www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

CHATTING TEXT ENCRYPTION USING AES ALGORITHM ON NDROID

Jayaprakash. S[1]

[1]M. Sc Computer Science, Sri Krishna Arts And Science College, Coimbatore

ABSTRACT

When sensitive data is transferred across a network, encryption is crucial. For the same, a number of encryption techniques, including AES, DES, RC4, and others, are available. AES is the algorithm that is most commonly used. On the Android platform, we have created an application that enables the user to encrypt messages before they are sent over the network. To encrypt and decrypt the data, we employed the Advanced Encryption Standards algorithm. Any Android-powered device is capable of running this application. This programme offers data encryption that is quick, secure, and robust. It is extremely challenging for an attacker to decipher the encryption pattern because of the massive amount of confusion and data diffusion that occurs during encryption. the encrypted data in plain text form. The application that was built can encrypt messages while protecting them from brute-force and pattern attacks. In this paper, the functionality of the application and its numerous real-world applications are discussed.

General Terms-Security Algorithm, Symmetric Key Encryption, Android Application, Chatting.

Keywords- Chatting, AES, Android, Application**.**

1. INTRODUCTION

The programme created for SMS end-to-end security transmission. The Advanced Encryption Standards algorithm is employed. This app is unique and was created on the Android platform. The latter section of the paper describes how SMS, the AES algorithm, and our built application function.

1.1 Need for secure data transmission

Information security is the process of preventing unauthorised individuals from accessing, using, disclosing, disrupting, altering, viewing, inspecting, recording, or destroying data and information systems.

Everyone wants to keep their personal communications private.This privacy can be attained by encryption. It was created with that exact goal in mind. [5] Since short message service (Chatting app) is now a common business tool, both corporate organisations and customers are quite concerned about its security. In order to offer a safe means for communication, end-to-end text encryption is required for chat.

2. LITERATURE SURVEY

Mobile device security is becoming crucial due to recent trends in corporate mobility. In 2010, IDC noted that smartphone sales had now surpassed PC sales. Organizations are establishing bring-your-own-device (BYOD) policies more frequently as a result of the influx of devices and their recognition of the productivity and financial advantages. According to research firm J. Gold Associates, over 50% of businesses presently have a BYOD policy, with that number rising to between 25% and 35% during the next two years. Considering that Mobility changes from being a desirable feature to a competitive advantage. However, if smartphones and tablet PCs are not sufficiently shielded against mobile device security risks, the competitive edge and other advantages of mobility may be lost. Despite the market showing no signs of slowing down, IT organisations list security as one of their top worries with regard to increasing mobility. Consequently, a variety of encryption approaches are employed. [2] Governments and militaries have traditionally utilised encryption to enable covert communication. In many different types of civilian systems, encryption is now frequently employed to protect data. For instance, according to the Computer Security Institute's 2007 report, 71% of the firms examined used encryption for some of their data while it was in transit, and 53% used encryption for some of their data while it was being stored [3]. It is possible to employ encryption to safeguard data that is "at rest," such as files on computers and storage devices. (e.g. USB flash drives). There have been numerous cases in recent years of sensitive information, including consumer personal information, being stolen or lost from backup drives or laptops. Such files are more protected if they are encrypted while in transit than without it. [2] Another somewhat different example of utilising encryption on data at rest is digital rights management systems, which limit the use or reproduction of copyrighted content without permission and shield software from reverse engineering (see also copy protection).

