MESSENGER: ANDROID MESSENGER WITH END TO END ENCRYPTION

Mr. Anas Dange[1], Mr. Danish Memon[2], Mr. Avinash Sahu[3], Mr. Brijesh Menon[4], Mr. Gaurav Datt[5]

[1,2,3,4,5]*Department of Computer Engineering Universal College of Engineering Vasai, India*

---***---

Abstract: The involvement of generation in our existence makes it more boost and affords get right of entry to our fingertip. It provides us with the capability to get connected with human beings and discover the data on the topics which could be very useful for the ease of existence. Hence our lives are dependent on numerous mobile chatting applications which offer exclusive protection to user and chatting information but leads to boom in vulnerabilities and threat of attack on facts. As in sensitive enterprise and prison conversation records safety is maximum important for stopping from undesirable hacking activities. To overcome this form of state of affairs, it's miles proposed an encrypted messaging protocol for secure conversation. Inside the International messaging, there is lots of encrypted messaging applications, however all those are based totally on a software generated encryption key in conjunction with SQLite database which is used to keep the message of respective customers which are now not comfy and the messages of any consumer can be obtained by a 3rd party. The proposed software used the Elliptic Curve Diffie Hellman Key change (ECDH) set of rules to generate the important thing pair and alternate to supply the shared key to be able to be used for the encryption of statistics by symmetric algorithms. The proposed utility lets in the customers to talk via textual content messages, voice messages and snap shots. For the text message protection the same old AES algorithm with a 128 bit key are used. The generated key (160 bit) minimized to 128 bit period via deciding on the primary 128 little bit of the generated key in order to be used by the AES set of rules. For the voice and photo protection procedures the proposed utility used the symmetric set of rules RC4 for this purpose.

Keyword: Android, Chatting Application, ECDH (Elliptic Curve Diffie Hellman Key Exchange), AES (Advan Encryption Standard), RC4 (Rivest Cipher 4).

I. INTRODUCTION

The mobile immediately message applications have beaten the fast Message service (SMS) operated through cell network providers, with 19 billion messages despatched for each day contrasted and extra than 17 billion SMS messages immediate message will anticipate an crucial component in a while enterprise territories, which might be prevalently known as mobile trade, mobile banking, administrative use, and everyday life correspondence. moreover, instant message has become a well-known wi-fi provider all over the world as it encourages a purchaser to keep up a correspondence with any cellular smartphone subscriber wherever on earth. With the increasingly more developing dependence on cell chat gadget in a single hand, and the growing number of vulnerabilities and attacks however, there may be an undeniably hobby for the safety solutions. There are likewise some extra protection troubles inside the wi-fi media that are not the scenario in a stressed framework in this way, awesome secure protocols are required for collection mobile chat gadget platforms clients utilize a cell chat service to communicate with each other, a manner that could incorporate relaying individual facts. The security and safety of such communications ought to be considered important. Anyways, past due scenes of powerlessness inside the enormous chat offerings find that they won't be robustly actualizing protection and safety highlights. The late years, statistics Confidentiality, Authentication, Integrity, Nonrepudiation, get right of entry to manipulate, and Availability are the most imperative safety offerings in the security standards that must be considered in comfortable programs and frameworks. However, there may be no association for such protection offerings in the cellular chat structures. each mobile chat system client and cell chat system server are defence against each passive and lively attacks. Passive risks be a part of arrival of message substance, and visitors examination whilst active risks consolidate adjustment of message substance, masquerade, replay, and denial of provider (DoS) reality be advised, all of the designated risks are appropriate to the cell chatting communications the security and protection saving additives of distinct versatile applications have long gone under the highlight. There are diverse safety and protection highlights given by different cell chat programs, yet there aren't very many transportable talk packages that provide a stop-to-stop encryption administrations safety to their customers

II. LITERATURE SURVEY

Right here for our mission we've carried out many studies paper a number of them are given beneath:

Encryption software the usage of Ceasar Cipher and Vigner Cipher which was published on IEEE in 2016 It became posted by means of Ferri Fahrianto, Siti ummi Mashruroh There proposed paintings changed into to test which of the following algorithms paintings satisfactory for safety in android application and that they observed that to enhance records safety by means of encrypting the text by way of merging the two encryption technique which are ceasar cipher and vigner cipher.[1]

