International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 07, July 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Developing an End-to-End Secure FOX Chat Application

Amar Singh[1], Amreesh Kumar Singh[2], Ankit Srivastva[3],

Vipin Bahadur Nishad[4], Sachidanand Chaturvedi (AP)[5]

1,2,3,4 B.Tech. Student, 5Assistant Professor in Computer Science & Engineering

Buddha Institute of Technology GIDA Gorakhpur

Abstract: *FOX is an Online Chat Application is utilized fundamentally for visiting reason with the distant customers or clients on Internet. Online Chat Application project in PHP, permit its clients to visit with their companion circles and send greeting to their different companions to join this talk framework. This Online Chat Application undertaking can likewise permit its clients to choose talk room according to their decision and visit with different people. At the point when begin talking, clients should initially enlist with this new framework and browse their email which has been utilized during enrolment measure. The sign in id and secret word will be sent by the administrator upon the confirmation of the clients It is persuaded from application like WhatsApp, Snap Chat, Telegram, WeChat and so on We thought to foster an application which have all highlights of these applications in on application so chose to make the turtle online visit application. There are a few works has been done on this sort of task like WhatsApp Telegram application has been made. The principal objective for fostering this venture is to a web-based media application for clients of comparable interest the application on will have talk between gatherings or people's messages. It can help for overseeing coordinated correspondence framework between companions, workers, family, clients and so forth.*

Keyword: *Application, Communication, Chat, social media, Verification.*

1. INTRODUCTION:

A web talk Application permits clients to impart progressively utilizing effectively open web interfaces. It's anything but a sort of Internet online visits recognized by straightforwardness and availability to clients don't wish to set aside the effort to introduce and figure out how to utilize particular talk programming. This quality permits client's moment access and just an internet browser is needed to visit. Clients will consistently get the most recent adaptation of a visit administration on the grounds that no product establishment or update is required. Web visit is text-based talk between individuals or chatbots conveyed over the web. Individuals can speak with one another or bots over web visit on the web. In contrast to the fundamental visit applications, like WhatsApp, Facebook, Messenger, Twitter and other social stages, a talk on the web doesn't need to be introduced as an application on a Smartphone to utilize. They don't have web forms be that as it may this isn't what Web talk ordinarily implies. Additionally, web talk is ordinarily between an organization and its clients, not between two individuals visiting for individual reasons. It explicitly addresses the requirement for organizations to have the option to convey to clients, specifically those clients who are on their site. Like clients use WhatsApp or Twitter for instance to speak with organizations.

Visit applications that will be fabricated is electronic and portable applications. This visit application is an application that is utilized to convey and created to help particularly the city of Bandung and the Indonesian public as a rule. In this visit application, constructed utilizing HTML, CSS, JS, jQuery, Bootstrap, PHP, MySQL.

2. Mobile Chat Applications

In this part, we momentarily present a considerable lot of famous talk applications in the versatile market as indicated by security and protection concerns. Sadly, some visit applications are not public or open source makes it hard for assessed by the designer's local area, security specialists or scientist scholarly.

2.1. Viber

Viber is a texting and Voice over IP (VoIP) application for cell phones created by Viber Media. Notwithstanding texting, clients can trade pictures, video and sound media messages. Viber as of late upheld the start to finish encryption to their administration, yet just for coordinated and bunch discussions in which all members are utilizing the most recent Viber adaptation 6.0 for Android, iOS or Windows 10. Right now, in the Viber iOS application for iPhone and iPad, connections, for example, pictures and recordings which are sent by means of the iOS Share Extension doesn't uphold start to finish encryption [6]. Viber has security issues, for example, adding a companion without his insight or adding him to a gathering without his authorization. Also that, nearby capacity isn't gotten. It's anything but open source making it hard to assessment.