6.1 trillion SMS text messages were sent in 2010. This amounts to 192,192 SMS sent each second. With a global market value of about $81 billion as of 2006, SMS has grown into a sizable commercial sector. While mobile networks charge each other interconnect costs of at least $0.04 when connecting between other phone networks, the global average cost of an SMS message is $0.11 worldwide. The SMS sector is vulnerable to attacks because it is growing so rapidly. The need to encrypt SMS before transmission has therefore increased.[3] Different encryption and decryption algorithms are in use. The most popular algorithm out of the entire bunch is AES.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

AES uses relatively little RAM and is extremely quick. AES encryption on Pentium Pro processors uses just 18 clock cycles per byte, providing an approximate throughput of 11Mib/s for a 200MHz processor. This was the primary justification behind our choice of the AES algorithm for encryption and decryption. [6] On Google Play, there are just a few SMS programmes that use the AES technique to encrypt messages. Our application was carefully built with a number of user-friendly elements in mind. It is really light, which actually makes it speedier, at less than 200Kb in size. All of the features that a regular SMS programme should have are available, including conversation view, Inbox, Draft, Backup, and Restore. The biggest benefit is that it is a really straightforward programme that is simple to use and comprehend. The primary encryption functionality's user interface is extremely straightforward and lightweight. and decryption of c h a t is carried out very efficiently.

3. SHORT MESSAGE SERVICE (SMS)

SMS, or short message service, is an acronym. Simply described, it is a means of communication that involves sending text from a PC or handheld device to a mobile phone, or from one cell phone to another. The word "short" relates to the maximum character limit for text messages, which is 160.The maximum SMS character length for other alphabets, such Chinese, is 70 characters.

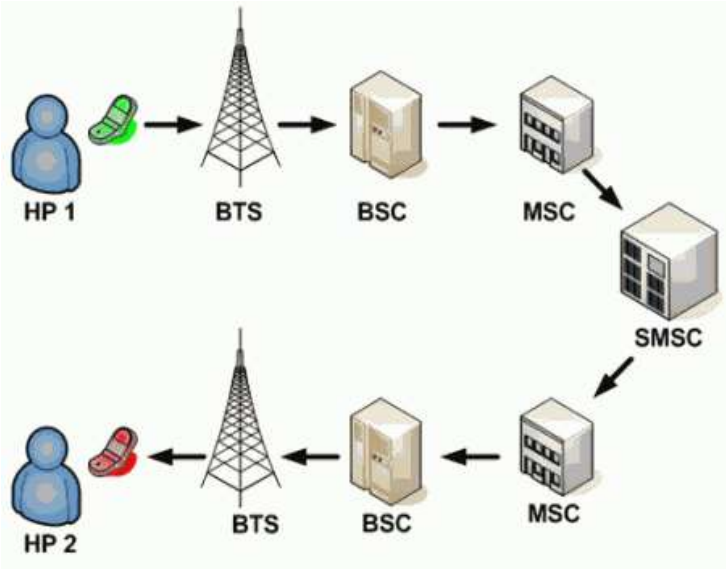


Fig. 1: Transmission of SMS

3.1 Working of SMS

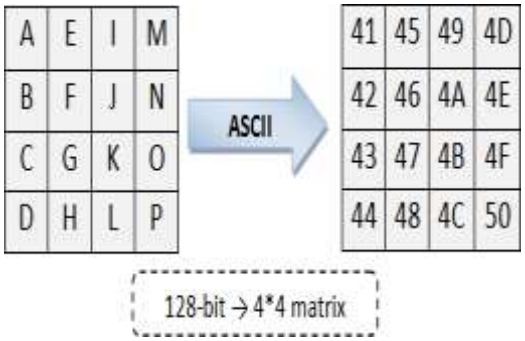
It is common knowledge that SMS service is a mobile phone feature, although SIM cards are not a requirement for SMS to function on other computing devices like PCs, laptops, or tablet PCs. A SIM card is required for SMS service because it has an integrated SMS centre client.

3.2 BTS

A piece of technology called a base transceiver station (BTS) enables wireless communication between user equipment (UE) and a network. Mobile phones (handsets), WLL phones, WiFi and WiMAX devices, laptops with wireless internet connectivity—among other things—are examples of UEs.

