END TO END MESSAGE ENCRYPTION USING BIOMETRICS

Dr S. Brindha[1], Ms B. Nivedetha[2], Mr V. Dhivyadhanush[3], Mr S. Karthi[4], Mr M. Mukeshwaran[4]

[1]Head of Department, Department of Computer Networking, PSG Polytechnic College, Coimbatore, India
[2]Lecturer, Department of Computer Networking, PSG Polytechnic College, Coimbatore, India
[345]Student, Department of Computer Networking, PSG Polytechnic College, Coimbatore, India

---***---

Abstract - The messenger is used to send messages or to convey the message in different format .This messenger is similar to the existing messengers except the message is encrypted using face biometrics during the message exchange. The send message is encrypted and the received message is decrypted using the 128 bit key. In this proposed method, we have used face biometrics to unlock the encrypted messages, photos, voice message and also video messages Android application has been created using Android Studio, End to end message encryption between firebase server to client, Media sharing has been introduced to the mobile application.

Key Words: Face biometrics, end to end Message encryption

1. INTRODUCTION

Biometric Systems are automated methods of verifying or recognizing the identity of the living person on the basis of some physical characteristics, like a fingerprint or face pattern, or some of the behavior, like hand writing or key stroke patterns.

Some of the most used biometric characteristics are shown in the figure 1. A biometric system based on physical characteristics than one which even if the latter may be easier to integrate within certain specific applications.

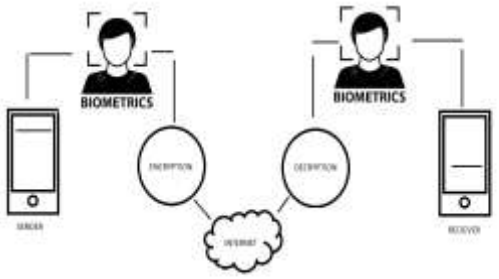


Fig 1 Block diagram

2. PROPOSED SYSTEM

The messenger is used to send message with the normal security system. The message like text, video, voice etc.., is encrypted with end to end encryption using AES encryption method for security to avoid the third party entry. The encryption used for the messenger with 128 bits of 10 rounds of encryption. The encryption already breakers is 32bit and 64bit. The messengers like this are much secured when third party uses the phone.

Biometrics are measures of biological quantities or pattern but also means measurements of an individual's features, such as fingerprints, that can identity or authenticate a person.

3. LITERATURE SURVEY

Automated person identification is highly researched in recent years because of its applications, like protected access to computer systems, buildings, cellular phones, ATMs and video surveillance. Person identification is the process of associating an identity to the individual. Person identification techniques are there classified into three, namely knowledge based, token based, and biometric based. A knowledge-based approach depends on something an individual knows to make a personal identification, like a password or a personal identification number (PIN).

Token-based approaches are based on something an individual have to make a personal identification like a passport, driver's license, ID card, credit card, or keys. These two approaches have several demerits: tokens may be stolen, lost, forgotten or misplaced. The password or PIN code can be forgotten by an authenticated person or predicted by an attacker.

4. MESSENGER APPLICATION

The application is build using the software android studio. It is the best android application development platform. The following paragraph describes about the application.