2.2. WhatsApp

WhatsApp is perhaps the most mainstream informing application, as of late empowered start to finish encryption for its 1 billion clients across all stages. WhatsApp utilizes part of a security convention created by Open Whisper System, so gives a security-confirmation code that can impart to a contact to guarantee that the discussion is encoded [7]. It is hard to trust in WhatsApp application totally in light of the fact that the application isn't open source, making it hard to check the working interaction and match them with crafted by the encryption convention which was reported. 2.3 Telegram is an open source texting administration empowers clients to send messages, photographs, recordings, stickers and documents [8]. Wire gives two methods of informing is standard visit and mystery talk. Standard visit is clientserver dependent on cloud-based informing, it doesn't give start to finish encryption, stores all messages on its workers and synchronizes with all client gadgets [9]. More, neighborhood stockpiling isn't encoded of course. Secret visit is customer gives start to finish encryption. In spite of normal talk messages, messages that are sent in a mysterious visit must be gotten to on the gadget that has been started a mysterious talk and the gadget that has been acknowledged a mysterious talk they can't be gotten to on different gadgets. Messages sent inside secret visits can be erased whenever and can alternatively fall to pieces [8]. Message utilizes its own cryptographic convention MTProto, and has been reprimanded by a huge piece of the cryptographic local area about its security[9]. The enlistment cycle of Telegram, Viber and WhatsApp rely upon SMS. SMS is shipped through Signaling System 7 (SS7) convention. The weakness lies in SS7 [10]. Assailants abused SS7 convention to login into casualty's record by blocking

SMS messages [11]. Due to Telegram cloud-based, the aggressor misuses it and makes full control of the casualty account and can forestall him to go into his record. To make the record safer ought to enact two-factor verification [12]. 2.4 Facebook Messenger Facebook Messenger is a well known informing administration accessible for Android and iOS. It gives two methods of informing is customary talk and mystery discussions. Normal visit doesn't give start to finish encryption just secure correspondence by utilizing TLS, and it stores all messages on its workers. Secret discussions have a similar thought of Telegram secret talk [13].

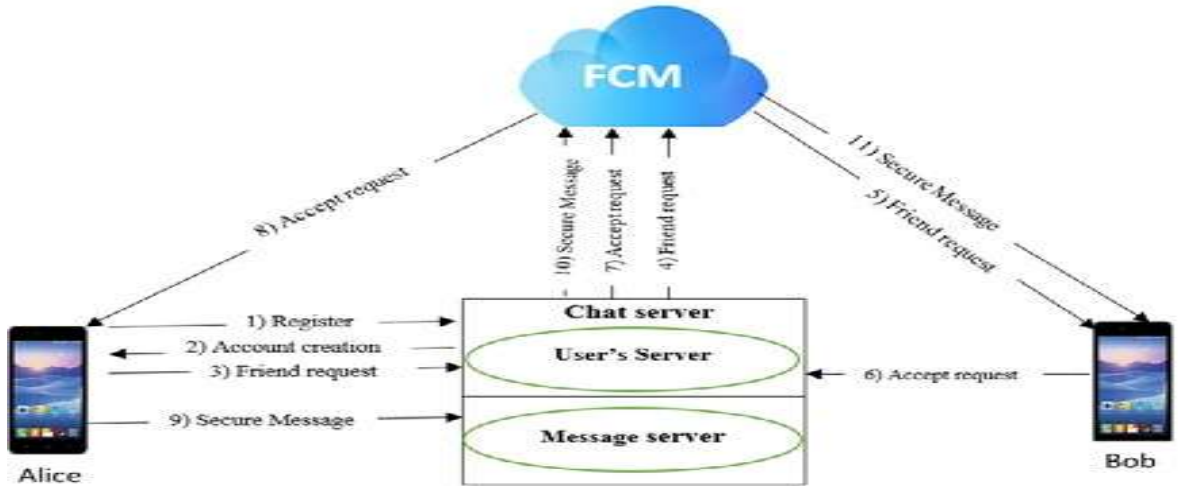
3. Proposed architecture

3.1 Secure Mobile Chat Requirements

In this part, we propose a bunch of prerequisites to make secure talk application: req1: Password put away on the visit worker ought to be scrambled. req2: Providing either secure meeting or TLS. Secure meeting is a novel key for every meeting. Guarantees that correspondence is with the opportune individual and no man-in the-center can peruse the messages. req3: Messages should be scrambled to keep up with security and protection. req4: Local stockpiling should be ensured by encryption. req5: Messages are not put away on the visit worker yet put away on the client's gadget. req6: It isn't permitted to trade messages in the event that they are not companions.