3.3 MSC

The mobile switching centre (MSC), which routes voice calls, SMS, and other services, is the main service delivery node for GSM/CDMA.The MSC establishes and releases the end-to-end connection, manages call-related requirements for mobility and handover, and handles billing and real-time pre-paid account monitoring.



www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

3.4 SMSC

When an SMS is sent from a mobile device, the SMS Center (SMSC) of the mobile carrier receives it, performs destination determination, and then sends the message to the destination devices. (cellphone). SMSC stands for SMS Service Center, and it is installed on the main networks of mobile carriers. SMSC serves as a temporary storage facility for SMS messages in addition to SMS forwarding. Therefore, if the target mobile device is not active, SMS will save the message and deliver it when the target mobile device becomes active. Additionally, the SMSC notifies the sender if the SMS delivery was successful or unsuccessful. However, due to limited storage space, SMSC cannot permanently save SMS messages not unlimited.SMSC and the sender's cell phone are in constant communication while the SMS is being delivered.Therefore, SMSC immediately alerts the sender cell phone that the SMS delivery was successful and informs it if the non-active destination cell phones become active.

This is the general operation of the SMS. The AES algorithm is discussed in the section after this algorithm

4. ADVANCE ENCRYPTION STANDARDS ALGORITHM/ RIJNDAELALGORITHM

AES-128, AES-192, and AES-256 are the three block cyphers that make up the Advanced Encryption Standard. AES uses a key size of 128, 192, or 256 bits and a fixed block size of 128 bits. The key-size has no theoretical bound, although the block-size has a maximum of 256 bits. The cypher employs a number of rounds of encryption to change plain text into cypher text. Each round's output serves as the next round's input. The output of the final round is the cypher text, which is ordinary text that has been encrypted. The State Matrix is a matrix into which the user's input is inputted.

Following are the four steps.

4.1 Sub Bytes Step

The SubBytes step of the AES algorithm is the same as this phase. Each byte in the matrix is rearranged using an 8-bit substitution box in the S-Box Substitution step. The Rijndael S-box is the name of this substitution box. The non-linearity in the cypher is provided by this process. The multiplicative inverse over GF (28), which is renowned for having good non-linearity qualities, is how the S-box was created. The S-box is built by fusing the inverse function with an invertible affine transformation, preventing assaults based on elementary algebraic features. The S-box was chosen in order to avoid both any fixed points that are opposite to one another and any derangements. [7] Data in the matrix become jumbled as a result of this process. For LPT and RPT, S-Box Substitution is done independently.

4.2 Shift Rows Step

On the rows of the state matrix, the ShiftRows step is carried out. It periodically moves each row's bytes by a specific offset. The front row stays the same. The second row's bytes are all moved one position to the left. Similar shifts are made to the third and fourth rows, which are moved by two and three positions, respectively. Both blocks with a size of 128 bits and those with a size of 192 bits have the same shifting pattern.

4.3 Mix Columns Step

The four bytes of each state matrix column are mixed using an invertible linear transformation in the MixColumns step [5]. A 4*4 matrix contains a polynomial that was produced randomly. During decryption, the same polynomial is utilised. The state matrix's columns are XORed together using

the polynomial matrix's corresponding column. The same column receives the revised result. The input for AddRoundKey is the output matrix.

4.4 Add Round Key

The cypher key is subjected to a number of processes to produce a round key.

Each byte of the state matrix is XORed with this round key. The Rijndael key scheduling technique generates a fresh round key for each round.

Decryption of the Proposed Algorithm

The terms "cipher" and "inverse cypher" are used to describe the encryption and decryption algorithms, respectively. The cypher and inverse cypher operations must also be carried out in a way that makes them cancel one another. Additionally, the rounds keys must be used in reverse. The input for the decryption procedure is the 256-bit 4*8 matrix-based cypher text.

