Global Scientific JOURNALS

GSJ: Volume 9, Issue 5, May 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

SECURE TRANSMISSION SYSTEM

Dakshta Sengar
Department of computer science and engineering
Galgotias University
Greater Noida, India
dakshtasengar@gmail.com

Prashant Kumar Mayank
Department of computer science and engineering
Galgotias University
Greater Noida, India
mayankprashant67@gmail.com

Nilesh Kumar Yadav
Department of computer science and engineering
Galgotias University
Greater Noida, India
nilesh9307398100@gmail.com

Abstract— In this research paper we have done research on "SECURE TRANSMISSION SYSTEM" using face recognition. An Application that we have designed utilizes encryption and decryption techniques and facial recognition using Machine Learning, this implies that if someone wants to see the message in the transmission then he will not be able to do the same as the message is encrypted, firstly he/she will need to recognize his face and if he don't have secret key than he will get nothing but some random bytes. In this research paper we found an optimal method for encryption and decryption between sender and receiver and did a 2 layer protection using face recognition using Advanced Encryption Standard (AES) algorithm in Android studio as the environment. Furthermore we compared the different proposed methods of encryption with existing ones in the market and chose Advanced Encryption Standard (AES) to move forward with. We used the ML tool kit of Google firebase to give the functionality of face recognition.

I. INTRODUCTION

On the Android open-source platform, there are certain malwares that can break down a message that is being transmitted over the public network. We have also learned that there are many malwares that can intercept a message being transmitted like using brute force attack. This means that the message itself is not safe enough, therefore it is necessary to protect the data from data breaches. For this reason, this research paper is a necessity. The output of this research paper is to learn a method to secure the messaging system. Also, we gained some experience on Java cryptography programming and Facial Recognition using Machine Learning Modules of Google firebase .Due to the advancements in the Internet technology, huge digital data are transmitted over the public network. Since the public network is open to everyone, this data preservation is a critical issue. Therefore, numerous encryption and decryption algorithms have been used to secure such data from unauthorized persons. The AES (Advanced Encryption Standard) algorithm is highly insulated from these algorithms.

II. COMPARATIVE ANALYSIS

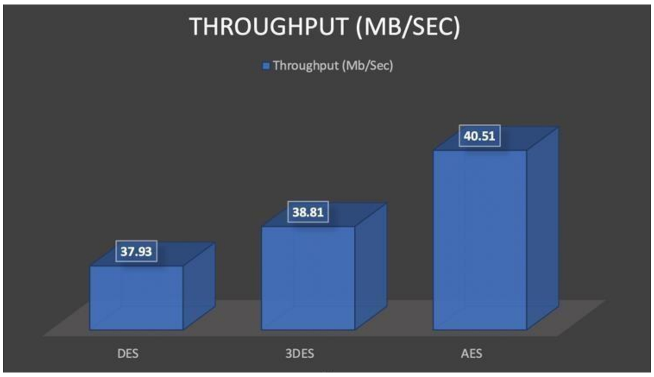
There are some most useful algorithms such as firstly Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DEA), and Advanced Encryption Standard (AES). DES, 3DES and AES were tested for their capability to secure data and the time it took to encrypt the data (throughput).

The output expected by these different algorithms as the size of the inputs increases or decreases is shown.

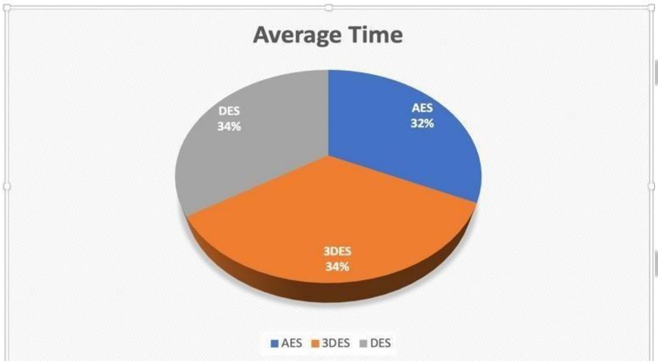
Properties	DES	3DES	AES
Key Length	56 bits	168 or 112 bits	128,192 or 256 bits
Block Size	64 bits	64 bits	128,192 or 256 bits
Keys	2^(56)	2^(168) or 2^(112)	2^(128),2^(192) or 2^(256)
Time required to check	400 days	800 days	5x10^(21) years

This Table shows the comparison between DES, 2DES and AES algorithms at different factors such as the keys, key size, block size, key rounds according to key size respectively, and power consumption (time required to check different key rounds).