Implementation software internal Chat Messenger using Android gadget which turned into posted on IEEE in 2017 with the aid of Robi Sanjaya Abba Suganda Girsang their proposed work become to analyse system requirement and person requirement to make the messenger greater feasible and user pleasant and they founded that Its basically approximately how api works in android running device how on the spot messaging works and the way prototype model works.[2]

Android Forensics analysis: Non-public Chat on Social Messenger which became published on IEEE in 2016 by way of G. B. SatryaP. T. Daelyd S.Y. Shin.Their proposed work changed into to find what are the distinction among the public and private chat utility and their findings. To discover difference between private chat and normal chat and the way it's far very effective.[3]

Group-based totally conversation in WhatsApp which changed into published on IEEE in 2019 with the aid of Michael Seufer Tobias Hobfeld. Their proposed work changed into discover how the organization chats and messaging works and their finding changed into how media is shared inside the groups and which type f records base is used to store the messages and how can we make that records base comfortable.[4]

Green records security for cellular immediate messenger which turned into published on IEEE in 2018 by means of Rita wonda Houg I Jie.Their proposed paintings became to check whether the approach produce green time in authentication and encrypt method while applying in application and their finding changed into how the storage isuue is solved in latest and maximum popular chat app and what features the chat app have to incorporate.[5]

Exploring user's belief of storage control capabilities in on the spot Messaging applications: A Case on WhatsApp Messenger become posted on IEEE in 2019 by Mashael M.Alsulami and Arwa Y Al Aaama .Their Proposed paintings changed into To cure the problem of garage control and protection management of the person in effective way and their locating changed into how the garage isuue is solved in recent and maximum famous chat app and what functions the chat app should incorporate.[7]

III. SECURITY AND PRIVACY CHAT APPLICATION

Before we present the info of the proposed structure for mobile chat applications, this phase provides a brief requirements that the sort of idea need to meet:

Req1: The sign-up system must require minimum records associated with the consumer. The account introduction procedure need to no longer depend closely on non-public identification records (PII).

Req2: The important thing trade manner must be relaxed, seamless and aid o -line chat.

Req3: Encryption/decryption of messages ought to no longer require user interaction (i.e. least interplay).

Req4: Comfy one messages can be communicated securely at the side of potential key share.

Req5: Customers have a mechanism to authenticate every other, assuring themselves they are speaking with the proper character

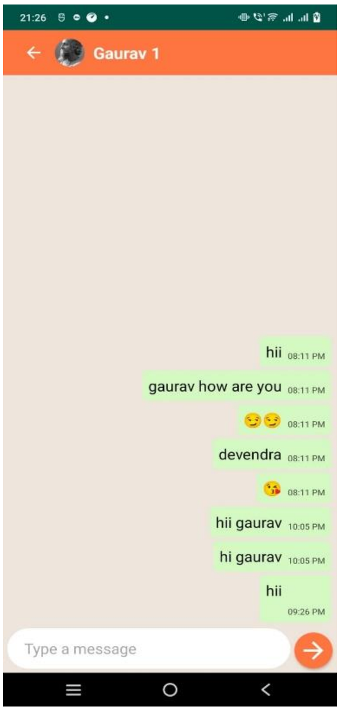
Req6: Communications aren't saved on the chat server. One's chat is stored on user's cell.

Req7: Nearby chat storage must be appropriately covered.

Req8: To protect the privateness of the customers and their chat, the message-server ought to now not be able to retrieve the messages.

IV. MESSAGE COMMUNICATION

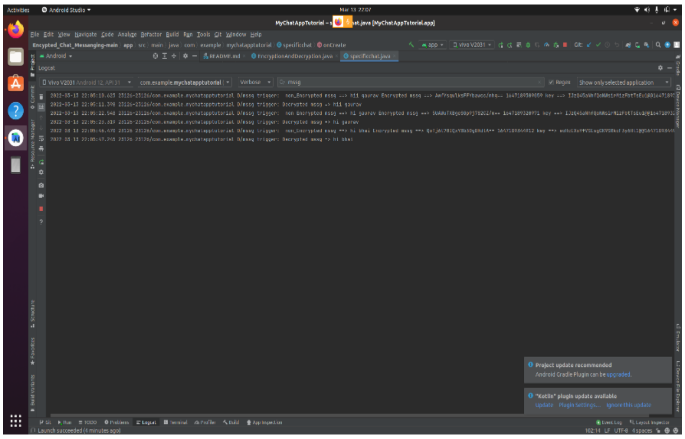
On this segment, we talk how character messages are constructed and the way shared grasp secrets used to generate message keys. The keys are then used to encrypt and decrypt the messages. every message send by using character customers is encrypted with the aid of a key, generated the usage of the shared grasp key and four random numbers. To generate message keys, we use the Pseudorandom variety Generator (PRNG) design. The shared (four) random numbers are taken as the seed le: for each generation a random wide variety (n) is encrypted using the shared master key. The output is used because of the message key. The output is once more encrypted the use of the shared master key, the output is XOR with n. The output of the XOR operation then replaces the fee of n inside it.