3.2 Proposed Architecture

The proposed engineering is intended to be Client-Server talk application. In customer side, when a client sets up the application, the client either chooses enlistment or sign in. In worker side, the visit worker comprises of clients' worker and a message worker. Client's worker that deals with client's qualifications. Message worker handles messages between clients by utilizing Firebase Cloud Messaging (FCM).If the beneficiary is disconnected, the messages will be put away briefly on the FCM line for a particular timeframe, and when beneficiary becomes online these messages are sent to him then, at that point erased from the line. The nonexclusive engineering is displayed in Fig. 1



3.3 Registration an account

Prior to beginning the application, there should have a lock screen to design the Keystore that gives a safe holder to store the neighborhood stockpiling key to make more hard for extraction it from the gadget by

unapproved people or different applications [14].

Each record has just a single gadget and it is recognized by gadget id. Also, Email and username are remarkable. Name, email and secret phrase are needed to enlist another record. In the wake of composing the enlistment data, the secret phrase is encoded by utilizing XSalsa20 calculation [15]then the client accreditations are shipped off the worker. After confirmation, the worker creates a remarkable identifier that goes about as the client ID. From that point onward, the affirmation message is gotten for effective enlistment to the customer application and the customer data is put away in neighborhood stockpiling.

The application generates a set of keys:

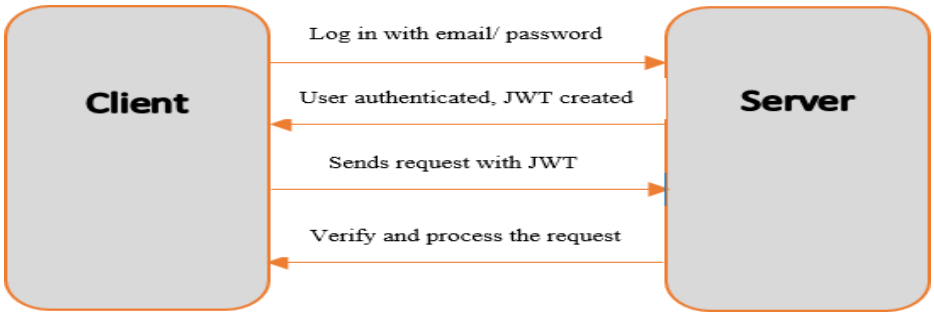
(a) Key for encrypting the password.

(b) A public key pair for calculating session key.

(c) Symmetric storage key for encrypting/decrypting localstorage contains contact list, chat history and key store.

3.4 Login

Email and secret key are needed for client validation. In the wake of composing the confirmation data, the secret word is encoded then the client qualifications are shipped off the worker. The worker browses if the email and secret phrase are substantial. After approval, JSON Web Token (JWT)[16] is made and ships off the customer to store it. At the point when a customer makes a solicitation at the later time, JWT is passed with the solicitation. The worker checks of the JWT, on the off chance that it is legitimate, the solicitation is prepared (Fig.2).



3.5 Firebase Cloud Messaging

Firebase Cloud Messaging (FCM) is an assistance that works with informing between versatile applications and worker applications. It's based on Google Play Services that supports cross-stage (iOS, Android and Web). It's anything but a free assistance that permits sending lightweight messages from the worker to the gadgets at whatever point there is new information available[17]. This saves a ton of client's battery by trying not to demand to the worker for new messages. It gives TLS to getting channel.

At the beginning of running the application for the first time gets the following:

(1) The application connects to FCM server and registers itself.

(2) When successful registration, FCM provides registration token to the device. This registration token uniquely identifies each device.

(3) The application sends the registration token to theserver to store it in MongoDB database.

The above steps are shown in Fig. 3.