4.5 Implementation

Any language can be used to implement the algorithm. Additionally applicable to image processing, this algorithm. We used Java to implement it because it is an open-source, cross-platform language. Below are the pseudo codes for each part of the cypher

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

4.5.1 Add Round key:

```
public byte[ ][ ]  addRoundKey(byte[ ][ ] state,byte[ ][ ]roundkey)
{
for (int i=0;i<4;i++)
{
for (int j=0;j<4;j++)
{
  state [i][j]=doExclusiveOR(state[i][j],roundkey[i][j]);
}
}
return state;
}
```

4.5.2 Substitute Bytes:

```
public byte[ ][ ] subBytes(byte[][] state)
{
for (int i=0;i<4;i++)
{
for (int j=0;j<4;j++)
{
int row = getFirstFourBits(state[i][j]);int column =
getSecondFourBit(state[i][j]);
state[i][j] =sBoxSubstitution(row,column);
}
}
return state;
}
```

4.5.3 MixColumns:

```
public byte[ ][ ] mixColumns(byte[ ][ ] state)
{
for (int c=0;c<4;c++)
{
state [c]=matrixMultiplication(state[c], polynomial);
}
return state;
}
```

4.5.4 ShiftRows:

```
shiftRows(byte state[][])
{
for(int i=0;i<4;i++)
{
//cyclic left shifts „i‟th row, „i‟timescyclicLeftShift(i);
```

4.6 Strength of the Algorithm

The technique uses a cypher key with a 128-bit length. Therefore, checking 2128 possible outcomes is practically unfeasible in order to crack the cypher key. As a result, the Brute-force Attack on this algorithm is unsuccessful.There must not be a fixed pattern in any of the algorithm's steps, according to the algorithm's flow. The suggested algorithm's components have significantly increased diffusion and confusion. As a result, ciphertext statistical and pattern analysis is unsuccessful. The fact that this method cannot be compromised by differential or linear assaults is its key security benefit.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

5. CHAT APPLICATION

The application functions as follows:

1. The user launches the app and logs in with a pattern lock.

2. User has the option to create a new message or reply to one that has already been sent.

3. If the option to create a new message is chosen, the user types the message and clicks the Encrypt button after adding the recipient's name. Before sending the message, the user must enter a cypher key. If the user doesn't enter a cypher key, one is automatically produced.

4. If the user chooses to reply to an already-sent message, he must first decrypt the message by holding down the long press key before typing the reply. Before the communication is sent, the user is prompted to input a cypher key.

5. The message is successfully sent and shown in the thread in encrypted form after the cypher key is entered.

5.1 Application Snapshots

Here are a few screenshots of the programme. It should be noted that, for obvious reasons, we are not publishing the entire application's layout. However, some of the most important pictures are included below. The user utilises this to confirm his identity. Once the user has authenticated and logged into the program, he can modify the lock code. The application closes after three unsuccessful tries.

5.2 Login

Fig. 3: Authentication

5.2 Chat Activity

The message and the sender's name are typed in by the user. As soon as the user begins writing the name, the appropriate contact information is shown in the dropdown menu. He can choose the name and number from the drop-down option after that. The dropdown menu below the name field displays any contacts with the initials "ro" or with "ro" as a subtext if the user enters "ro" in the name field, along with their phone number.

Fig. 4: Create Message

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

The user can send the message by inputting the cypher key or save it as a draught. By clicking the "Recent" button, the user can select any recent contact from his call history.

5.2.1 Thread View

The messages are shown as threads in the application's inbox. When you long-press a thread, you can choose to delete it, view the thread's contact information, or get in touch with the contact it belongs to.

