International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# BlinkBuzz-The Messenger Application using SHA-256 with RSA Algorithm

*Mr. Dhananjay Shravan Aher*[1]*, Mr. Pratham Ganesh Kotkar*[2]*, Mr. Gaurav Mahendra Vadnere*[3]*, Miss. Komal Keshav Walke*[4]*, Prof. A.S. Gaikwad*[5]

[1,2,3,4] UG Student, Department of Computer Engineering, LOGMIEER, Nashik
[5]Guided, Department of Computer Engineering LOGMIEER, Nashik
[1]aherd2002@gmail.com, [2]prathamkotkar111@gmail.com, [3]gauravvadnere789@gmail.com, [4]komalwalke1620@gmail.com, archanagaikwad17@gmail.com[5]

**ABSTRACT:**

In an era dominated by digital connectivity, thedemand for secure, user-friendly, and feature rich messenger applications Is at an all-time high. This abstract introduces a cutting-edge messenger application designed to meet the evolving communication needs of user worldwide. Our messenger application, stands out with its emphasis on robust security, seamless user experience, and innovative features. Security isparamount, and end-to-end encryption ensures that user conversations remain private and protected from unauthorized access. The application employs state-of-the-art encryption algorithms to safeguard user data, giving users confidence in the confidentiality of their communication. Userexperience is a key focus, and the interface is intuitively designed for effortless navigation. A minimalist yet functional design approach ensures that users can easily access a plethora of features without compromising simplicity. The application supports multimedia sharing, voice and video calls, and real-time location sharing, enriching the communication experience.

**Keywords: Instant Messaging, Voice and Video Calls, Status Updates, User Profiles, Integration with Social Media, QR Codes.**

## 1. INTRODUCTION

### *1.1 Motivation –*

**Instant Communication**: Acceleration of Communication: The primary motivation is to provide users with a platform for instant and real- time communication. The goal is to reduce communication barriers and enable people to connect instantly, regardless of geographical distances.

**Global Connectivity**: Breaking Down Borders: Real-time messenger apps aim to break down geographical barriers, allowing users tocommunicate seamlessly with friends, family, and colleagues around the world. This fosters a sense of global connectivity.

**Multimedia Rich Communication:** Diverse Expression: Enabling users to share not only text butalso multimedia content like photos, videos, and voice messages enriches the communication experience. The motivation is to provide users with diverse and expressive means of communication.

**User-Friendly Interface:** Accessible Technology: Real-time messenger apps strive to create user- friendly interfaces that are easy to navigate. This motivation ensures that people of all ages and technical backgrounds can comfortably use the app for communication.

**Innovation in Features:** Continuous Improvement: To stay competitive and relevant, messenger apps are motivated to introduce new and innovative. features. This could include functionalities like voice and video calls, group chats, status updates, and more, enhancing the overall user experience.

**Privacy and Security:** User Trust: Ensuring user privacy and security is a crucial motivation. By implementing features like end-to-end encryption, messenger apps aim to build trust among users, assuring them that their communication is secure and private.

**Adaptation to Changing Needs:** Dynamic UserNeeds: The motivation to adapt and evolve is drivenby changing user needs and technological advancements. Messenger apps continuously update their features to meet the dynamic expectations of users in a rapidly evolving digital landscape.

**Business and Productivity:** Professional Communication: Real-time messenger apps are motivated to cater to the communication needs of businesses and professionals. This includes features like document sharing, collaboration tools, and integration with other productivity apps.

**Customer Engagement:** Enhancing Customer Experience: For businesses, messenger apps serve asa tool for engaging with customers in real time. Thismotivation aligns with the goal of providing excellent customer service and support.

### *1.2 Problem Definition:*

Users across the digital landscape seek an advanced messaging application that goes beyond basic communication. The existing solutions often face challenges, prompting the development of Unified Chat. The identified problems are:

**Privacy and Security:** Current messaging appslack robust end-to-end encryption, leaving user data vulnerable to unauthorizedaccess.

