

Privacy Focused Messenger

Rakesh.B¹, Lakshman Kumar M²

^{1,2}Dept of Computer Science Engineering

^{1,2}Panimalar Engineering college

Abstract- One of the most important pieces of technology in our generation is messaging. The drawback with modern messengers is that users need a phone number tied to their name and which has their personal information. Our application targets users who cannot carry their personal phone with them at all time or if their battery died and they are in an emergency situation and need to contact their family and friends they cannot use their account since they need their number and one-time password. Our application tackles the problem by using a simple login method such as email and password so users can login to their accounts at any time and wherever they want.

Keywords- Messenger,privacy

I. INTRODUCTION

Messaging and texting are among the most popular methods of communication among children and teenagers. Messaging and texting can be much more than ways to communicate. They can also be tools that help young people learn and master important skills.

Online messaging apps are often used by young people to talk to their friend and peers. Staying connected with your friends is valuable, but online messaging also gives young people opportunities to develop their social skills in a range of formal and informal contexts.

Online messaging can help young people to:

- appreciate different perspectives
- understand the difference between appropriate and inappropriate behavior
- become more effective non-verbal communicators.

Privacy focused Messenger does not collect any. Adversaries cannot learn who is conversing with whom, or if anyone is conversing at all. Relationship unobservability does not exist in consumer-grade messengers.

II. LITERATURE SURVEY

Data privacy is not in the interest of the app providers because there is a lucrative financial benefit to be made by the use of your privacy.

III. EXISTING SYSTEM

Encryption in messenger apps does not always mean that metadata of the communication is protected. Anyone capable of tapping into the communication can theoretically gain access to collected metadata such as the timing of the conversation, who is chatting with whom, the conversations' traffic volumes and the identities of the devices. Metadata is sometimes just as important as the sensitive content of the messages.

IV. PROPOSED SYSTEM

The drawback with modern messengers is that users need a phone number tied to their name and which has their personal information. Our application targets users who cannot carry their personal phone with them at all time or if their battery died and they are in an emergency situation and need to contact their family and friends they cannot use their account since they need their number and one-time password. Our application tackles the problem by using a simple login method such as email and password so users can login to their accounts at any time and wherever they want.

V. IMPROVEMENT AS PER REVIEWER

COMMENTS

HAVE YOU READ ANY PRIVACY POLICY FOR MESSENGER APPLICATIONS?

one actually attempts to read the privacy policy of any given app, the digital advertising company third parties that receive your detailed profile are often not mentioned by name. If the third parties are actually listed, and there are typically hundreds of them, the user then has to read the privacy policies of these third parties to understand how the data is being used.

1. Implementation of video call functionality.
2. Adding video files to messages.
3. Adding GIFs support
4. adding file attachments
5. adding image attachments

VI. CONCLUSION

We have successfully designed a PRIVACY FOCUSED MESSENGER. Our group messenger is controlled entirely by the users and with a little technical knowledge users can add their own server for their community group text. We believe that privacy is a basic human right which should be respected by everyone. We as people need privacy and it is a basic constitutional right that every human should have. Many companies and organizations including private and government organizations spy on their users in the name of national security. Let us encourage free and open-source projects where the users can view the source code and everything is free from telemetry.

REFERENCES

- [1] Android studio documentation, google, <https://developer.android.com/docs>
- [2] Flutter documentation, google, <https://flutter.dev/docs>
- [3] Firebase documentation, google, <https://firebase.google.com/docs>
- [4] xcode developer documentation, apple, <https://developer.apple.com/documentation/xcode/>