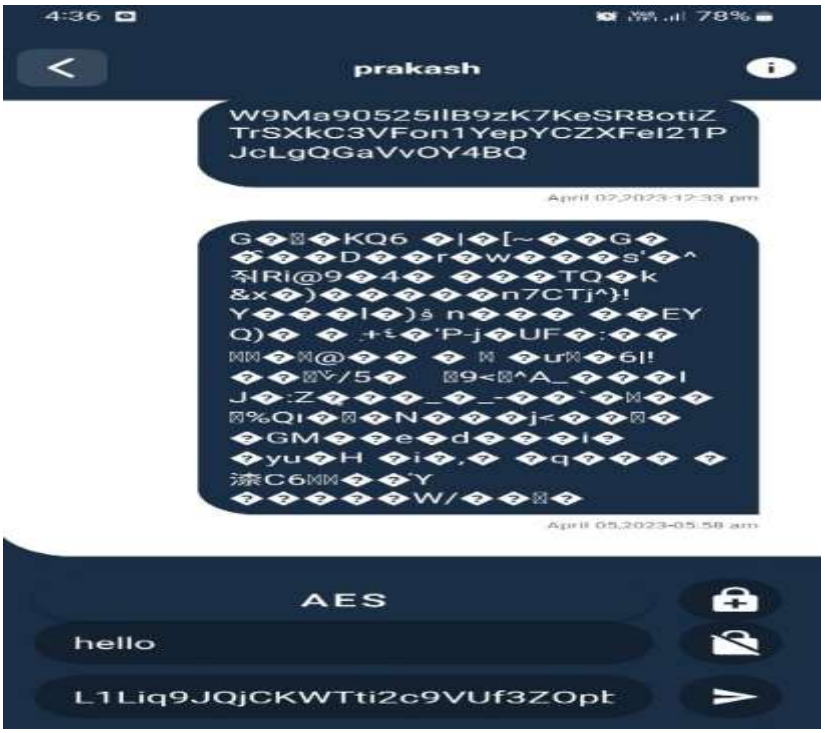


Fig. 5: Message Inbox

5.2.2 Thread View

The messages are presented as threads. The first two messages are displayed in encrypted form for ease of understanding, and the next two are displayed in decrypted form. Utilizing AES decryption, the message's encryption is broken.

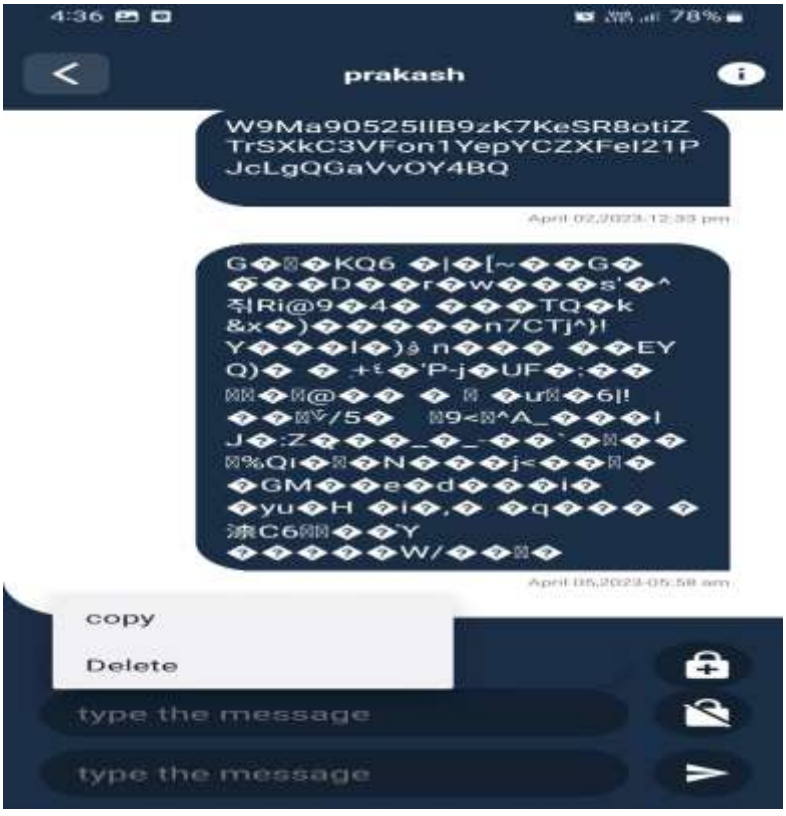


Fig. 6: Messages in Encrypted and Decrypted Form

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

5.3 Features of this Application

The application has the functionality listed below, among others:

1. Both the sender and the recipient can see all messages in a thread in encrypted form.

2. If you long-press the thread, an action box will appear with options to delete, browse contacts, or call the recipient.