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE



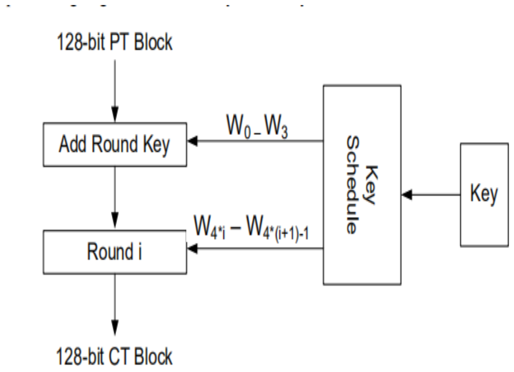
This shows the Throughput (Megabyte/Sec) of these cryptographic algorithms (DES, 3DES, and AES) in the experiment. This shows that the AES algorithm has the highest throughput for all sizes of keys available in the particular algorithm.



This Figure shows the Average Time for the Encryption.

It is obvious from the displayed graphs that the algorithm requires far more time to locate a key in the case of the AES brute force attack algorithm. It has strongerprotection than DES and Triple DES.

In terms of time consumption and throughput, AES has an advantage over other 3DES and DES. Results from the comparative analysis done on these algorithms demonstrated the potential of each algorithm and thus it is concluded from this that AES is the best performing algorithm than other common cryptographic algorithms used.



III. IMPLEMENTATION

These cryptographic algorithms are based on firstly mathematical theory and secondly on computer science practice also. However, by attempting all key combinations or executing what is called a brute force attack, one can still assume that each modern encryption algorithms technically breakable.

On the other hand, the amount of time needed by these encryption algorithms is quite high so the current computational powers are not able to break these algorithms. Moreover, due to continuous improvement in science and computational power also these encryption algorithms need to be improved in terms of breakability.

There are two types of modern cryptography algorithms, firstly the symmetric encryption algorithms, and second asymmetric encryption algorithms. Symmetric algorithms have the same key for encryption and decryption of the text and the asymmetric algorithms use each pair of key communication, the public and the private key. The public key is given to everyone who wants to access the document, I.e. public, and is used for encryption whereas the second key I.e. the private key is owned by the owner and is used for decryption of the text at receiver's end. Certification authorities and digital certificates are also used at the receivers end to improve the security of data.

Symmetric algorithms:

Symmetric algorithms as the name suggests use the same key for encryption and decryption of the text as presented in Fig.2. The major disadvantage of these algorithms is that the key has to be shared among the communicated parties over the network which also should be done in a secretive manner. As there are several parties in a conversation over the network, Each of them should have a secret key, as a result, there are keys for "n" user party and n*(n-1)/2 keys, so this is known to be an "n" user group.

These algorithms have another drawback. In Spite of the several disadvantages of symmetric encryption there are several advantages also over the asymmetric encryption. As the symmetric algorithms use small inputs they are quite faster than asymmetric algorithms.

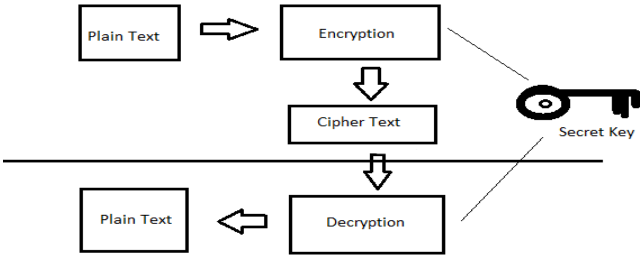


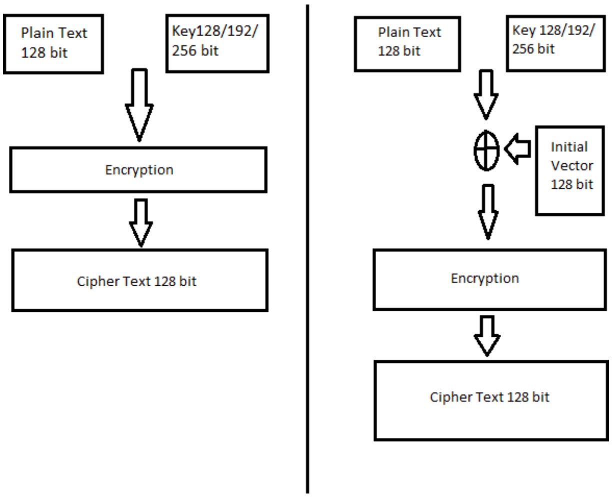
Fig. 2 - Symmetric encryption diagram.

AES's encryption feature performs 128-bit input mathematical operations. In several rounds that differ from the key length, these operations are repeated. Therefore, there are 10 rounds for the 128 bit key, 12 rounds for the 192 bit key size and 14 rounds for the 256 bit key size. Each round has 4 steps. These steps include byte substitution also called substitution box, permutation, arithmetic operations and then XOR with a key.

AES parameters:

AES algorithm is all about encryption mode whether it is Electronic Codebook (ECB) or Cipher-Block Chaining (CBC) only two or three parameters given. When the mode is ECB two parameters are given, firstly a 128 bit plain text and second a 128, 192 or 256 bit key. In comparison, as discussed in Fig. 3, if CBC encryption mode needs another extra parameter, it is an initial 128 bit vector. It always produces a 128 bit result.

