data but the selection of the algorithm should dependant on fast, strong and implementation features. For that reason, we choose the advanced encryption standard (AES) algorithm for encryption data because of its speed and easy implementation on small devices and has some other features and modified AES for increased speed computation process for encryption and decryption, and efficiency of security of file encryption.

Keywords: AES, Block Cipher, Extended Key, Extended Plain Text, Cascaded Keys

1. Introduction

The rapid evolution is taking place in mobile device compared with a personal computer and has become more important to deal with sensitive data or personal data. This data in the mobile device should be protected from unauthorized access or theft (Skillen, 2013). The way to protect data is encryption of this data and choosing the best encryption algorithm for encryption (Martinez, 2012). Therefore, AES algorithm will be chosen with modification, to make it different from the classic algorithm. It is considered as the most important encryption algorithms today and has some features such as highly secure, simple design, and very fast. The modified AES algorithm focuses on the increase in the speed process for taking less time for encryption and decryption, because the mobile device has specification less than computers, and at the same time should have increased security (Scripcariu & Frunza, 2012).

2. Related Work

Mandavkar et. al. (2014) presented secure SMS message between phones only. To achieve high security to SMS, two cryptographic algorithms were combined. First, PBE (Password-Based Encryption) password was used for generation key for encryption and decryption and

add some random of bytes to the key. The second algorithm used was Diffie Hellman key, exchange algorithm is used to exchange key between sender and receiver, third use AES for encrypting the data of the message, and finally hash function is used to generate a hash value (manipulation detection code). The data message contain voice data, fax, image, video data, and text data.

Al-Hassan et. al. (2013) presented data security between smartphone and cloud. It used two algorithms for encryption, first, it used public key encryption by using RSA algorithm between smartphone and main server to prevent an attack on data in the communication, and second, it uses private key encryption algorithm DES for encryption data on the server, to prevent authorized access to data stored on the server. The decryption key is not stored in the server but stored in a smart device.

In Naik et. al. (2014), encryption and decryption of data and messages by using AES symmetric algorithm, and using Elliptic Curve Cryptography (ECC) asymmetric algorithm to generate key (public key) used to exchange key between phones was presented. This paper allowed the user to encrypt data in a smartphone before transmutation in channel communication network. This system provides reliable, security, confidentiality, authentication, and integrity of data. At receiver, the user uses the same key for decryption of the data.

3. Mobile Device Security

Mobile device security is the protection of the system and personal data stored on the mobile device. The aim of security of mobile includes saving the devices from disclosure, theft, recording, unauthorized access. The main responsibilities of device security are maintaining "the confidential", "integral", and "available" information to the user. The amount of data that it handle in the mobile devices has become one of the most security challenges facing mobile (Martinez, 2012).

Confidentiality keeps specific information stored on the device from disclosure to a third party (ex: protected data credit card transaction is done on mobile from unauthorized hands). Confidentiality is an important factor to secure the system, but it's not enough to provide complete security on the system (Martinez, 2012).

Integrity is considered one of the pillars of mobile security. The major function of integrity is to ensure the data is not modified without modification by the system. This leads to all data accessed by the user is trustworthy. The system provides message integrity with data confidentiality, to ensure the data is not manipulated (Martinez, 2012).

Data available is when the user requires it. That means the system must save and process the data, a method is used to preserve it, how to get to the data, and transfer it correctly to work on inside system. The system is secure when the data is confidential, integral, and available (Martinez, 2012).

4. The Proposed System

The proposed system represents the internal work of system to protect mobile data. Part of the system is done by the user such as selecting data which will be encrypted, and the user

should choose the initial key that is used in encryption process (user enters initial key for all encryption process and can change the initial key at any time). The other part of the system works internally after the user selects the data or chooses an initial key, this part represents the algorithms to encrypt data and algorithm to generate a key (Ahmed & Faisal, 2015). Figure 1 illustrates how the system works.

