A Secure Chat Application

Atishay Jain | Vasudha Bahl | Amita Goel | 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. 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. This arises the problem of data security. It is difficult for the security personnel to send classified information to the sub ordinates without the data breach. 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. And the messaging app can only be opened by the Biometrics of the authorized user. Moreover, to make it more secure we have also added an extra layer of passcode security. The user has to enter an automatically generated OTP passcode every time when user tries to send any messages on the application. This will ensure that no fake messages will be sent by any other person on the application.**

I. INTRODUCTION

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 and security personnel to send classified information to the sub ordinates without the data breach.

Biometric Authentication is a technology adapted by many mobile manufactures for mobile security. Biometric authentication means authenticating a person based on their biological characteristics such as Biometric, face, iris, voice, and retina. Biometric Biometric recognition is used in majority of the smart phones. This feature frees users from having to remember additional app-specific passwords, and avoids the need for you to implement your own authentication user interface. Biometric recognition may seem to be a bit more secure because a Biometric is extremely unique and difficult to mimic.

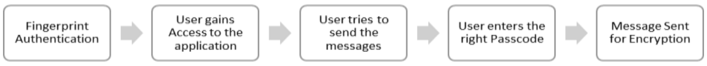

Fingerprint Authentication
User gains Access to the application
User tries to send the messages
User enters the right Passcode
Message Sent for Encryption

Fig. 1 displays the process how the user passes through all the security measures to get into the application

Biometric Manager will be used to store the Biometric data. This is a class that we will be using throughout the Biometric authentication process. Create a Biometric helper class. This class will be responsible for triggering the authentication method and processing the various call back events that can occur depending on whether the authentication has succeeded, failed, or an error has occurred.

The key biometric authentication component is the BiometricPrompt class. This class performs much of the work that previously had to be performed by writing code in earlier Android versions, including displaying a standard dialog to guide the user through the authentication process, performing the authentication and reporting the results to the app.

The advantage of Biometric is the uniqueness, high performance. All the people in the world have their own unique Biometric, two persons cannot have same Biometric not even the twins.

A One Time Password (OTP) is a unique code/token generated by our application, sent to a user via SMS text and then entered into our application flow for additional security. One-Time Passwords are only effective for a fixed period of time and become invalid once the user enters it, making them exceptionally useful against spyware such as key logging programs.

One we have added built One Time Passwords into your application flow a One Time Password will be texted everytime depending on the time frequency that you have set. This flow will dramatically improve account security.

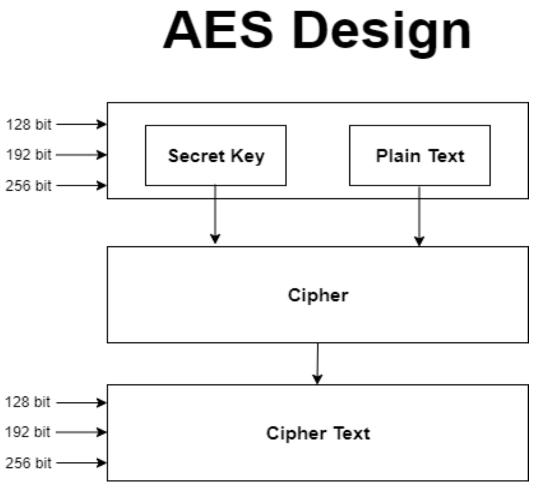


Fig .2 displays how the AES Encryption Algorithm works and how it converts simple text into Cipher Text

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 method of Biometric recognition has been used as a method of identifying since the nineteenth century. According to The Public Domain Review (2011), the projections and dermal folds were described for the first time in the eighteenth century, by the English botanist Nehemiah Grew.

Nowadays, because of the technological progress, have appeared applications abled not only to store a large amount of data, but also to compare the Biometrics. Biometrics have become one of the most popular features used by physiological biometric technology. This popularity is due to both historical considerations and the fact that currently, they can achieve very high performance in the checking of identity.

The Biometric identification points called minutiae refer to discontinuities that may appear in papillary ridges. There are two types of information: termination (ending abruptly ridges) or fork (which branches into two peaks).

The pre-processing of the Biometrics consists of:

Acquisition- The Biometrics images are taken with aresolution between 250 and 625 dpi (dots per inch). Most systems use a resolution of 500 dpi and the stored images are often represented using 8 bpp (bits per pixel) in 256 levels of gray.

Pre-processing- Higher image quality by emphasizing differences in intensity between ridge lines and intergrowths.

Detection of minutiae- The automatic Biometric identification systems use only two types of characteristic known as basic details or minutiae: ridge ending and bifurcation.

Biometric Matching Techniques

The large number of approaches to Biometric matching can be coarsely classified into three families.