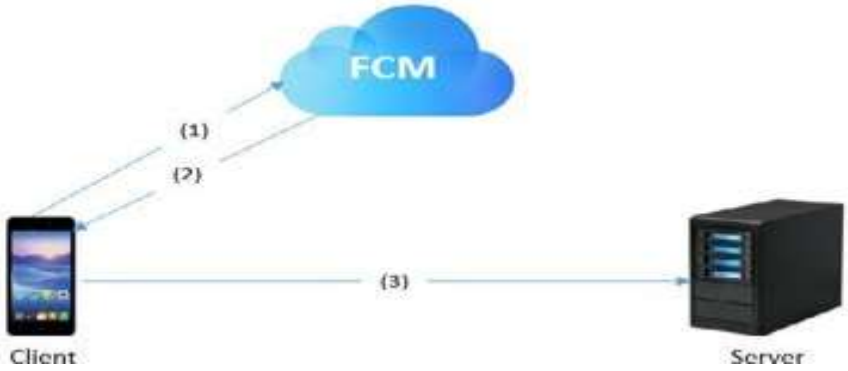


Fig. 3. Firebase Cloud Messaging.

FCM identifies the target device byusing registration token then starts to push data.

3.6 Session key Setup

To add users to contact list either by username or by emailaddress.

For sending a solicitation to a companion with the understanding that the main client knows the username or email of the subsequent client due to the username and email are an interesting for every client and the subsequent client ought to have effectively enlisted in the worker. Probably, the principal client is called Alice and the second is called Bob.

When the send demand, Bob name is composed by Alice and her public key is gotten from the nearby stockpiling then the solicitation is shipped off the worker.

At the point when a solicitation is gotten, it's anything but a warning (Fig. 4). On the off chance that the companionship demand is acknowledged by Bob, his private key is brought with Alice's public key to ascertain the meeting key by utilizing Elliptic Curve Diffie-Hellman (ECDH) over the bend Curve25519 [18] and hashes the outcome with HSalsa20 [15] then the meeting key is put away in neighborhood stockpiling (Fig. 5). Eventually, the acknowledgment is sent with his public key to the worker to be conveyed to Alice. Endless supply of the acknowledgment of the solicitation, similar strides on the above are taken. The meeting key is determined by utilizing Alice private key and Bob public key then it is put away in the neighborhood stockpiling for sometime in the future.

The meeting key is something similar for the two players and this is the strength of the Elliptic Curve Diffie-Hellman (ECDH) and hence it is hard to assault by the man-in-the-center. Notwithstanding, the shortcoming of the customary Diffie-Hellman has been disposed of.

International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 07, July 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

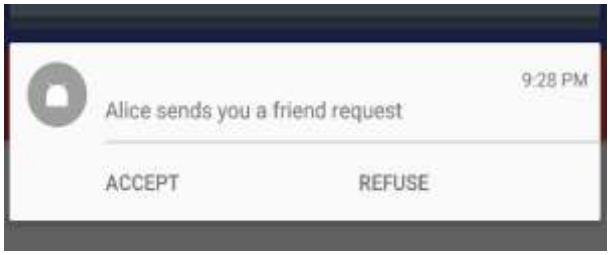


Fig. 4. Friend request notification

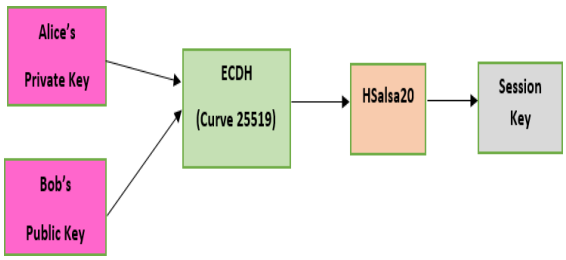


Fig. 5. Session key Setup

3.7 Exchanging Messages

At the point when a message is composed, the application encodes the message utilizing XSalsa20 encryption calculation to scramble the message body and Poly1305 to figure a Message Authentication Code (MAC) [19]. Each message has its own different key and nonce which brings better security for each single message in such finding one of the keys can't unscramble past messages. In the wake of scrambling the message, it is encoded again utilizing the beneficiary's meeting key then it is shipped off the worker (Fig. 6).