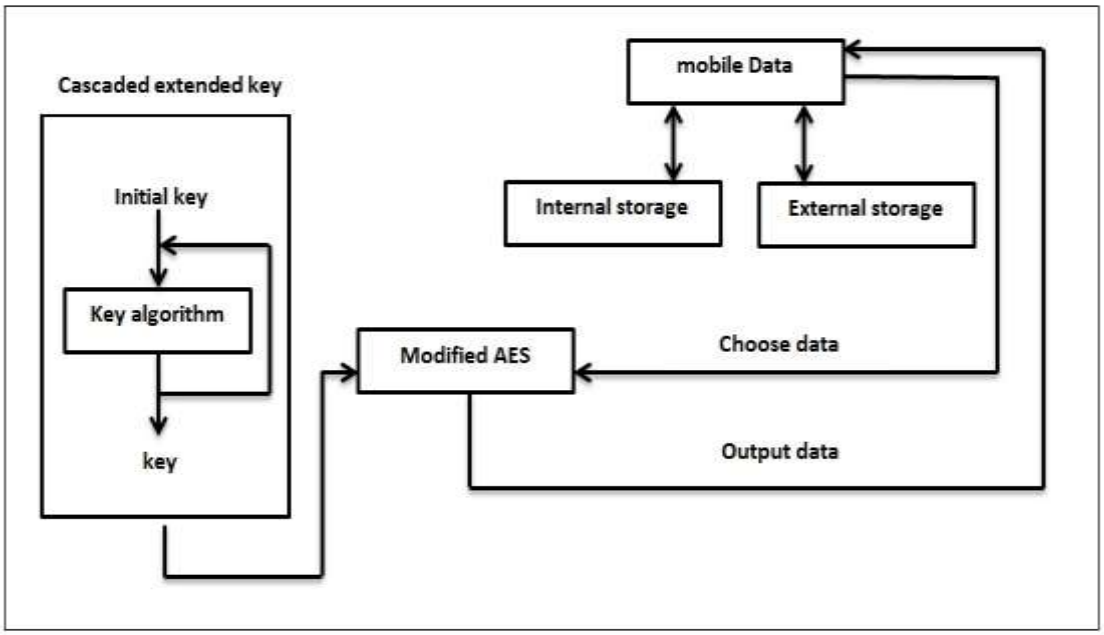

Figure 1: The proposed system

From figure 1, it was observed that the system is divided into three parts. The first part represents the mobile data, the data is stored into two sub-parts (internal storage, external storage), and the file selected by the user from data is transferred to proposed AES for encryption. The second part is the proposed AES, which represents the encryption algorithm that encrypts data selected by the user from the first part, and transformation of the output encryption file to the first part again to store. Finally, the third part is a key generation. This part is divided into three sub-parts, which are "initial key" that is chosen by user is used to generate another key, "key algorithm" that uses initial key for generation of key, finally "key" which is random byte used with proposed AES to encrypt data (Ahmed & Faisal, 2015).

5. Modified AES

In Ahmed & Faisal (2015), a modified AES to increase the robustness and speed of encryption and decryption data was presented. For that, take several changes in AES used longer key encryption and longer data matrix encryption to increase the speed encryption process with algorithm complexity. Discusses this modification briefly in this section.

5.1 Extended input size

To increase the robustness of the AES, extended the data matrix and key matrix. The data matrix is extended to 8x8 matrix instead of a 4x4 matrix and the key matrix is extended to the same size. This extended is also increase the speed of encryption process.

5.2 Key to key mapping

In this stage modified Add round key stage by using part of the key to determent the sequence key matrix well used in XOR operation. The parts of key matrix most to be 11 matrixes. Each matrix contains values less than 12 because the number of key matrixes is 11 matrixes.

5.3 Key based shift row

In this stage modified the shift row, after extended data matrix from 4x4 to 8x8 matrix, shifted 8 rows instead of 4 rows. Also, the number of shift depended on parts of keys. The parts keys array is 80 bytes and must be a value less than 8 because the number of columns is 8 and number of shift equal 8 bytes only.