hii 08:11 PM
gaurav how are you 08:11 PM
😏😏 08:11 PM
devendra 08:11 PM
😘 08:11 PM
hii gaurav 10:05 PM
hi gaurav 10:05 PM
hii 09:26 PM

V. PROPOSED SYSTEM

1. Proposed Encryption Method


Activities
Android Studio
Mar 13 22:07
MyChatAppTutorial – specificchat.java [MyChatAppTutorial.app]
File Edit View Navigate Code Analyze Refactor Build Run Tools Git Window Help
Encypted_Chat_Messanging-main app src main java com example mychatapptutorial specificchat onCreate
app
vivo V2031
Android
README.md
EncryptionAndDecryption.java
specificchat.java
Logcat
Vivo V2031 Android 12, API 31
com.example.mychatapptutorial
Verbose
mssg
Regex
Show only selected application

```
2022-03-13 22:05:10.623 23126-23126/com.example.mychatapptutorial D/mssg trigger:  non_Encrypted mssg --> hii gaurav Encrypted mssg --> AmfYoqwlksFFYbawco/mhg== 1647189309059 key --> IJzQ4SaWhfQoNWsirM1zFbtTsEu1@01647189
2022-03-13 22:05:11.398 23126-23126/com.example.mychatapptutorial D/mssg trigger: Decrypted mssg -> hii gaurav
2022-03-13 22:05:22.548 23126-23126/com.example.mychatapptutorial D/mssg trigger:  non_Encrypted mssg --> hi gaurav Encrypted mssg --> 5UAWuTX8ge9Bp9j782C2/w== 1647189320971 key --> IJzQ4SaWhfQoNWsirM1zFbtTsEu1@01647189
2022-03-13 22:05:23.519 23126-23126/com.example.mychatapptutorial D/mssg trigger: Decrypted mssg -> hi gaurav
2022-03-13 22:05:46.470 23126-23126/com.example.mychatapptutorial D/mssg trigger:  non_Encrypted mssg --> hi bhai Encrypted mssg --> QuIj6L7BJQxY8b5DgBKdlA== 1647189344912 key --> wdlcEXuYfVSLagGK9SBkcF3y6HL1@01647189
2022-03-13 22:05:47.268 23126-23126/com.example.mychatapptutorial D/mssg trigger: Decrypted mssg -> hi bhai
```

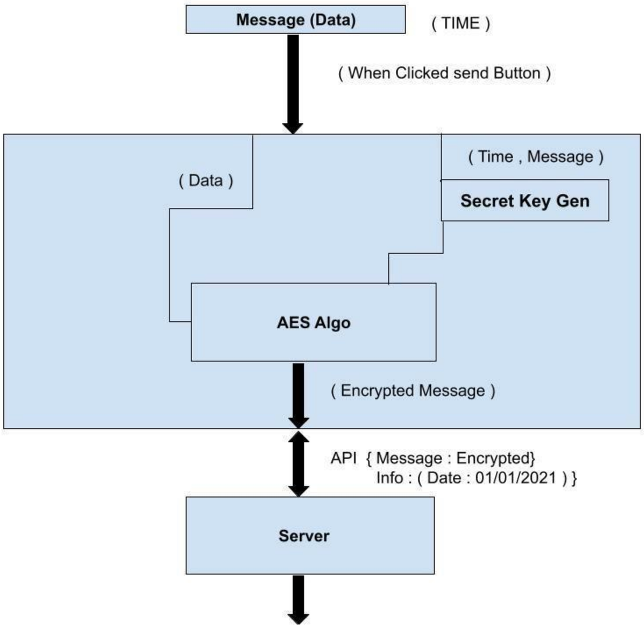
Project update recommended
Android Gradle Plugin can be upgraded.