Correlation-based matching: Two Biometric images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

Minutiae-based matching: This is the most popular and widely used technique, being the basis of the Biometric comparison made by Biometric examiners. Minutiae are extracted from the two Biometrics and stored as sets of points in the two-dimensional plane. Minutiae based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings

Pattern-based (or image-based) matching: Pattern based algorithms compare the basic Biometric patterns (arch, whorl, and loop) between a previously stored template and a candidate Biometric. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the Biometric image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned Biometric image. The candidate Biometric image is graphically compared with the template to determine the degree to which they match. In Our project we have implemented a minutiae based matching technique. This approach has been intensively studied, also is the backbone of the current available Biometric recognition products.

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 SECURE CHAT APPLICATION

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.

The application will only get unlocked using the owner's Biometric only else it will not open and no one can use it. And even at the receiver's end the user has to unlock the application using the Biometrics else the user will not be able to open the application and read the messages.

Even after unlocking the application after the biometric authentication the user has to enter a Pre-received OTP on their mobile number to get into the application. Once the user passes all of this security features and then tries to send the message, the user again has to enter the OTP to send the message on the application. The OTP will be valid only for a specific amount of time.

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.

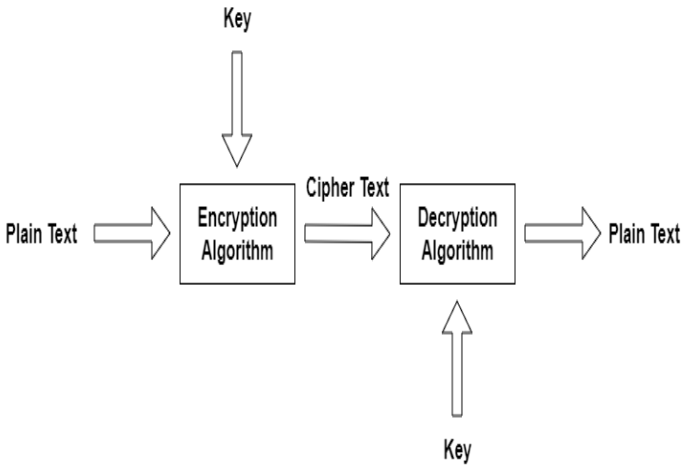


Fig. 3 displays how the message is sent over the system and how the encryption and decryption algorithm works

