iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: V Month of publication: May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5135

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue V, May 2018- Available at www.ijraset.com*

# Cryptography on Android Messaging Application using End to End Encryption

Prof. Vidya Pujari[1], Ram Motwani[2], Aakash khiani[3], Jitesh Ahuja[4]
[1, 2, 3, 4]*Vivekanand Education Society's Institute of Technology*

***Abstract: Communication through messaging service is very popular now-a-days and it is cheap, fast and simple. However, when confidential information is exchanged using messaging service, it is very difficult to protect the information from messaging service security threats like man-in-middle attack and eavesdropping. Most of the times, these threats are difficult to detect and therefore increasing the security of messaging service communication is the only way to avoid such threats. Earlier messaging security was generally provided through single encryption mechanism but this mechanism is not sufficient to encrypt a file (i.e. audio, video, text and image). Also, there were no systems that would encrypt a file in a single system in messaging service communication. This system implements self-destructing messages using layered encryption, an enhanced messaging architecture equipped with self-destructing feature and encryption of a file in a mobile environment. Senders will be able to set sensitivity levels for their messages. This system presents a design for Android platform application and is equipped with three modes for sending the messages, namely- Insecure, Secure and Ultra Secure. In this system we propose an efficient algorithm for cryptography which is based on end to end encryption. Asymmetric encryption and decryption is used in this system. This application makes use of end to end AES Encryption algorithm and a self- destructing timer to send and receive messages. Our system is different from others because in our system, sender sends the private information to the receiver with a specific sensitivity level. With that sensitivity information, the message will be destroyed from the database and the user's device. All the data stored in the database will be encrypted to increase the security of the system.***

***Index Terms*: Encryption, Decryption, Cryptography, AES algorithm.**

## I. INTRODUCTION

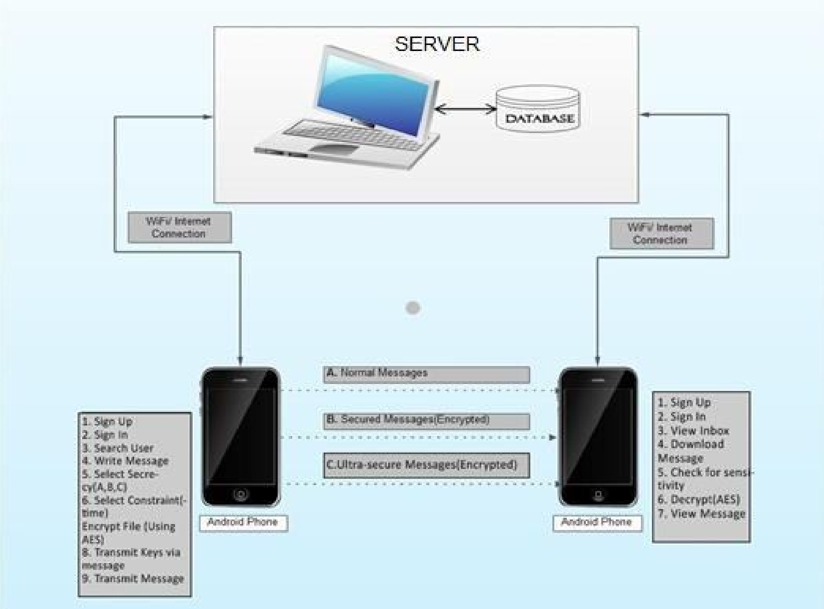
Communication through messaging service is very popular nowadays and it is cheap, fast and simple. However, when confidential information is exchanged using messaging service, it is very difficult to protect the information from messaging service security threats like man-in-middle attack and eavesdropping. Most of the times, these threats are difficult to detect and therefore increasing the security of messaging service communication is the only way to avoid such threats. Earlier messaging security was generally provided through single encryption mechanism but this mechanism is not sufficient to encrypt a file (i.e. audio, video, text and image). Also, there were no systems that would en- crypt a file in a single system in messaging service communication. We propose self-destructing messages using layered encryption, an enhanced messaging architecture equipped with self-destructing feature and double encryption of a file in a mobile environment. Senders will be able to set sensitivity constraints for their messages. The constraints will determine where and when the sent messages are decrypted. The paper presents a design for Android platform application and is equipped with three modes for sending the messages, namely- Insecure, Secure and Ultra Secure.