After the message is gotten from FCM, the MAC of the encoded message is determined and contrasts it and the got MAC to confirm the honesty of the message. On the off chance that the outcomes are not the equivalent, it is dismissed and doesn't show to the client else it is decoded by the sender meeting key. Then, the message body is checked in similar strides above. Presently the key and nonce to unscramble the message are known. The message is then unscrambled and put away in the neighborhood stockpiling and showed to the beneficiary.

On the off chance that the application is behind the scenes the message will be shown as a notice while if the beneficiary uses the application it will be shown in the visit window.

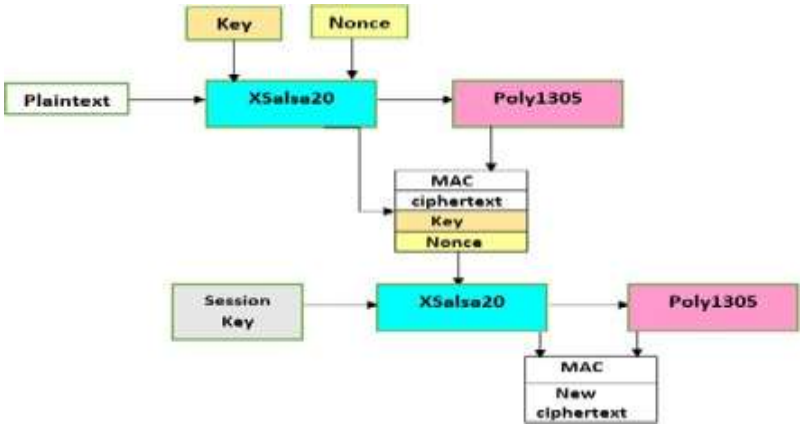


Fig. 6. Procedure to encrypt a message.

3.8 Local Storage

The information is put away locally in the application by utilizing Realm data set. Domain is a lightweight portable information base that supports cross-stage. It's not difficult to utilize and quick. More, it has heaps of current highlights like JavaScript Object Notation (JSON) support, a familiar API, information change warnings and encryption support [20]. Scrambled information is shielded from unapproved access and is open just if have been a right encryption key. Domain utilizes AES-256+SHA2 calculation and 64-byte

key for scrambling stockpiling [21]. To get ready Realm stockpiling goes through a few stages that are:

Step 1: The application checks whether the lock screen is present or not. If it exists, the following steps are completed.

Step 2: Generate Realm Key that is used for encrypting storage.

Step 3: Generate key from Keystore.

Step 4: Realm key is encrypted with the key generated in step 3 by using AES in CBC mode.

Step 5: Save the encrypted key in shared preferences in private mode so that other applications cannot access this data directory.

Three files are stored in the local storage. UserInfo file that stores all information pertaining to the user. While Friends file stores all information pertaining to the friends. Finally, Messages file stores all information pertaining to messages.

3.9 Server-Side Implementation

Worker side has depended on Node JS[22] and MongoDB database[23]. Hub JS is quick, equipped for taking care of countless synchronous associations with high throughput, which is comparable to high adaptability. MongoDB and Node JS have frequently utilized together on account of their utilizing JSON so no compelling reason to invest energy for changing the information between them making it simple to manage one another. Also, MongoDB gives TLS that makes a safe association (Fig. 7).

To perform a client request passes through several steps that are:

Step 1: Initially, must run the MongoDB connection then run the Node JS from Command Prompt. At this stage, theserver is ready to receive the client's request.

Step 2: When the client sends a request, the server receives the HTTP request in JSON format. The request then parsed.

Step 3: The HTTP request is compared with the base path if it is matched, it is handed to Express framework.

Step 4: The Express receives the HTTP request and routes it to the specific endpoint that matched it. In case of not matched with any of the routes will display error in Command Prompt. Otherwise, it will be forwarded to the controller which handles the required function.

Step 5: Make a request to MongoDB database by mongoose for processing function.