3. By long-pressing any message in the thread, an action box will appear that allows the user to decrypt, delete, or forward the message.

4. If the user doesn't enter the cypher key, one is produced at random.

5.The user can choose from a number of options, including notification settings, display settings, encryption settings, tone settings, and personalization settings.

6. The Android platform was used to construct this application. Similar to other mobile operating systems, Android OS enables connectivity, messaging, language support, media support, Bluetooth, etc. This is why it is used. Java support and open source technologies would be Android's key features. Along with security and privacy, it also offers multitasking, multitouch, Wi-Fi, tethering, and 3G services.

5.4 Goals of this application

Our application's primary objectives are:

1. Creating a secure chatting application.

2. Keeping track of message receivers' encrypted data.

3. Message decryption in accordance with user preferences

4. Defense against information in messages being misused.

5. High privacy and enhanced security

5.4.1 Commercial Domain

In certain commercial settings, it is essential that information flow between different departments stay confidential and that other departments not become aware of it. When numbers and digits are more important than documentation, this application can be employed. The suggested application can be used to conduct secure network transactions.

5.4.2 Non-Commercial and Personal Use

There are situations when a user would prefer to retain secret and confidential conversations between two persons. chat encryption comes extremely handy in situations like this. A hacker would need a valid authentication key in order to comprehend the message.

5.5 Scope

The Android platform was used to create the application. It can therefore be used on any gadget running the Android operating system. Industries can use this application to communicate data securely. This application is available for non-commercial and private usage in addition to business and commercial use. This application's goal is to securely transfer data between two devices.

5.6 Pseudo Codes of Android Application

The code was created using the Android language. For obvious reasons, the original codes are not provided. The codes' primary logic is provided, though.

4.5.1 Send Message

In Android, There is a class SmsManager. We create instance of this class and there is a sendTextMessage() method in SendMessageManager class.

```
private void sendMessage() {
HashMap<String, Object> message = new HashMap<>();
message.put(Constants.KEY_SENDER_ID, pregerenceManager.getString(Constants.KEY_USER_ID));
message.put(Constants.KEY_RECEIVER_ID,receiverUser.id);
message.put(Constants.KEY_MESSAGE, binding.inputMessage.getText().toString());
message.put(Constants.KEY_TIMESTAMP, newDate());
database.collection(Constants.KEY_COLLECTION_CHAT).add(message);
if (conversionId != null) {
updateConversion(binding.inputMessage.getText().toString());
}els{
HashMap<String, Object> conversion = newHashMap<>();conversion.put(Constants.KEY_SENDER_ID,
pregerenceManager.getString(Constants.KEY_USER_ID));
```

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 1008-1016

e-ISSN : 2583-1062

Impact Factor : 5.725

conversion.put(Constants.**KEY_SENDER_NAME**,**pregerenceManager**.getString(Constants.**KEY_NAME**));
conversion.put(Constants.**KEY_SENDER_IMAGE**,**pregerenceManager**.getString(Constants.**KEY_IMAGE**));
conversion.put(Constants.**KEY_RECEIVER_ID**,**receiverUser**.**id**);
conversion.put(Constants.**KEY_RECEIVER_NAME**,**receiverUser**.**name**);
conversion.put(Constants.**KEY_RECEIVER_IMAGE**,**receiverUser**.**image**);
conversion.put(Constants.**KEY_LAST_MESSAGE**,**binding**.**inputMessage**.getText().toString());
conversion.put(Constants.**KEY_TIMESTAMP**,**new**Date());
addConversation(conversion); }