## II. OBJECTIVE

This design is implemented in an android application to develop a secure chat application. The android mobile application must be capable of handling numerous different users wherein a user should be able to use it smoothly. Today's messaging services, the users are subjected to constant unwanted leakage of confidential information compromising on the integrity of their privacy. Present day systems have features like self-destruction for message transmission. These systems do not provide layered encryption for the data along with the time constraints. Hence this system will incorporate features like End-to-End encryption along with self-destructing timer. Since the main objective of this system is to provide a platform for secure and efficient messaging services, this system can be used by any organization where confidentiality of information is the top priority. As the messages have a time constraint along with levels of sensitivity, they cannot be decrypted by any third party. Due to this feature, the application can find it's use in government and private organizations including army. It can be also used at personal level for a secure transmission of data.

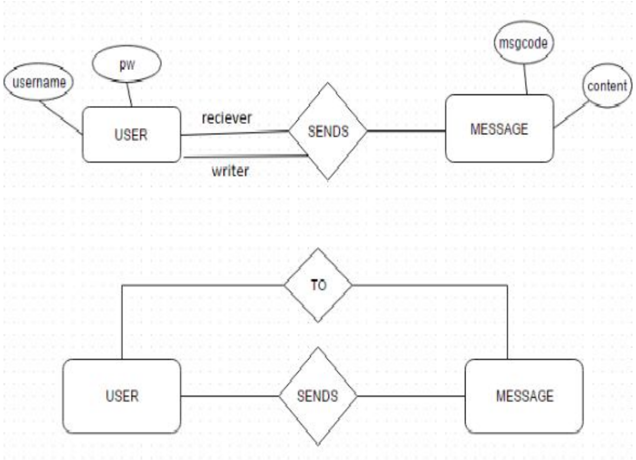
## III. PROPOSED WORK

The paper aims at creation of an instant messaging service that will provide encryption in three different modes- Insecure, Secure, Ultra-secure and destruct the message from the server automatically after certain time elapses. The proposed system will encrypt and decrypt text. Any user can state the location constraint for the message which will determine where the message will be decrypted. The user's mobiles will have to be connected to the network. For this purpose, either virtual router or hotspots can be used. Once the users are connected in the network they can make request to the server and get access to the web services. The server that we have used is the AWS server as it is known to be one of the most efficient servers .



The main components of the process are as follows Operations performed by a user

1) *Sign Up:* The sender has to register first to use the application. The sender has to give their Unique ID, a valid mobile number and a password in the registration process.
2) *Sign In:* Once the sender has sign up, sender can sign in using the UID and password that has been set in the registration process
3) *Search User:* In this step, the sender will select the receiver to whom the message is to be sent. The UID of only those users will appear to the sender who are registered with the server. Other names from the sender's mobile phone will not appear in the list
4) *Send Message:* The sender then will select the message file that is to be sent. The file could be any file from the mobile.
5) *Select the Security Mode:* The sender will have to select the one of the three modes i.e. insecure, secure and ultra-secure. If the sender is selecting the ultra-secure mode, he/she first has to set a private key which will be used for encryption of the message and also for the decryption of the message by the receiver
6) *Set the Constraint:* Constraints determine the level of security and a flag. The user will select the flag constraint on his discretion, on selecting this constraint, the level of security can be set. A timer would then get associated based on the set constraints and message size
7) *Encrypt File:* As shown in fig 3.2 the file will be encrypted using AES-256 algorithm and in ultra-secure mode and AES- 128 in secure mode[2].
8) *Transmit Message:* Message will be sent to the receiver.
9) *Receive Message:* Receiver can view the files received along with the type of mode for encryption and time when they were sent.
10) *Decrypt message:* The downloaded message will be decrypted and stored in the receiver's mobile phone.