Step 6: When the data is fetched from MongoDB databaseand the required operations are done, Node JS receives theresponse then sends to the client.

The above steps are shown in Fig. 8.

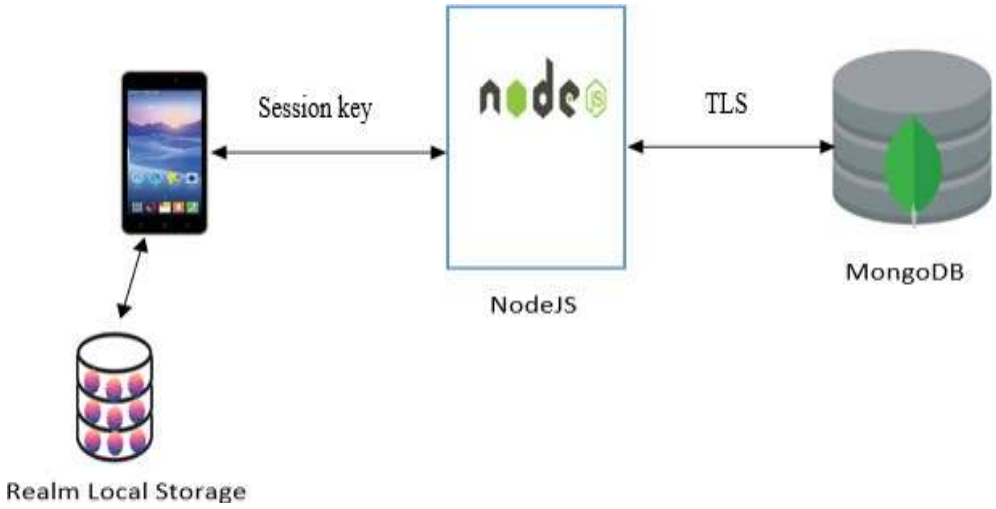


Fig. 7. The Specific Architecture of Proposed Chat.

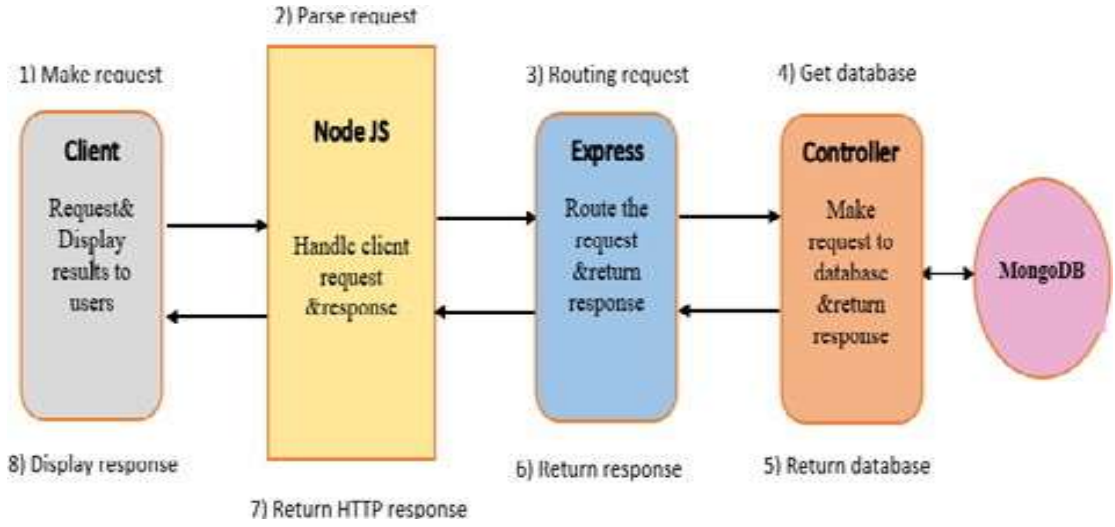


Fig. 8. Implementation of a client request.

4. METHODOLOGY:

The overall project would be divided into six phases:

First Phase: The start of the project will be deal with creating the front-end design or blue print of the web chat application.