5.4 Separated mix column

Mix column in AES classical algorithm is multiple the data matrix 4x4 with static matrix 4x4. In AES modified have four different static matrixes, each one of them is multiple with parts of extended data matrix 4x4.

5.5 Cascaded key extended

Key extended from 128 bits to 512 bits because of an extended data matrix from 16 bytes to 64 bytes. The extended process by repeated four times same algorithm for generation key, with used different initial for every time. The initial that used result XOR operation between last previous key matrix and any key matrix.

6. Security of Modified AES

The effort is required for cryptanalysis of ciphertext of an algorithm. It focuses on the evaluation of the practicality of the attack (Stallings, 2011). The classic AES uses minimum key of 128-bits, that means the brute force attack requires (2^{128}) possible i.e. (17179869184) possible number to decrypt the key used in the algorithm, and possible number to decrypt the ciphertext with key size of 128-bits is $(2^{128})^{11}$, the result is 3.66959779e+106 where the number 11 is number of using "Add Round key" stage (Yacob, 2012). This attack is considered impractical because it takes a lot of time and needs special equipment.

AES modification takes 512-bits of the key, this makes to the brute force attack very "difficult" or "impossible" because of the possibly large number for decrypt key. Also, part of the key is used with other stages in AES modification (shift is based on the key and the key to key mapping), thus increment the "randomness" in output ciphertext. Increase in possible number for key and increment the randomness for ciphertext gives more "complexity" for AES modification.

7. Experimental Results

To test the performance modified AES algorithm. The performance of the modified AES algorithm is done by taking three different size text files for comparing the speed encryption process between AES algorithm and modified AES. Table1 show compares between both.

Note: the result is different according to the mobile device.

Table 1: Compare between classic AES and modified AES

File size	***Classic AES***	***Modified AES***
1k	00:00:00:233	00:00:00:84
3k	00:00:00:607	00:00:00:156
5k	00:00:00:887	00:00:00:204

8. Conclusions

Development of proposed security application on Android mobile, this leads to the proposed system provides high security and confidentiality on data mobile in (internal and external storage) from unauthorized access and when mobile or SD card is lost or stolen. The application depends on modifications AES algorithm in encryption and decryption.

The modification AES algorithm has more robustness, more security, more complexity and increased the speed encryption process. The modification focuses on converting the sequential steps in AES classic algorithm to random steps inside modified AES algorithm by depending on some parts of keys.

REFERENCES

1. Ahmed T. Sadiq, Faisal H. Faisal (2015), "Modification AES algorithm based on Extended Key and Plain Text", accepted, Journal of Advanced Computer Science and Technology Research, vol. 5, Issue 4.
2. Al-Hasan M., Rahman M. O., and Uddin A. M. (2013), "User-Authentication Approach for Data Security between Smartphone and Cloud", *International Forum on Strategic Technology* (*IFOST) vol. 2*.
3. Mandavkar P., Patil G., Shetty C., and Parkar V. (2014), "SMS Security for Android Mobile Using Combine Cryptographic Algorithms", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4.
4. Martinez Hugo J. (2012), "Mobile Device Security: Current Challenges and Existing Solutions", MSc thesis computer science, Western Michigan University, spring.
5. Naik M., Sindkar A., Benali P., Moralwar C. (2014), "Secure and Reliable Data Transfer on Android Mobiles Using AES and ECC Algorithm", International Journal of Innovative Technology & Adaptive Management (IJITAM) vol.1, Issue 11.
6. Scripcariu L., and Frunza D. Mircea (2012), "Modified Advanced Encryption Standard", 11th International Conference on Development and Application Systems Vol. 2, Issue 3.
7. Skillen A. (2013), "Deniable Storage Encryption for Mobile Devices", MSc thesis Engineering and Computer Science, Concordia University Montreal, Canada.
8. Stallings W. (2011), "Cryptography and Network Security Principles and Practice, 5th Edition".
9. Yacob Z. B. (2012), "An Improved Algorithm for Partial Cryptography of Digital Video", PhD thesis