**Limited Multimedia Interaction:** The absence of comprehensive multimedia features restricts users from expressing themselves beyond text messages. **Real-Time Communication Gaps**: Reliable voice and video calling functionalities are not uniformly available, hindering seamless real-time interactions.

**User Interface Complexity: e**xisting interfaces lack universal appeal and intuitive design, posing challenge forusers with varying technical backgrounds.

**Notification Latency:** Current notification systems are not consistently responsive, leading to delays in updating users about new messages or app updates.

**Lack of Personalization:** Current messaging apps offer limited customization options, failing to meetthe diverse preferences of users. **Scalability and Performance Issues:** The existing backend infrastructures struggle to scale with a growing user base, resulting in compromised app performance and responsiveness.

## 2. SYSTEM ARCHITECTURE

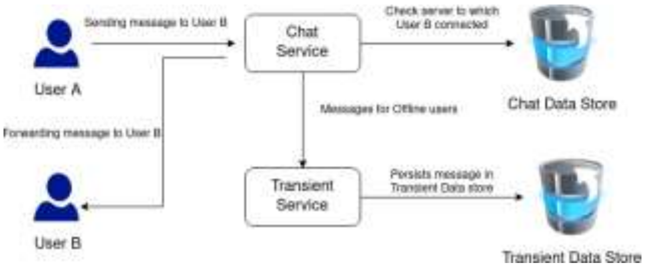

Sending message to User B
Chat Service
Check server to which User B connected
Chat Data Store
User A
Messages for Offline users
Forwarding message to User B
Transient Service
Persists message in Transient Data store
User B
Transient Data Store

Figure 3.1: System Architecture

## 3. SURVEY ON ALGORITHM

We are using SHA256 AND SHA256 with RSA. SHA-256 stands for Secure Hash Algorithm 256- bit and it's used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash.

SHA256 with RSA is a hybrid cryptographic algorithm that leverages the SHA-256 hashing algorithm and the RSA digital signature scheme. It sutilizes SHA-256 to generate a hash value for the data and then signs the hash using RSA with a private key. [4]

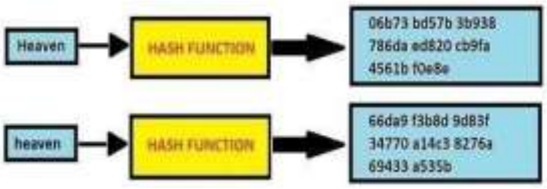
**SHA-256:**

You can divide the complete process into five different segments,

Step 1 — Initialize Hash Values (h) Now we create8 hash values

Step 2 — Padding Bits Step 3 — Padding Length

Step 4 — Initializing the Buffers Step 5 — Compression FunctionsStep 6 — Modify Final Values Step 7 — Concatenate Final Hash.



## 4. PROPOSED IDEA

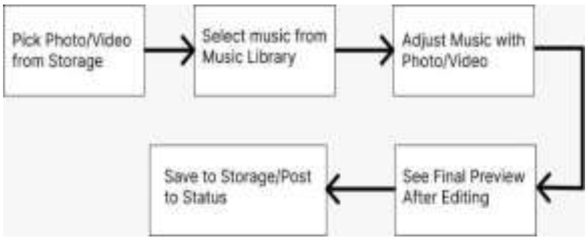
- Adding a Music from Music Library at the time of Upload.
- Downloading Status of Another Contact using Permission Manager.
- Chat Screenshot Taking with Permission Manager.

- Photo Quality selection using Slider when

Sending Message.

- Pin Important Messages in Chat.

### *4.1.1 Music Adding to Status while Uploading*

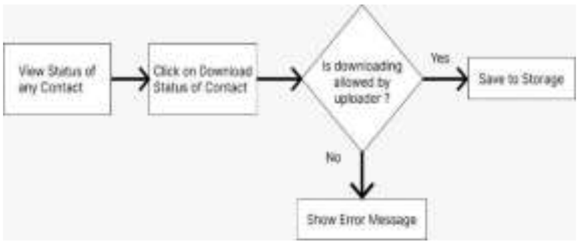

Pick Photo/Video from Storage
Select music from Music Library
Adjust Music with Photo/Video
See Final Preview After Editing
Save to Storage/Post to Status

**Enhanced Expression:** Users can express their thoughts and emotions more creatively by pairinga song with their status.