Second Phase: The next phase will be to implement the programming part. HTML, CSS and JS is used create the front-end design of the application.

Third Phase: The next phase will deal with the making of back-end which is also known as the server side programming.

Fourth Phase: In this phase, the main aim would be creation & manipulation of the database.

Fifth Phase: In this phase, the overall system is to be examined and verified for any errors. The system would be

running on localhost.

Sixth Phase: In this the last phase of the project, the project which is running on localhost will be deployed on the server.

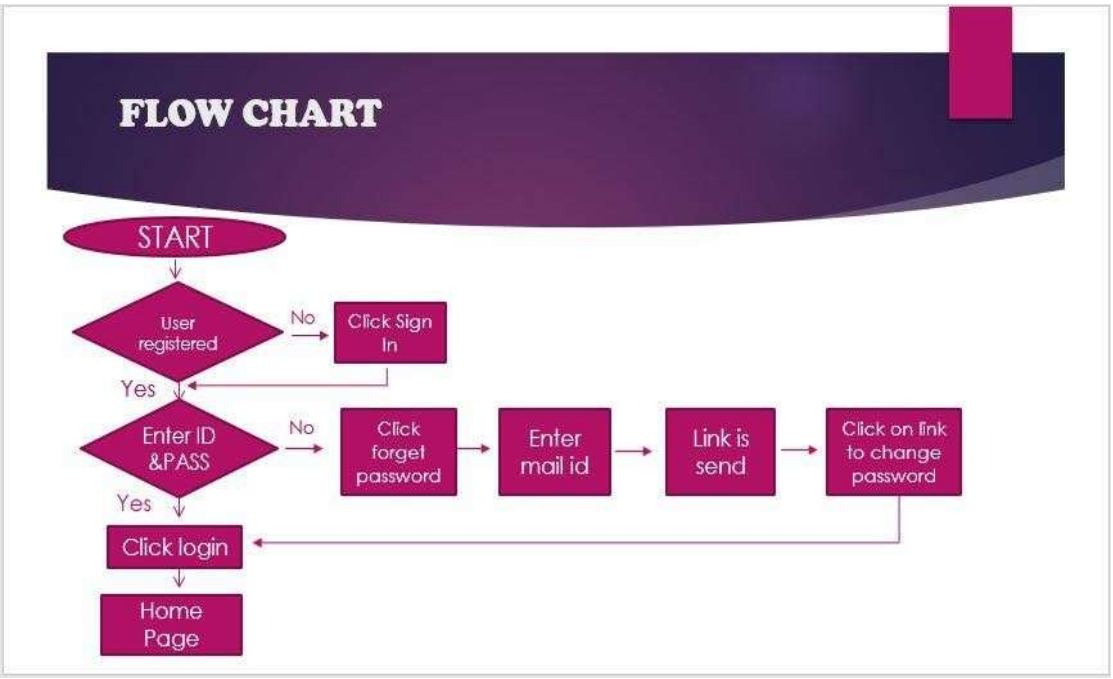


Fig. 2 User interface design of web-based chat application

The explanation for each flow from picture above is as follow:

1. When the main page is accessed by user it will show the login page first, instead of show the main page directly. User login credentials is required. If the user doesn't have an account yet, then they must register first.
2. After login, user must have friend before they can start a chat. Therefore, if user has no friend yet, they can find them directly from the application. Afterwards, user can add friend to their friend list, and waiting for friend request confirmation.
3. However, if user has friends in their friend list, then they can immediately start a chat.
4. Next step, the system will check if user has a chatroom with another user selected. If has not, then system will create the chatroom and if they already have a chatroom,they will enter that chatroom to start chat.

5. Finally, data will be sent and received.

5.Analysis the Proposed Chat

In section 3, we listed a set of requirements for securing chat. To analyze and evaluate proposed chat we have

compared proposed chat with popular applications discussed in section 2. The comparison is based on the requirements listed in Table 1.