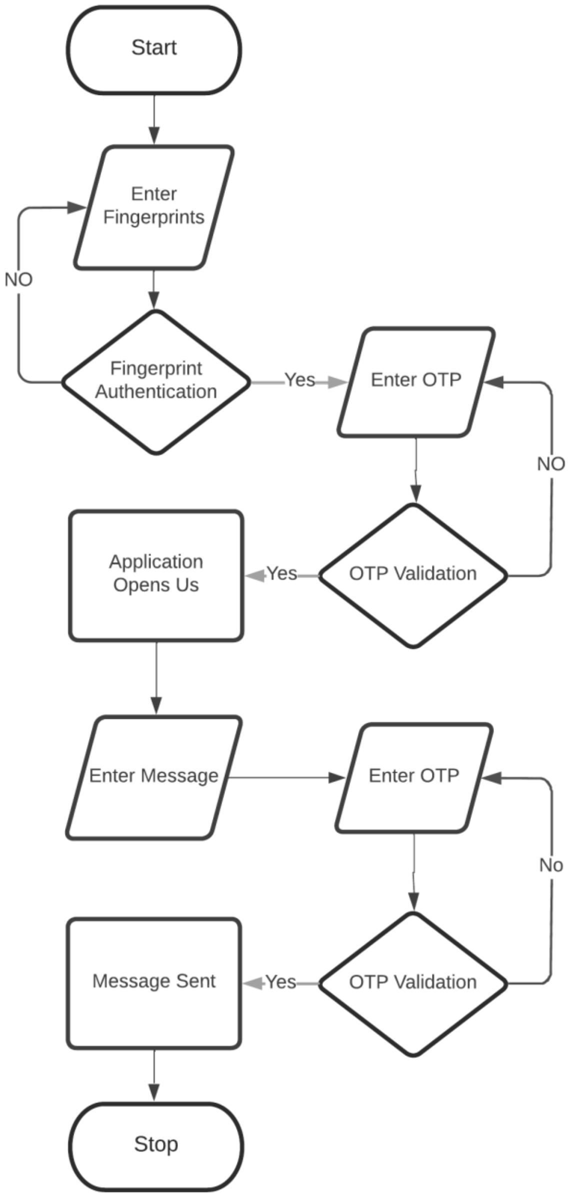


Fig. 4 displays the whole process of the application and its working

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

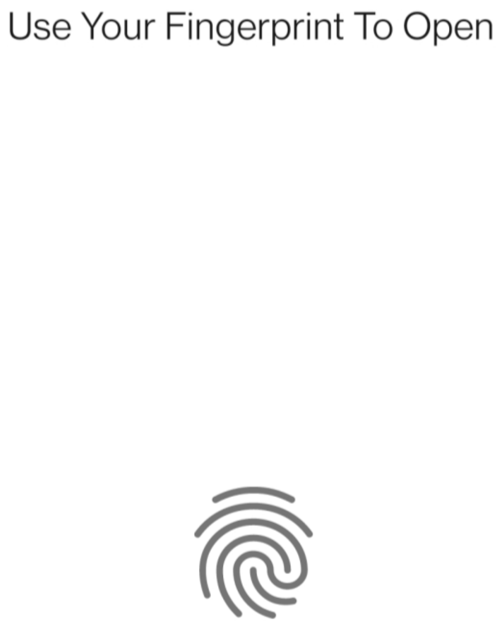
In a previous paragraph the overall operation of the application was described. This operation is supported using various subsystems that from an implementation point of view can be seen as commands that when properly combined lead to the desired result. The Biometric Authentication will help us in securing the application by only allowing the user to open the application. The OTP passcode security can be considered an extra layer incase if any bad entity passes through the fingerprint authentication, then the hacker has to bypass another level of security which will be very difficult. 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.

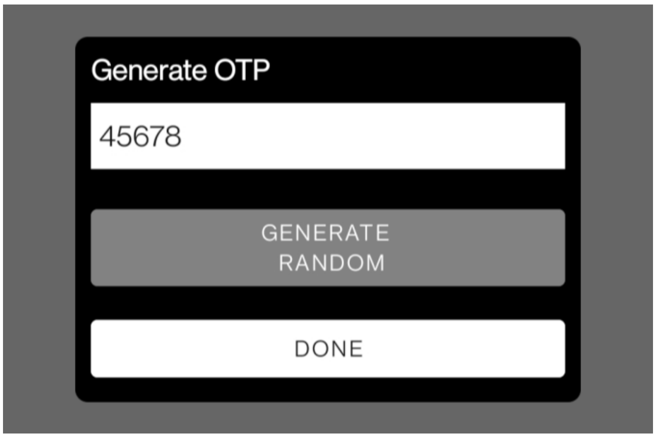
The chat application has an extra layer of biometric and passcode security without which the user will not able to access the application. This will help in minimising the problem of data theft and leaks of other sensitive information. The text stored on the database after encryption is secure and no one can steal data from this text. So, these text messages can be stored on a database without any problem.



Use Your Fingerprint To Open

Fig. 5 displays the application asking for biometric authentication for the access

The biometric authentication will ensure that no other than the rightful user will be able to open and use the application.

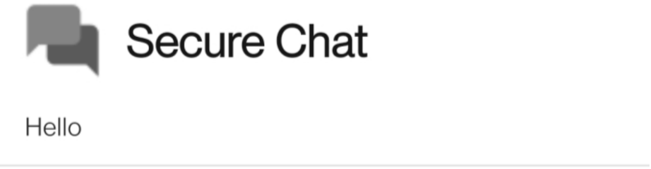


Generate OTP

45678

Fig. 6 displays the application asking for OTP to send the message on the application.

The Passcode security will add an extra layer of security. The user has to enter the OTP to enter into the application after he successfully passes through the biometric authentication. The user also has to enter that OTP passcode to send any message over the application. On the receiver end, the user also has to go through biometric authentication to read the messages on the application.



Secure Chat

Hello

Fig. 7 displays the message successfully sent over the application.

VI. CONCLUSION

The result above clearly states that the application is much more secure than the previous version. And it is reliable and 80% more efficient and secure than the the previous version in all the aspects. 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.

[4] Kataria, Adhyaru, Sharma, Zaveri, ―A survey of automated biometric authentication techniques‖ In Proceedings of the IEEE Nirma University International Conference on Engineering (NUiCONE), pp. 1-6, 2013.

[5] Charles Severance. ―Anil Jain: 25 Years of Biometric Recognition‖ IEEE Journal Computer, pp. 8-10, 2015.

[6] Weizhi Meng, Wong, Furnell, Jianying, ―Surveying the Development of Biometric User Authentication on Mobile Phones‖ Communications Surveys & Tutorials, IEEE, pp. 1268- 1293, 2014.

[7] G. Kwang, R. H. C. Yap, T. Sim, and R. Ramnath, “An usability study of continuous biometrics authentication,” in Proc. ICB, 2009.

[8] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, “It’s a hard lock life: A field study of smartphone (un)locking behavior and risk perception,” in Proc. SOUPS, 2014.

[9] A. Jain, “ Android Chat Message App With End-To-End AES(Advanced Encryption Standard) Method Using Firebase Database.” in IJSREM, 2021