**Engagement:** Adding music can increase engagement and interaction with other users, as music is a universal language that resonates with many.

**Personalization:** Allows users to share a bit of their musical taste and personality with their contacts

### *4.1.2 Downloading Status of Contact using Permission Manager*

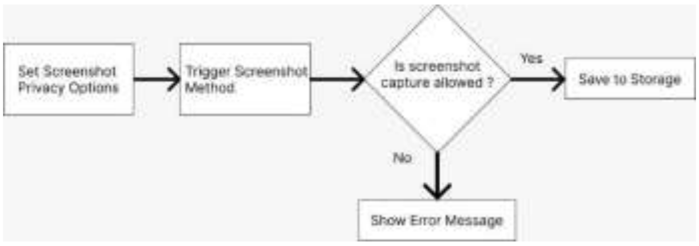

View Status of any Contact
Click on Download Status of Contact
Is downloading allowed by uploader ?
Yes
Save to Storage
No
Show Error Message

with system using keys. checks the userthrough the private key and updates thedatabase with the time , which is the time given to the user to interact with the system. After login the user they can setup the profile, then user can directly go to Main Activity in that main activity there are different fragments they are chat fragments, call fragments, profile fragments and status fragments.

**Offline Viewing:** Allows users to view their contacts' statuses even whenthey are not connected to the internet.

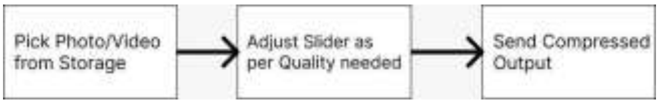
**Sharing:** Users can share downloaded status with others who might not have seenthem.

### *4.1.3 Chat Screenshot Taking using Permission Manager*


Set Screenshot Privacy Options
Trigger Screenshot Method
Is screenshot capture allowed ?
Yes
Save to Storage
No
Show Error Message

**Personal Record:** Helps users maintain a personal record of chats they consider valuable.

### *4.1.4. Photo Quality Selection usingSlider while Sending Message*

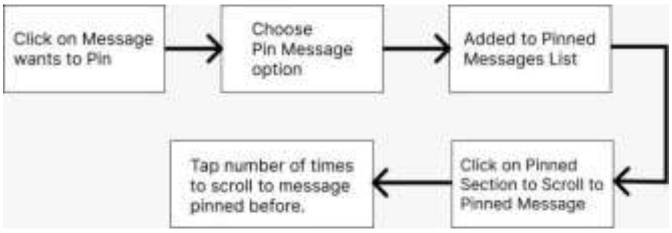

Pick Photo/Video from Storage
Adjust Slider as per Quality needed
Send Compressed Output

**Personal Record:** Reduced Data Usage: Smallerimage sizes reduce the amount of data required tosend and receive images, especially on slower connections.

**Faster Sharing:** Smaller images are quicker to upload and download, improving the overall userexperience**.**

**Storage Conservation:** Smaller images consumeless storage space on users' devices.

### *4.1.5 Pin Important Messages in Chat*


Click on Message wants to Pin
Choose Pin Message option
Added to Pinned Messages List
Click on Pinned Section to Scroll to Pinned Message
Tap number of times to scroll to message pinned before.

**Visibility:** Pinned messages remain at the top of the chat, ensuring that important information is easily accessible. **Organization:** Helps group members quickly find crucial messages in a busy chat.

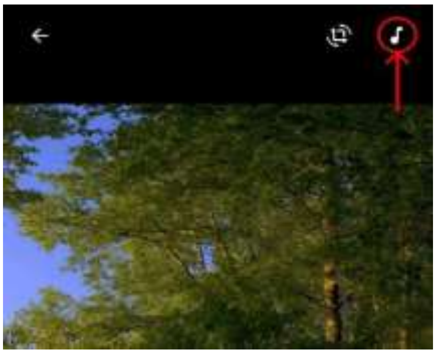
**Context:** Pinned messages can provide context for on going discussions, especially in large groups.