Figure 3: AES encryption in ECB and CBC mode.



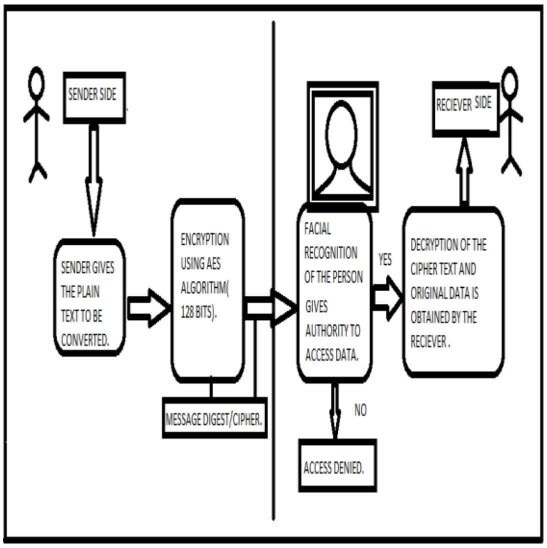
Security

AES is considered to be the most secure symmetric algorithm. There are only a few attacks that can break it and they are applicable only on special conditions. To break it with brute-force attack it is almost impossible because there are too many combinations and it will take billions of years. But with the original one each of these attacks requires a lot of time and therefore it is not useful. To sum up, the NSA finds AES to be sufficiently reliable to protect even top secret information. This data explains the best level of protection. Furthermore, we have carried out attacks of brute force against cipher texts.

ML Kit for Firebase:

ML Kit is a mobile SDK that puts the machine learning knowledge of Google into a strong but easy-to-use kit for Android and iOS apps. You can incorporate the features you need in just a few lines of code, whether you're new or experienced in machine learning. To start a new project, one doesn't need to have in-depth knowledge of neural networks. On the other side, if you are an experienced Machine Learning developer, ML Kit offers convenient APIs in your mobile apps that help you use your custom Tensor Flow Lite models. Before you apply face detection to an image, if you want to change any of the face detector's default settings, specify those settings with a Firebase Vision Face Detector Options object.

IV. PROPOSED SYSTEM


SENDER SIDE
SENDER GIVES THE PLAIN TEXT TO BE CONVERTED.
ENCRYPTION USING AES ALGORITHM(128 BITS).
MESSAGE DIGEST/CIPHER.
FACIAL RECOGNITION OF THE PERSON GIVES AUTHORITY TO ACCESS DATA.
YES
NO
ACCESS DENIED.
DECRYPTION OF THE CIPHER TEXT AND ORIGINAL DATA IS OBTAINED BY THE RECIEVER .
RECIEVER SIDE

There are two sides of this application. The one is the sender side and the other is the receiver side. We have made a research paper for a secure message system which has two layers of security, firstly is encryption with AES, secondly face recognition of the person receiving the message.

So the first step of processing of the message from the sender includes the encryption of the plain text with the help of AES. Then the message digest or cipher from the previous step is given to the receiver side.

Here at this step, the second stage of security is done i.e. face recognition which is done using ML kit for firebase. Once this stage is completed, then only further the decryption of the message is done. For the decryption the ciphertext given by the sender is now converted back to plain text and the receiver finally gets the message after two stages of security.

V. PROBLEM FORMULATION

There are three times more documented bugs in Android than in iOS. To ensure data protection in your application, the addition of cryptographic algorithms and facial recognition is therefore vital. Some algorithms are quick and simple to implement, such as symmetric encryption and hashing, but they provide you with limited security. Others take a lot of time to process data but guarantee its reliability, such as digital signature and asymmetric encryption.

ACKNOWLEDGMENT

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them. We would like to express our special thanks and gratitude to our guide Tarun Kumar Sharma, Assistant Professor who gave us the golden opportunity to do this wonderful project on the topic (Secure Transmission System), which also helped us in doing a lot of research and we came to know about so many new things for that we are really thankful to them. Secondly, we would also like to thank our parents and friends who helped us a lot in finalizing this project within the limited time frame. The generosity and expertise of one and all have improved this study in innumerable ways and saved us from many errors; those that inevitably remain are entirely our own responsibility.

REFERENCES

1. Abdalbasit Mohammed ,Nurhayat Varol " A Review Paper on cryptography", ISDFS, June 2019.

2. Sivakumar, R., Balakumar, B.A Study of Encryption Algorithms for Information Security.International Research Journal of Engineering and Technology

3. Matsui, M. Linear Cryptanalysis Method for DES Cipher

4. https://www.tutorialspoint.com/cryptography

5. https://firebase.google.com/

6. https://www.sciencedirect.com/topics/computer-science/cryptographic-technique