Table 1. Comparison with Popular Chat Applications

Criteria	WhatsApp	Viber	Telegram	Facebook Messenger	Proposed Chat
Req1	N	N	N	N	Y
Req2	Y	Y	Y	Y	Y
Req3	Y	Y	P	P	Y
Req4	Y	N	N	P	Y
Req5	Y	Y	N	N	Y
Req6	N	N	N	N	Y

Note:"Y" it means that it meets the requirement. "N"does not support the requirement. "P"only the secret part supports it.

6.Conclusion

In this paper, we presented a particular for saving the security and protection of the visit application. We depicted a bunch of prerequisites for making secure talk and carry out it by utilizing current techniques and lightweight for giving pace and great assurance to its customers. XSalsa20 calculation ideal for cell phones in light of its high security, superior and keeps up with battery life. Customers can be sure that no one can peruse their messages, regardless of whether the cell phone arrives at wrong hands can't enter to the application and can't get to the information put away locally.

7. References

[1] Ash Read, "How Messaging Apps Are Changing SocialMedia," 2016. [Online]. Available: https://blog.bufferapp.com/messaging-apps.

[2] Most popular messaging apps 2017 | Statista," 2017. [Online]. Available: https://www.statista.com/statistics/258749/most-popular- global-mobile-messenger-apps/.

[3] D. Moltchanov, "Client/server and peer-to-peer models: basic concepts," 2013.

[4] Martin Kleppmann, "The Investigatory Powers Bill would increase cybercrime — Martin Kleppmann's blog," 2015. [Online].Available: https://martin.kleppmann.com/2015/11/10/investigatory- powers-bill.html.

[5] D. P. Roel Hartman, Christian Rokitta, Oracle Application Express for Mobile Web Applications - Roel Hartman, Christian Rokitta, David Peake - Google Books. 2013.

[6] Viber Encryption Overview." [Online]. Available: https://www.viber.com/security-overview/.

[7] WhatsApp inc, "WhatsApp security whitepaper," p. 10, 2017.

[8] "Telegram F.A.Q."[Online]. Available:https://telegram.org/faq. T. Susanka, "Security Analysis of the Telegram IM," p. 70, 2016.

[9] B. O. B. Kamwendo, "Vulnerabilities of signaling system number 7 (ss7) to cyber attacks and how to mitigate against these vulnerabilities. bob kamwendo," vol. 7, no. 7, 2015.

[10] John Leyden, "SS7 spookery on the cheap allows hackers toimpersonate mobile chat subscribers • The Register," 2016. [Online].Available:
https://www.theregister.co.uk/2016/05/10/ss7_mobile_chat_ hack/.

[11] "Active Sessions and Two-Step Verification." [Online]. Available: https://telegram.org/blog/sessions-and-2-step-verification.

[12] T. Whitepaper, "Messenger Secret Conversations," 2016.

[13] "Android Keystore System | Android Developers." [Online].Available: https://developer.android.com/training/articles/keystore.htm l.

[14] D. J. Bernstein, "Extending the Salsa20 nonce," no. Mc 152,pp. 1–14, 2011.

[15] M. B. Jones, "The Emerging JSON-Based Identity ProtocolSuite," 2011.

[16] "Firebase Cloud Messaging | Firebase." [Online]. Available:https://firebase.google.com/docs/cloud-messaging/.

[17] D. J. Bernstein, "Curve25519 : new Diffie-Hellman speedrecords," vol. 25519, 2006.

[18] D. J. Bernstein., "Poly1305." [Online]. Available:https://en.wikipedia.org/wiki/Poly1305.

[19] "Realm: Create reactive mobile apps in a fraction of thetime." [Online]. Available: https://realm.io/.

[20] "Realm Swift 2.10.2." [Online]. Available:https://realm.io/docs/swift/latest/.

[21] "Node.js." [Online]. Available: https://nodejs.org/en/.

[22] "NoSQL Databases ExplainedMongoDB." [Online].Available: https://www.mongodb.com/nosql-explained.

[23] "NoSQL Databases Explained | MongoDB." [Online].Available: https://www.mongodb.com/nosql-explained.