**Announcements:** Useful for making important announcements or sharing critical updates with group members.

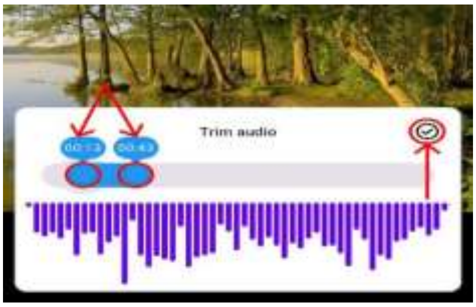
## 5. RESULT / OUTPUT OF MODULES

### *5.1 Adding Music from Phone Music Library.*

1. Click Music Icon located at top right corner.



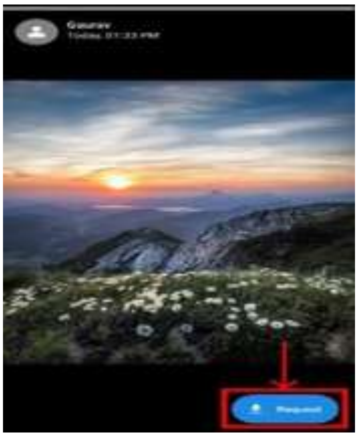
2. Drag the start and end points of range slider to match the desired output (Max duration 30seconds).
3. After you get desired output, click the check icon. 4.After complete transformation, you can send it to status.

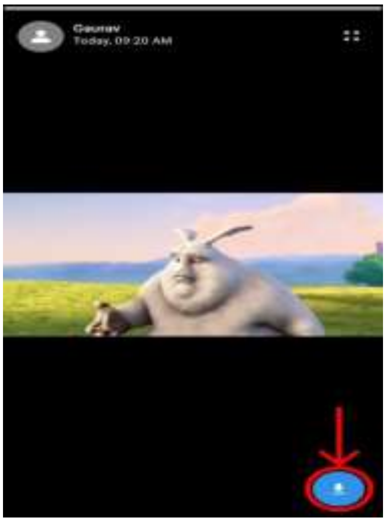


### *5.2 Downloading Status :-*

1. While viewing status, check for download button at bottom if it is showing Request label then click the label to send the status download request to status uploader Or If user gets the Download Button instead of Request then user can download status as per Step 3.

2. Then if uploader approves the request for download, the downloader needs to restart the app to see download button.
3. Then when user clicks on download button the user needs to grant Storage Permission, if not already granted. After permission grant the status will be downloaded.

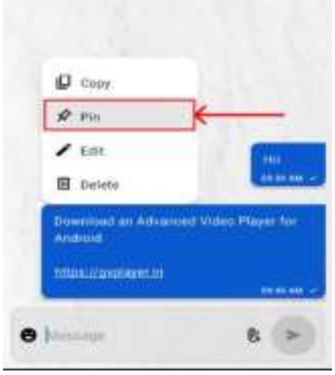




### *5.3 Pin Message in Chat :-*

1.Click the message want to pin. 2.In shown menu, click Pin option.

3.The message will be pinned and added to pinned messages bar which will be displayed at top below toolbar.



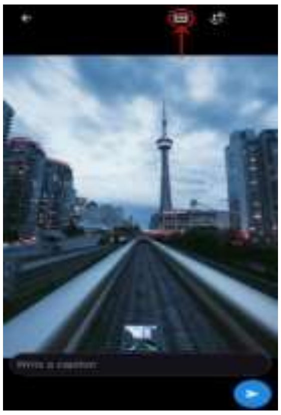
Hi!