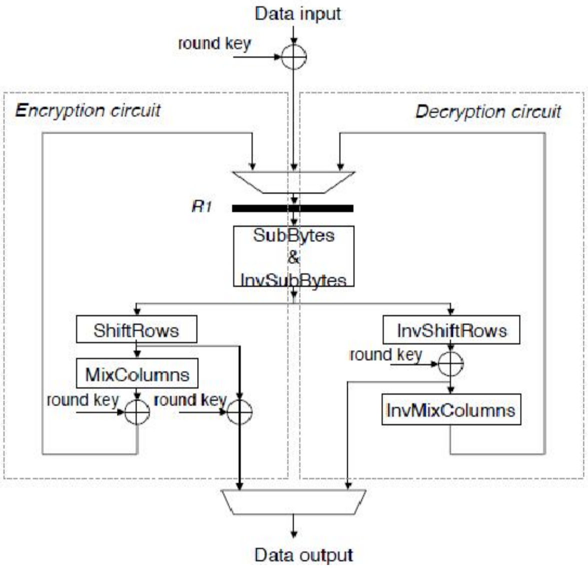


FIG 3.2 AES Block Diagram

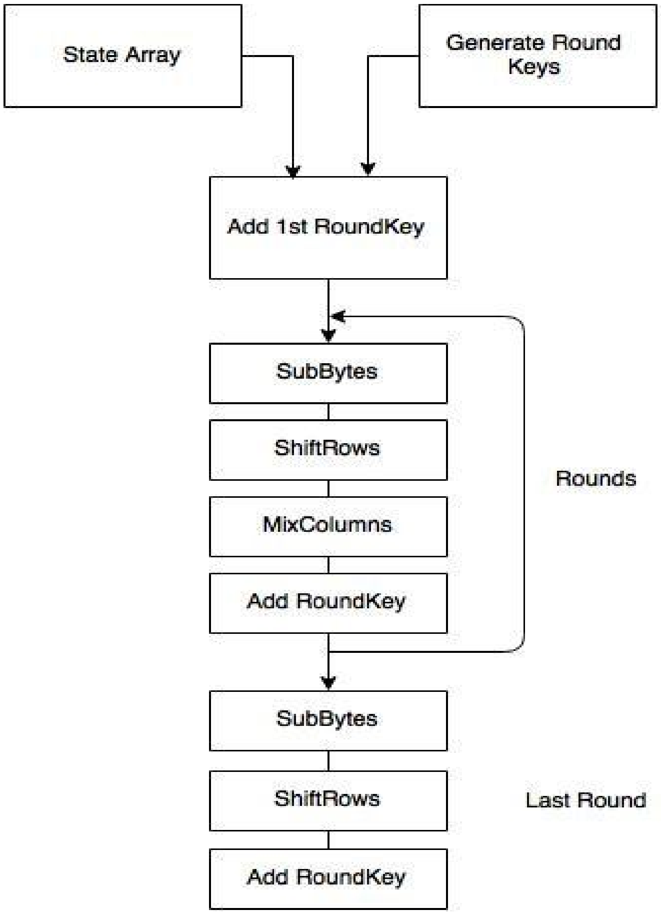
### *A. Aes Encryption And Decryption*

Rijndael is the block cipher chosen by NIST to replace the older Data Encryption Standard (DES). The version of Rijndael selected for AES accepts a 128-bit block of input plain-text data and either a 128, 192, or 256-bit key encryption key. The encryption process applies four different transforms over a series of rounds with the number of rounds depending on the key size chosen. Each transform acts to either add diffusion or non-linearity to the "state" or data be encrypted in the step. The four transforms are:

Sub Bytes substitute state bytes with bytes from the predefined Rjindael S-box

Shift Rows right shift bytes by row by incrementing values Mix Columns – multiply each column by a fixed MDS matrix ( Add Round Key XOR each byte of the state with it's corresponding byte of the current round's key

While the first three transforms involve only the state data, the last step mixes the encryption key using a derived "partial" key that is unique for each round. These partial keys are created via the key schedule. The key schedule is a complex process wholly separate from the rest of the cipher and must be done either in advance or run in parallel.The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? the data to be encrypted. This array we call the state array. You take the following aes steps of encryption for a 128-bit block.. 1.Derive the set of round keys from the cipher key the state array with the block data (plaintext). 3.Add the initial round key to the starting state array. 4.Perform nine rounds of state manipulation. Perform the tenth and final round of state manipulation. Copy the final state array out as the encrypted data (ciphertext).



## IV. REVIEW OF LITERATURE

and select "send". Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. messaging has existed in some form or another for decades. Generally, it is a process by which users on a computer network can quickly communicate with one another using short text-based sentences rather than using email. Each user has a piece of software that communicates with a common server that connects the chat sessions[5]. Over the past few years, two distinct settings for the use of instant messaging have evolved. The first is the corporate or institutional environment composed of many potential users but who are all under the same organizational umbrella. The second setting is individual users "after work" or at home who do not have a mission-oriented commonality between them, but are more likely family and friends. In the corporate setting, security risks are apparent from the outset. What stops a disgruntled employee from messaging some sensitive company data to a colleague outside the enterprise? The reverse of that would be the example disgruntled employee downloading some virus or spyware onto his machine inside the corporate firewall to release as desired. Accordingly, organizational offerings have become very sophisticated in their security and logging measures. Typically, an employee or organization member must be granted a login and suitable permissions to use the messaging system. This creating of a specific account for each user allows the organization to identify, track and record all use of their messenger system on their servers[5].

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation. The systems are designed to defeat any attempts at surveillance or tampering because no third parties can decipher the data being communicated or stored. For example, companies that use end-to-end encryption are unable to hand over texts of their customers' messages to the authorities[2]

This system incorporates AES-128 and AES-256 bit encryption algorithms for providing end to end encryption solution. AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation, and is fast in both software and hardware[6]. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or
256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits[6].

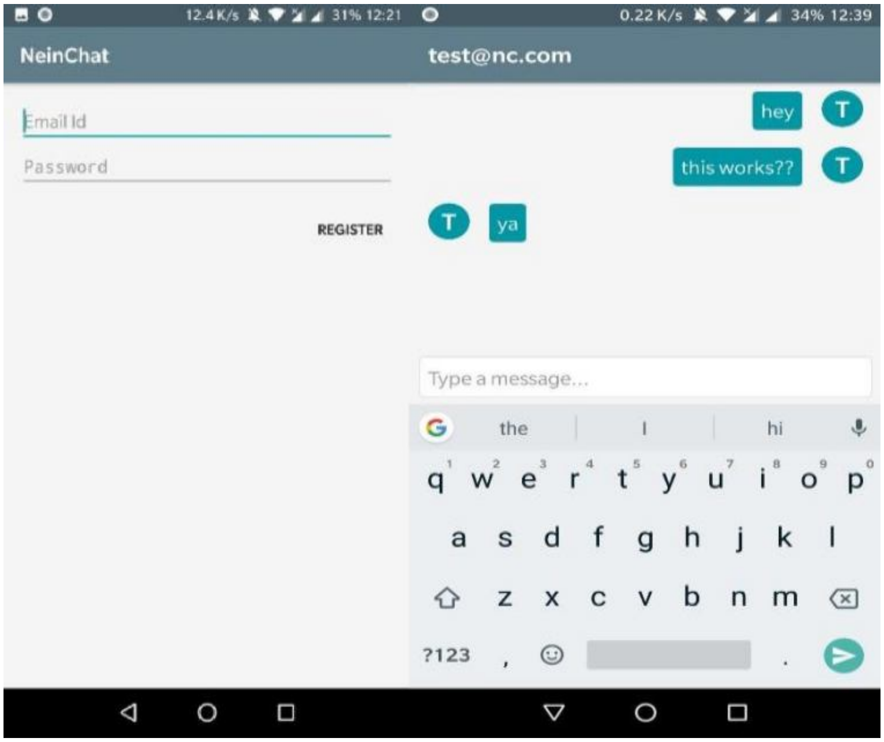
Instant messaging (IM) is a type of online chat that offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted between two parties, when each user chooses to complete a thought