if(!**isReceiverAvailable**){
try{
JSONArray tokens = **new** JSONArray();
tokens.put(**receiverUser**.**token**);
JSONObject data = **new** JSONObject();
data.put(Constants.**KEY_USER_ID**, **pregerenceManager**.getString(Constants.**KEY_USER_ID**));
data.put(Constants.**KEY_NAME**, **pregerenceManager**.getString(Constants.**KEY_NAME**));
data.put(Constants.**KEY_FCM_TOKEN**, **pregerenceManager**.getString(Constants.**KEY_FCM_TOKEN**));
data.put(Constants.**KEY_MESSAGE**, **binding**.**inputMessage**.getText().toString());
JSONObject body = **new** JSONObject(); body.put(Constants.**REMOTE_MSG_DATA**, data);
body.put(Constants.**REMOTE_MSG_REGISTRATION_IDS**, tokens);
sendNotification(body.toString());
}**catch**(Exceptionexception) {
showToast(exception.getMessage()); }
}**binding**.**inputMessage**.setText(**null**);

4.5.2 Receive Message

For receiving any messages we create one BroadcastReciver. And we override onRecieve method of it which is basically called by system when any messages are received. But to doso we first have to register our receiver.

private void listenMessage() {

database.collection(Constants.**KEY_COLLECTION_CHAT**) .whereEqualTo(Constants.**KEY_SENDER_ID**,

pregerenceManager.getString(Constants.**KEY_USER_ID**)) .whereEqualTo(Constants.**KEY_RECEIVER_ID**, **receiverUser**.**id**)

addSnapshotListener(**eventListener**);
database.collection(Constants.**KEY_COLLECTION_CHAT**) .whereEqualTo(Constants.**KEY_SENDER_ID**, **receiverUser**.**id**)

whereEqualTo(Constants.**KEY_RECEIVER_ID**, **pregerenceManager**.getString(Constants.**KEY_USER_**addSnapshotListener(**eventListener**);

4.5.3 Notification-Using NotificationManager and Notification classes we caneasily create and display notifications on receiving message.public void createNotification(Context ctx)

NotificationManager notifManager = (NotificationManager)getSystemService(NOTIFICATION_S ERVICE);

// create object of Notification class Notification notification = new Notification();

// set the notification details. Here last parameter isPendingIntent

notification.setLatestEventInfo(ctx, “title”, “notification text”,null);

// Notify the system notifManager.notify(0,notification);

6. CONCLUSION

The goals for speed and compactness were therefore satisfied. The programme can be installed on an Android-powered mobile device and has a size of 50 kB. The lack of any delays experienced by the user while using the programme is a definite sign that the speed requirement is satisfied. We ensured that the user interface was easy to use and simple to navigate. Our programme can be used to authenticate the sender of a message in applications where access control is important.Additionally, it is possible to determine whether the message has been tampered with or corrupted during transmission. Most crucially, even if the device is obtained by an enemy, the messages containing sensitive information are securely saved and kept private. The security of the encrypted data against different attacks, such as Brute Force attack, pattern attack, etc., is the most distinctive and important factor to be taken into account. This application ensures secure, error-free data transport from beginning to end.

7. REFERENCES

[1] J.Daemen and V.Rijmen, AES Proposal: Rijndael, NIST"s AES home page, http ://www:nist:gov/aes."Announcing the Advanced Encryption Standard (AES)",Federal Information Processing Standards Publication 197, November 2001

[2] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.

[3] Hassinen M.: SafeSMS 1.0 user manual. October 2004,Department of Computer Science, University of Kuopio.

[4] http://www.cs.uku.fi/~mhassine/SafeSMS/Manualen.pdf

[5] G. Racherla, D. Saha, "Security and Privacy Issues in Wireless and Mobile Computing", Proceedings of 2000 IEEE International Conference on Personal Wireless Communications, Dec 17-20, 2000, pp.509-513.

[6] [6]H. Marko, H. Konstantin, "Strong Mobile Authentication",Proceedings of 2nd International Symposium on WirelessCommunication Systems, Sept 5-7 2005, pp.96-100.

[7] Advanced Encryption Standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[8] http://ieeexplore.ieee.org/document/7301181/

[9] http://ieeexplore.ieee.org/document/6603755/