Download an Advanced Video Player for Android

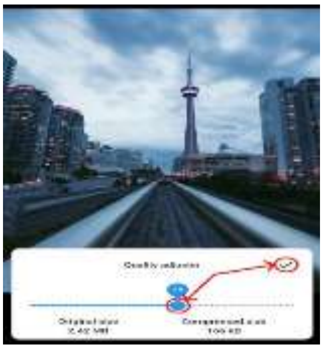
https://gxplayer.in

### *5.4 Image Quality Selection using Slider :-*

1. In chat, pick the media you want to send, after selection click the HD icon located at the top.



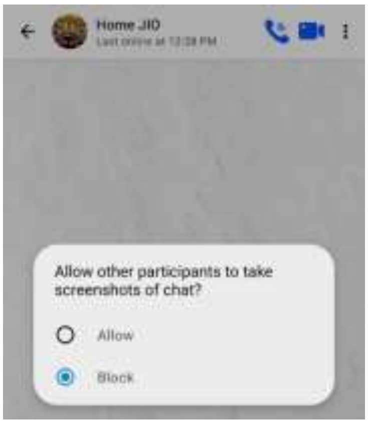
2. After clicking the HD icon, it will open the Quality Adjustment Page.



3. You can drag the slider and check the actual size and compressed size after dragging a slider.
4. After you desired file size, click the Check icon to send the desired file.

### *5.5 Screenshot prevention using Permission Manager within One-to-one chat :-*

1. Open chat where you want to enable/disable screenshot capturing by another user.
2. Click on three dots at top right.
3. Click on Screenshot privacy option.
4. The dialog box will show to either Allow or Block (Default value: Block).
5. If another person of chat captured a screenshot and you blocked them then it will show error message as “this app doesn't allow taking screenshots”.



Allow other participants to take screenshots of chat?

○ Allow

● Block

## 6. CONCLUSION

In this paper a study different features is proposed. The content of this paper are studied from variety of sources and also we have introduced our contribution in this system. The main intention of this application is to introduced new features of whatsapp .In this project, we have successfully designed and implemented an instant messaging application that replicates the core functionalities of WhatsApp while introducing two significant additional features: the ability to add music to user statuses and the capability to download statuses shared by other users. This effort involved extensive software development and testing to ensure a seamless user experience.

## 7. **REFERENCES**

[1] Sanskar Shukla Student,SCSE,Galgotias University Greater Noida,India,”Android Based Chat Application Using Firebase”,2021 International Conference on Computer Communication Informatics(ICCCI- 2021),jan27-29,2021 Combatore, INDIA Rick Cents Politie Nederland Dutch Police Utrecht,The Netherlands,2020,”Towards A NEW Apporach To Identify WHatsapp MEssages”,2020 IEEE 19th International Conference on Trust,Security Privacy in computing Communication (TrustCom)

[2] Zhi-Hui Wang School of Software Dalian University ofTechnology Dalian, Liaon-ing, China, 2009,”Emoticon-based Text Steganography in Chat”,2009 Second Asia- Pacific Conference on Computational Intelligence and Industrial Applications .

[3] Royal Kaushal Raman ChadhaDepartment of Computer Science and Engineering Chandigarh University Mohali,India march 2023,”A Survey of Various Sentiment Analysis Techniques of Whatsapp”,2023 2nd International Conference for Innovation in Technology (INOCON) Bangalore, India.

[4] Noveline Aziz Fauziah Department of Informatics Engineering Dian Nuswantoro University Semarang, Indonesia,2018”Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application”,2018 International Seminar on Research Technology Intelligent System(ISRRTI)

[5] Khushboo Rathi, Umit Karabiyik Department of Computer Science Sam Houston State University Huntsville, Texas,2017,”Forensic Analysis of Encrypted Instant Messaging Applications on Android”

[6] Isil Karabey Department of Computer Hacettepe University Ankara, Turkey,2016,”A Cryptographic Approach for Secure Client - Server Chat Application using Public Key Infrastructure (PKI)”,The 11th International Conference for Internet Technology and Secured Transactions (ICITST- 2016) .

[7] Taishi Nemoto Graduate School of Information Sciences and Arts Toyo University Tokyo, Japan,2019, ”The Seamless Communication Mechanism both for Individuals and Groups” ,2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)

[8] Rick Cents Politie Nederland Dutch PoliceUtrecht,The netherlands,2020,”Towards A NEW Apporach To Identify WHatsapp MEssages”,2020 IEEE 19th International Conference on Trust,Security Privacy in computing Communication.