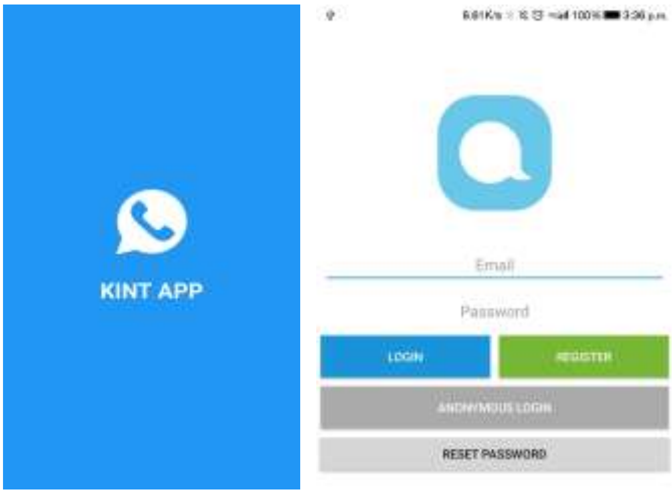
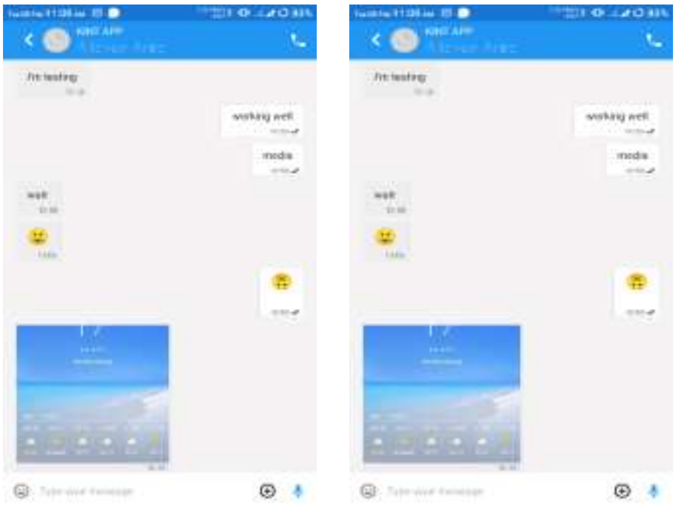


Fig 2 KINT App

Application is built using any android version above 5.0. The android application is named as KINT the application name is referred to “Keep IN Touch”. The Application logo and the login page are shown in figure 2 .The application supports the media transformation such as picture, video, audio and voice. It supports the voice call and video call. The message history and database is also stored like firebase databases. The message is shown in figure 3.



I'm testing

working well

media

wait

Fig 3 Messenger Application

The message is encrypted and decrypted using the AES (Advanced Encryption Standard) algorithm of 128 bit key size. The encryption is done with the key generated from the real-time face biometrics. This key is compared with the face biometrics saved in the database, if they are same then the message is encrypted. During the message transmission, the message is encrypted and authenticated using face biometrics.

The decryption of message is done only when the face is matched with the image in the database. The authentication fails if the captured face does not match with the database image. When the face biometric is not matched, the messages in the messenger are in encrypted form which are unreadable by humans so it remains more secured and safety.

5. DATABASE

The database of the application is designed by the firebase database. It is the familiar database for the real time storage and Encryption as shown in Figure 4

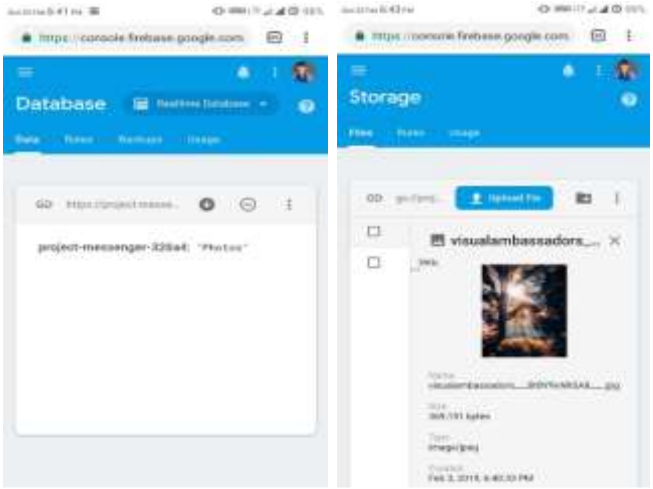

https://console.firebase.google.com
Database
Realtime Database
Storage
Upload file
project-messenger-32ba4: "Photos"
visualambassadors_...