"Kotlin" plugin update available
Update Plugin Settings... Ignore this update

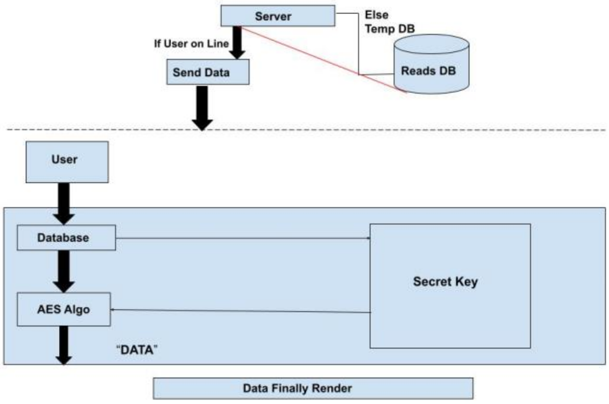
Launch succeeded (4 minutes ago)

2. Theory of our Encryption

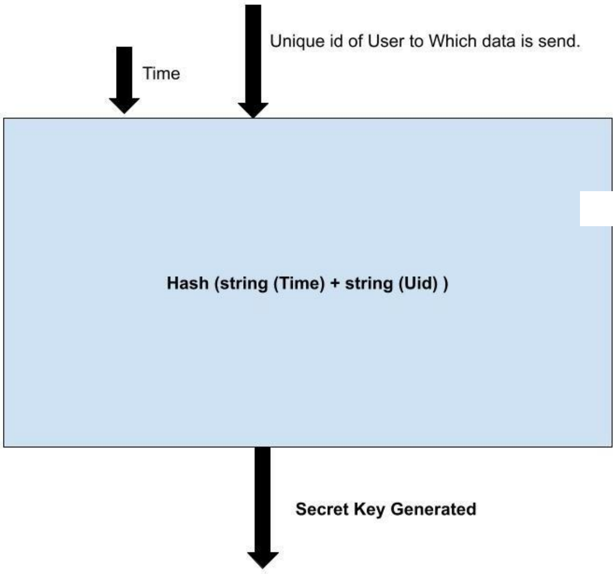
In our project we are basically using the AES algorithm because it's the one of the most powerful encryption algorithm. We are trying to overcome one of the drawback of the present AES algorithm that It always encrypt the message in a same way. Now here we are trying to overcome this drawback and make this Algorithm more strong. Now let us consider there are 2 users that is user A and User B Both the users will be having their unique id now when the user A wants to send the message to user B and the message sended by the user A will trigger to the AES algorithm in the form of Secret key Now then it will be passed to the server now the server will check whether the User B is online or not.[1]



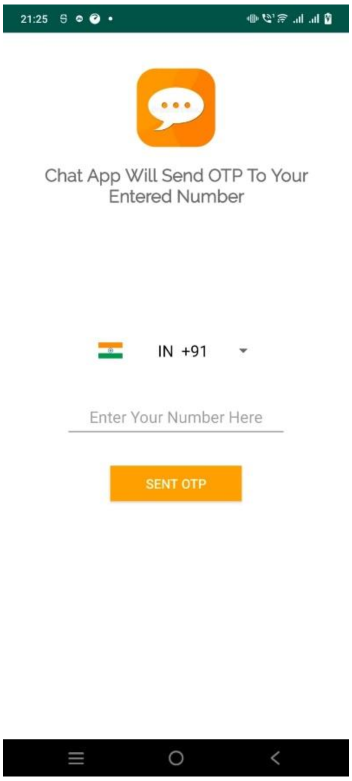
If the user B is online the server will Send the Cipher text that is the secret key to the user B and it will be store in the local Data base now let us consider that the user B is offline Now this message will be store in the Database DB Sever will try to contact the user B Whenever the user B comes online it will be connect to the user and the server will contact to the database where the message for user B is Stored in Encrypted form then it will give it to User B and the message in the form Of Cipher text will be store in the local database Then The user B will Able to Decrypt this message with the help of Secret key after that the message will be Passed Through AES algorithm For Decryption And the User B will Able to see the message.[2]