## V. IMPLEMENTATION

The system implements Java, Android Studio, Firebase Real- Time Database, Firebase Cloud, and JSON. The system is capable of running on Android devices. The interface for the system will provide a platform for users to send self- destructing messages.

### A. *Application Setup*

1) *Main Page*-The first page of the application will allow user to register/ Sign-In to the application. The main page have database connections via Firebase Console for registration and Authentication
2) *User Signup Page*-Customers will be able to sign-up/register for an account with the Chat Application. Incomplete information will be dropped from the database. Only information that is complete will allow to be submitted to the console. The page should check the values be submitted and determine if the value is null.
3) *User listing page*-This page will display a list of registered users. A user can send text messages to any user from the list. When a customer chooses to send a text message to a user, their User_id, Reciever_id, Message and Timestamp will be passed to the Firebase Console to store the information.
4) *Chat Activity Page*-This page will have a display area to view received and sent messages and an input text field allowing user to type and send messages.
5) *Server setup*- Firebase provides a realtime database and backend as a service. The service delivers files over a content delivery network (CDN) through HTTP Secure (HTTPS) and Secure Sockets Layer encryption (SSL). The method for deletion used is time stamp based, the database records the timestamp for when the receiver opens the chatting application. The trigger works when the user opens the chat interface. A timer stars counting the time in milliseconds and then deletes the tuple from the database, thereby securing the integrity.



hey
this works??
ya

## VI. RESULT ANDEVALUATION

The system was successfully implemented and covers all the major criteria which was set. A user can successfully communicate in a secure manner with another user without compromising on the security of their privacy.

The text entered is encrypted using AES-256 algorithm which is uploaded to the cloud server using Server Socket Layer security by implementing the HTTPS protocol, thus ensuring double protection for their data.

## VII. CONCLUSION

This application allows users to communicate privately because of the high-endsecurity measures provided within the application Users can communicate and transfer data with an ease and with comfort of being able to securely transferring text because of the self-destructing feature available in the app.

## REFERENCES

[1] Forensic Analysis of Secure Ephemeral Messaging Applications on Platforms Shraddha Badade, Rasika Borate, Sayali Dhobale, Pooja Ghogare. Department of Computer Engineering, Bhivarabai Sawant College of EngineResearch, Narhe, Pune, India, 2015.