Fig 4 Real Time Storing

Firebase's first product was the Firebase Real-time Database, an API that synchronizes application data across iOS, Android, and Web devices, and stores it on Firebase’s cloud. The product assists software developers in building real-time, collaborative applications as shown in figure 5.

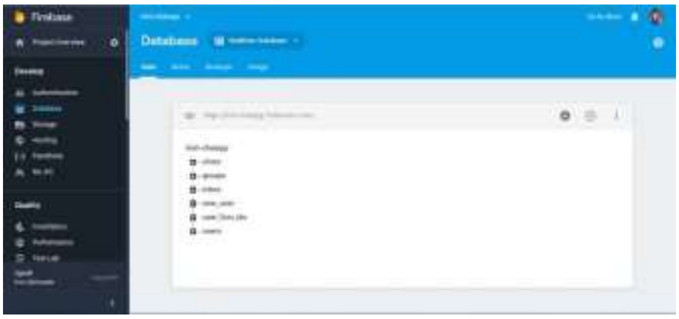
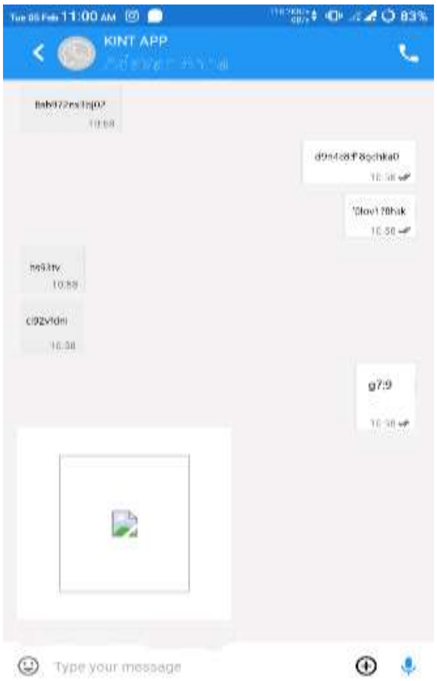


Fig 5 Database

4. AUTHENTICATION

The authentication for this messenger is based on the login page the authenticated phone number and the following OTP are used to login and for the account verification. The encrypted message will be displayed in human unreadable form as shown in the figure 6.



8ab872rs1qj0?
10:58

d9n4c8f8qchka0
10:58

'0lov178hik
10:58

hi93tv
10:58

ci92vldni
10:58

g7:9
10:58

Fig 6 Encrpted Message

6. CONCLUSION

Biometric Systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physical characteristics, like a fingerprint or face pattern, or some aspects of behavior, like hand writing or key stroke patterns. Some of the most used biometric characteristics are shown in the figure. A biometric system based on physical characteristics. Than one which even if the latter may be easier to integrate within certain specific applications.

ACKNOWLEDGEMENT

I express my sincere thanks to **Dr. B. Giriraj**, Principal, PSG Polytechnic College, Coimbatore, for providing me an opportunity to take up this Mini Project Report.

I also express our sincere thanks to Mr. **Jeevanantham**, **Jasper KeyPlay** for the support and the guidance to take up this project.

I also express our sincere thanks to our **Faculty** and **Friends** for their kind support and encouragement during the project.

BIOGRAPHIES

Dr.S.Brindha
Head of Department
Department of Computer Networking, PSG Polytechnic College Coimbatore, India.

Ms.B.Nivedetha,ME
Lecturer
Department of Computer Networking PSG Polytechnic College Coimbatore, India.

Mr.V.Dhivyadhanush,
Student
Department of Computer Networking PSG Polytechnic College Coimbatore, India.

Mr.S.Karthi,
Student
Department of Computer Networking PSG Polytechnic College Coimbatore, India.

Mr.M.Mukeshwaran,
Student
Department of Computer Networking PSG Polytechnic College Coimbatore, India.