Here we will discuss about how Secret key is generated:- Consider the above example that suppose there Are 2 Users that is A and B now user A wants to message user B When the user A clicks on the Send button we will trigger the Date and Time of That instant using some function now User A and B have their unique id respectively now we will take time and the unique id of user A and then convert this into the H code This will be our Secret key which will be used to encrypt and Decrypt The message Through out. Here We are considering the variant parameters to protect the message from the Third Party. Time which will be always different for different messages. Like we can use Ip address which is different for different devices.[3]


Time
Unique id of User to Which data is send.
Hash (string (Time) + string (Uid))
Secret Key Generated

User can make an account by adding his/her mobile no and can click on verify then the OTP will be generated that is known as Two factor authentication.[4]

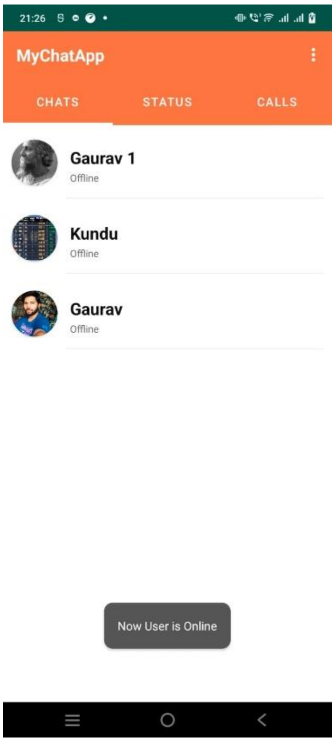


VI. PROPOSED ALGORITHM

```
Message (“ Hi ”) + send.button => Secret_key = hash (Date
+ user2.UID);
//message ecn.
AES (message, secret)
//api Data={
Mesaage : encrypt_message; Date: date
}
//user DB Data.save()
// generation of secret key Secret_key
= hash (Date + user2.UID);
```

VII. MAIN CHAT SCREEN

In this part the user can see the another user in our chat screen. whenever the user click on another user profile he/she can see the chat UI where the user can send the message and receive the message.



VIII. CONCLUSION

In this paper, we supplied an open specification for a comfy and privacy- maintaining chat service. We defined the fundamental necessities, structure and implementation reveal in in deploying this kind of service. The aim of the paper is to broaden cell chat offerings and discover any ability complexities worried in this type of service presenting privateness protection to its clients. In these papers, we explored the theoretical foundations and technical challenges confronted if privacy safety is constructed into a chat service. We found that maximum of the theoretical and technical components are already available. With a few minor changes, a strongly privacy-based chat provider can be constructed. We've proven that a secured and privacy -preserving chat software is technically feasible. In the course of the implementation of the framework, we did no longer face any severe issues regarding the generation or performance that would make this thought infeasible. Whether it's far a feasible enterprise its a distinctive aspect of this sort of provider. In destiny research, we would love to test with the scalability and performance of the chat server: this might screen a few bottlenecks in building and preserving a privateness-primarily based chat server. Some other potential factor is investigation of the way the text chat carrier proposed in this paper could be extended to a voice and video chat carrier. The demanding situations supplied in offering a secure and privacy preserving voice and/or video chat carrier is probably extra than those pre-sended by a textual content-primarily based chat carrier. This will deliver a much better insight into the development of secure and privacy-keeping services, their charges and usability necessities, supplying and possibility to understand the underlying reasons why such offerings are no longer regularly occurring or widely adopted by the users.

IX. REFERENCES

[1] Ferri Fahrianto, Siti ummi Masruroh. "Encryption Application using Ceaser Cipher and Vigener Cipher", 2016.

[2] Robi Sanjaya, Abba Suganda Girsang. "Implementation Application Internal Chat Messenger Using Android System", 2017.

[3] G.B.Satrya, P.T.Daely d S.Y.Shin. "Android Forensics Analysis: Private Chat on Social Messenger", 2016.

[4] Michael Seufert, Tobias Hobfeld. "Group-Based Communication in WhatsApp", 2018.

[5] Rita Wonda, Houg I Jie. "Efficient Data Security For Mobile Instant Messenger", 2018.

[6] Mashael M.Alsulami, Arwa Y. Al-Aama. "Exploring user's Perception of Storage Management Features in Instant Messaging Applications": A Case on WhatsApp Messenger.