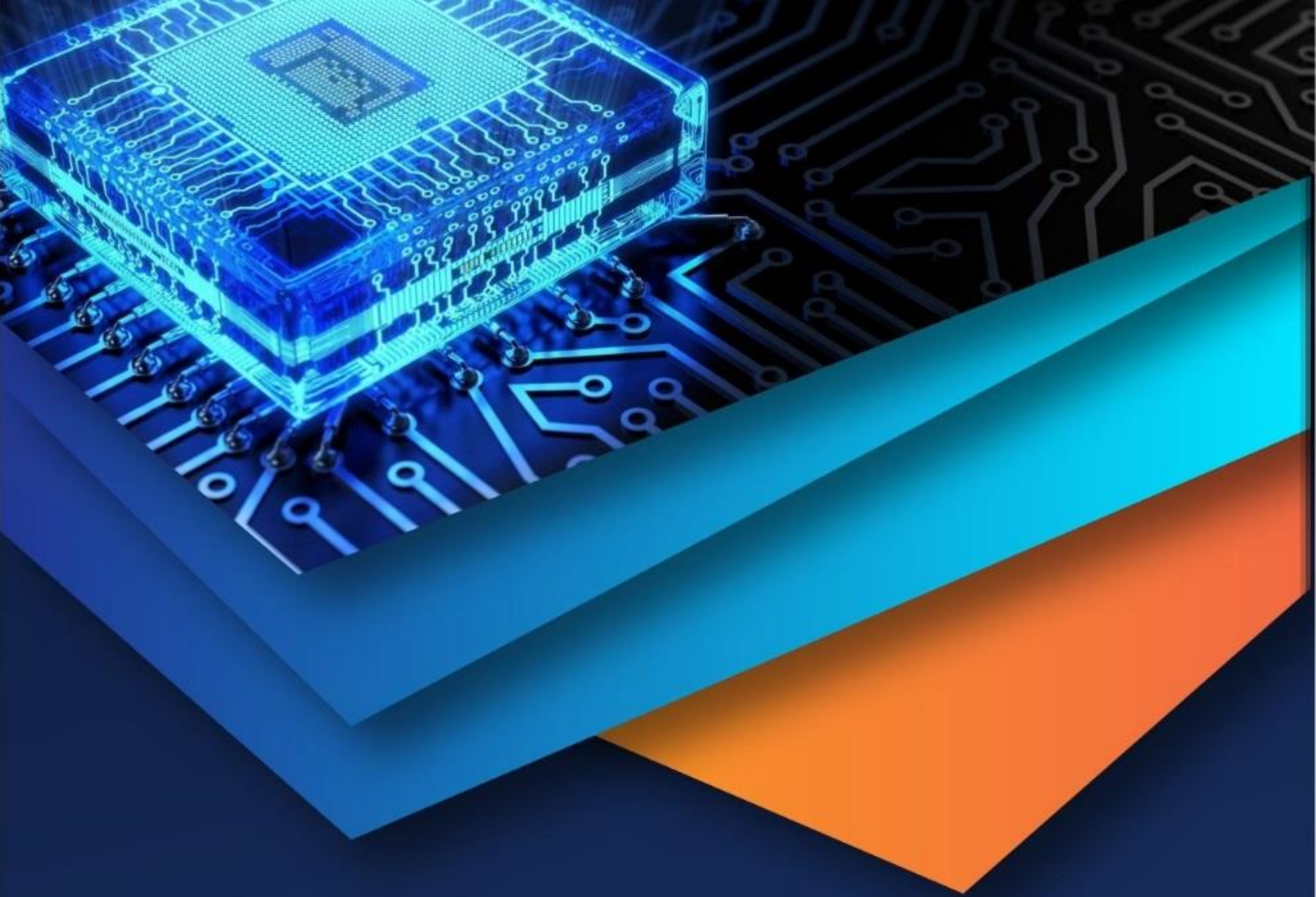
[2] Cryptography On Android Message Application Using Look Up Table And Dynamic Key (Cama) Manisha Madhwani1, Kavyashree C.V.2 , Dr. Jossy P. George. Department of Computer Science, Christ University, India, 2012

[3] Self-Destructing Messages Using Layered Encryption for Mobile Devices M.A Hannan Bin Azhar and Thomas Edward Allen Barton.Computing, Digital Forensics and Cybersecurity, Canterbury Christ Church University, Canterbury, United Kingdom

[4] “The Wickr Messaging Protocol” technical paper by Chris Howell, Tom Leavy & Joël Alwe

[5] https://en.wikipedia.org/wiki/Instant_messaging

[6] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno; et al. (May 2000). "The Twofish Team's Final Comments on AES Selection"



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY