INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 05 ISSUE: 12 | DEC - 2021 ISSN: 2582-3930

Android Chat Message App With End To End AES(Advanced Encryption Standard) Method Using Firebase Database.

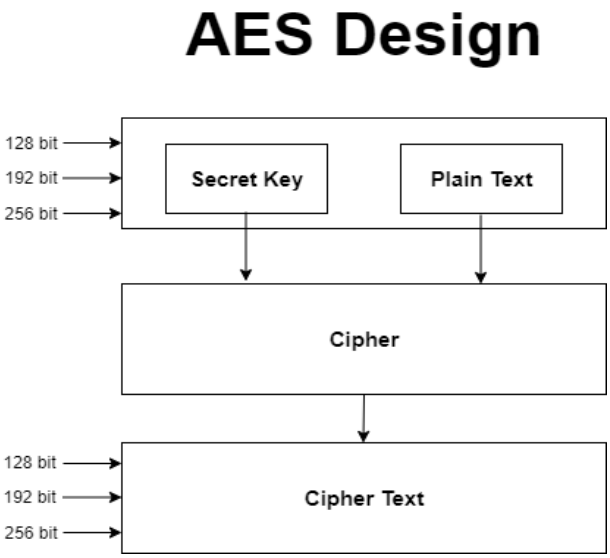
Mr.Atishay Jain | Ms.Vasudha Bahl | Ms.Amita Goel | Ms.Nidhi Senger
IT Department, Maharaja Agrasen Institute Of Technology

***Abstract*— This Paper presents the design and implementation of an android application for the provision of secure real time communication services between users, based on the AES cryptographic algorithm. The application has been designed based on the requirements of the users so as to allow users to communicate and read the transmitted messages. As the number of users are increased, Along with these users, there is also increase in number of unauthorized users which are trying to access a data by unfair means. This arises the problem of data security. Messages sent over an insecure transmission channel from different sources, some messages contain secret data, some messages itself are highly confidential, hence securing them from any attack is essentially required. To solve this problem, we are using AES algorithm for encrypting and decrypting messages in a messaging app.**

INTRODUCTION

A. One of the most important factors that determine the efficiency and effectiveness of an application in a modern world is its ability to safely store, retrieve information between verified users. The purpose of this work is to design and develop an android application that provides secure real time communication based on symmetric cryptographic algorithms. The ultimate aim of the application is to provide the infrastructure that will allow authenticated users to read messages that they exchange in pairs.

The Advanced Encryption Standard (AES) is symmetric block cipher. AES is implemented in software and hardware around the world to encrypt all the data. It is essential for government computer security, cybersecurity and electronic data protection. Each cipher encrypts and decrypts data in blocks of 128 bit using cryptographic key of 128, 192 and 256 bit, respectively. Symmetric, also known as secret key, cipher uses the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.



The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array, after which the cipher transformations are repeated over multiple encryption rounds.

II. BACKGROUND

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a variant of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. The government classifies information in three categories: Confidential, Secret and Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths.

A. Security

Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.

B. Cost

Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

C. Implementation

Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

A 256-bit encryption key is significantly more difficult for brute-force attacks to guess than a 128-bit key; however, because the latter takes so long to guess, even with a huge amount of computing power, it is unlikely to be an issue for the foreseeable future, as a malicious actor would need to use quantum computing to generate the necessary brute force.

Still, 256-bit keys also require more processing power and can take longer to execute. When power is an issue -- particularly on small devices -- or where latency is likely to be a concern, 128-bit keys are likely to be a better option.

When hackers want to access a system, they will aim for the weakest point. This is typically not the encryption of a system, regardless of whether it's a 128-bit key or a 256-bit key. Users should make sure the software under consideration does what they want it to do, that it protects user data in the way it's expected to and that the overall process has no weak points.

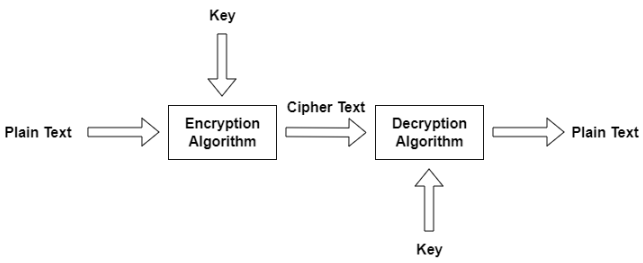
Additionally, there should be no gray areas or uncertainty about data storage and handling. For example, if data resides in the cloud, users should know the location of the cloud. Most importantly, the security software that has been selected should be easy to use to ensure that users do not need to perform unsecure workarounds to do their jobs.

III. OPERATION OF THE SYMMETRIC ENCRYPTED ANDROID CHAT APP

The basic operation principle for a chat app of symmetric cryptographic communication is the use of a shared secret key that is used for both encryption and decryption. The secret key is the most important component of the encryption system, as it is the principle means that transforms clear messages to ciphertexts. The disclosure of the key to malicious users jeopardises the essence of communication.

For a group of users of a symmetric cryptography system, the method of a shared secret key is widely used. The application uses the secret key of its owner for sending data to the network and use the same secret key for decrypting messages.

The operation of the encrypted communication is illustrated in Figure 1 below.



The plain text denotes the text that has been send to the other users on the chat app. The plain text is easy to see and can be read by anyone. The plain text is then converted to Cipher Text using AES Cryptographic Algorithm. And all the cipher text then will be stored on the Firebase database. As all the Text is already converted to cipher text so no one will be able to read it as it will be in gibberish.

Then the cipher text will be sent to the other end of the app from firebase and then will be decrypted using Same secret key and then it can be read by anyone on the other end.

The classical symmetrical cryptographic systems use a common secret key for both the two communication periods. These cryptographic systems are used for the secure communication between two users only and in case of the key break from intruders the communication is open in both the two periods.

Thus each hacker should make computational effort in order to break the personal secret keys or more keys consequently the total of communication. In order for each user that belongs in the certified group to communicate with the users that he wishes, he should know their personnel secret keys of encryption.

IV. ARCHITECTURE OF THE APPLICATION

In a previous paragraph the overall operation of the application was described. This operation is supported using various subsystems that from an implementation point of view can be seen as commands that when properly combined lead to the desired result. The encryption and decryption subsystems can be singled out as two such fundamental subsystems. As autonomous entities, these subsystems have as input the message and as output, a deciphered result. The process of calculating the result directly implements the mathematical model of the AES cryptographic algorithm.

After having implemented the encryption functionality and achieved the level of security necessary, the application must be integrated with the Firebase database to store the messages on a safe and secure environment.

V. RESULT

A chat application that encrypts and decrypts the text messages using firebase as a database will be made. This will help in minimising the problem of data theft and leaks of other sensitive information. The text stored on the database after encryption is secure and no one can steal data from this text. So, these text messages can be stored on a database without any problem.

The design of this application is based on state of the art encryption technologies, namely AES, and exploits this technology within an environment that promotes and facilitates the use of safe practices on the behalf of users.

References

[1] NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, Annabelle Lee, Security Technology Group -Computer Security Division -National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

[2] R. ANDERSON AND R. NEEDHAM, “Robustness principles for public key protocols”, Advances in Cryptology–CRYPTO ’95 (LNCS 963), 236–247, 1995.

[3] D.W. DAVIES AND W.L. PRICE, Security for Computer Networks, JohnWiley&Sons,New York, 2nd edition, 1989.