e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

REVOLUTION IN CHAT APPLICATIONS: PROVIDING ENCRYPTION FOR CHAT BACKUPS

Ratik Tiwari*1, Azhar Ahmed*2

*1Student, Department of Computer Science and Engineering, HMR Institute of Technology and Management, Delhi, India.

*2Professor, Department of Computer Science and Engineering, HMR Institute of Technology and Management, Delhi, India.

ABSTRACT

WhatsApp, Telegram, Signal, and other social media services are currently widely used from diverse circles due to their ease of use and extensive features. Security, when talking from the point of view of using WhatsApp and other applications is also very crucial at this time. WhatsApp from the network is very secure but if we analyze how WhatsApp exchanges the private keys after the user removes app and reinstalls it on new device, we would see a security being compromised. Also, if we talk about encrypted backups, top messaging providers lack in saving precious mobile data of users. In order to provide the proper encrypted backup service having fewer mobile data requirement, we have explained about our application which has a combination of the following technologies including AES encryption of user security key, storage of AES encrypted RSA private key on server, storing chats directly on server, encrypted individual chat classes rather than compiled into a file, etc., which can effectively realize a secure and prompt chat backup service. In the event a disaster impacts user's device, encrypted data recovery can be easily and securely achieved without user explicitly backing. Finally, we have also proposed future scopes along with some new features providing users a more interactive User Interface than WhatsApp.

Keywords: Android, Encrypted Backup, Chat Application, WhatsApp, Data optimization.

I. INTRODUCTION

Social media is a means of communication that allows people to share information, ideas, files, and other items that may be valuable to others or that may be false information that is frequently disseminated nowadays, particularly on Facebook [1], [2]. The development and trend of social media rapidly increased due to the sophisticated technology developments and increasingly easy to use, especially smartphone technology. Social media is divided into two categories: social media sites and social media applications. Telegram, Instagram, WeChat, Line, and WhatsApp [3] are examples of extensively used social media programs, with WhatsApp having nearly 1,300,000,000 – 2,000,000,000 active users and continually expanding [4], [5]. WhatsApp could only be used for private messaging at first, but with major improvement, it is now utilized for group messaging, video calls, and high-quality phone conversations [6]. WhatsApp recently introduced new feature called end-to-end encrypted backups. If we talk about this feature, WhatsApp will ask user for a strong password which will used to protect the backup file by encrypting it using the password as the key. It is certainly not cleared by WhatsApp yet that what algorithm is being used to encrypt the file. Before the roll-out of this feature, the backup files were not encrypted but they were directly uploaded to the respective Google Drive account of the user. Everything in this new feature is absolutely fine but in this paper, we are going to explain about an implementation by which the encrypted backups will consume only half of the data they are consuming right now along with improved privacy. Along with improving backup efficiency and security, we have also implemented a new feature called "feelings", in which users can express their feelings on a certain chat message. This implementation is not a full-fledged application which is ready to launch in market but it is a prototype to explain the possibilities of saving user's data by providing him surplus privacy. Coming in this article we will first learn about some terminologies and algorithms which are being used to implement certain features of the application. After which we will move further to next section which gives a brief about tools and technologies used in the application after which we will see methodology used to develop the application.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

Following the methodology, we will learn about the Design Framework of the application and at last we will have a brief discussion about future scope and possibility of innovations in the application.

II. TERMINOLOGIES AND ALGORITHMS

There are various terminologies and algorithms being used in this application, which we need to have knowledge about in order to move further. Let us discuss them one by one:

End-To-End Encryption

End-to-end encryption (E2EE) is a secure communication method that prevents unauthorized access to data as it travels from one end system or device to another. E2EE encrypts data on the sender's system or device, and the key to decrypt it is only known by the intended receiver. While the communication is travelling to its destination, an internet service provider (ISP), application service provider (ASP), hacker, or any other business or service cannot read or interfere with it. Many prominent messaging platforms, such as Facebook, WhatsApp, and Zoom, use end-to-end encryption. The decision to use E2EE has caused a dispute among these vendors. The technology makes it more difficult for service providers to share customer information with police, and it could allow criminals to communicate in private [7].

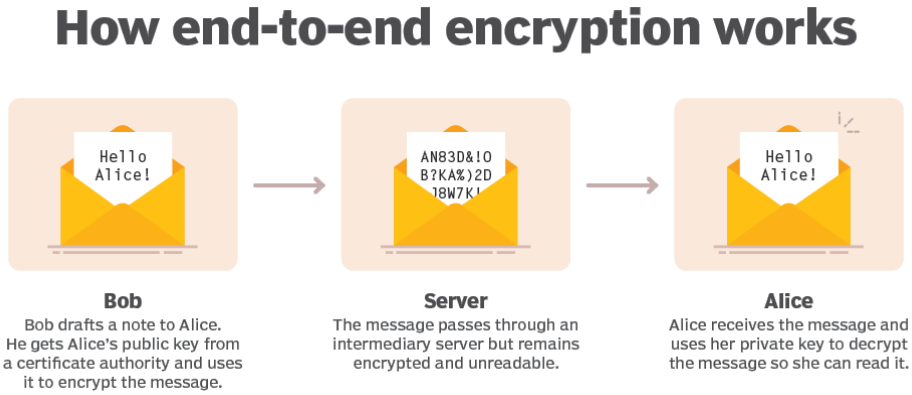

Figure 1: Working of End-to-End Encryption

Encryption takes place at the device level in genuine end-to-end encryption. Messages and files are encrypted before they leave the phone or computer, and they aren't decoded until they arrive at their destination. As a result, hackers are unable to access data on the server because they lack the private keys required to decrypt it. Instead, private keys are saved on the device of each individual user, making it far more difficult to access that person's data. The creation of a public-private key pair ensures end-to-end encryption security. This technology, also known as asymmetric cryptography, uses different cryptographic keys to encrypt and decrypt the communication. Public keys are extensively used to encrypt or lock messages and are freely distributed. The private keys, which are required to unlock or decrypt the message, are only accessible to the owner. The system generates public and private cryptographic keys for each individual who joins end-to-end encryption.

RSA Algorithm

Asymmetric cryptography includes the RSA algorithm. Because it uses two independent keys: a Public Key and a Private Key, it is asymmetric. The Public Key is shared with everyone, whereas the Secret Key, as the name suggests, is kept private.

As an example of asymmetric cryptography, consider the following:

1. A client (for example, a browser) sends the server its public key and requests data.

2. The server encrypts the data and delivers it to the client using the client's public key.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

3. This data is received by the client, who decrypts it.

The RSA concept is predicated on the fact that factoring a large number is difficult. The public key is made up of two numbers, one of which is the result of multiplying two huge prime numbers [8]. The private key is also made up of the same two prime numbers. As a result, the private key is compromised if the large number can be factored. When a result, encryption strength is totally reliant on key size, with encryption strength increasing exponentially as key size is doubled or tripled. RSA keys are typically 1024 or 2048 bits long, but experts believe that 1024-bit keys will be cracked soon. However, it appears to be an impossible feat at this time [9].

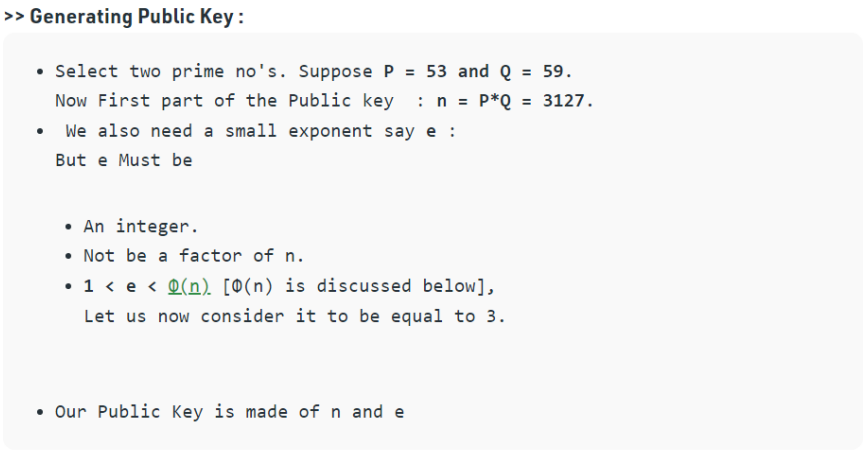

Figure 2: Generating Public Key

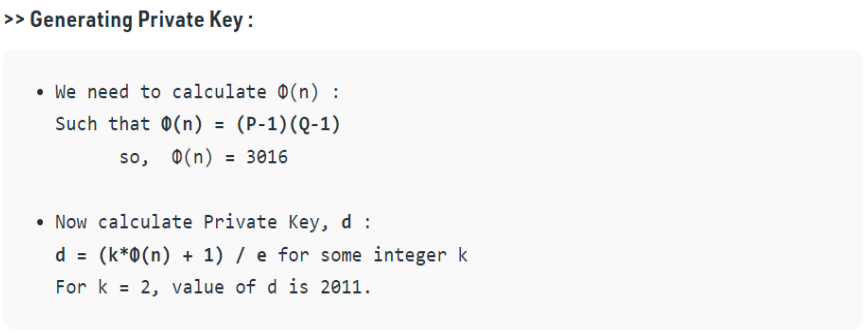

Figure 3: Generating Private Key

We now have our - Public Key (n = 3127 and e = 3) and Private Key (d = 2011).

We'll now encrypt "HI":

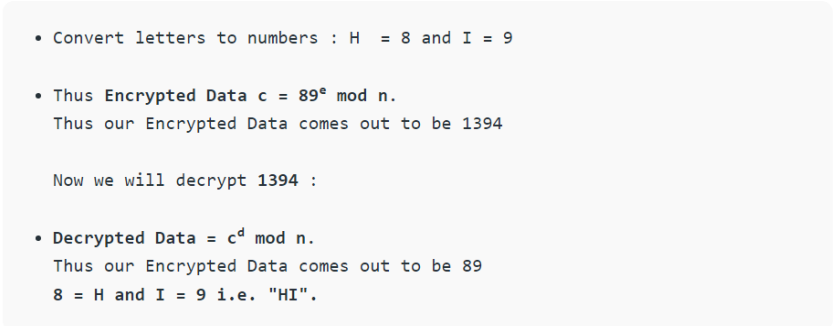

Figure 4: Decrypting Data

In our application, we have not derived the pair of keys by performing all these calculations, instead we have used RSA dependency for android which gets our work done in backend and provides us the pair we require.

AES Algorithm

The Advanced Encryption Standard (AES) was created by the US National Institute of Standards and Technology (NIST) in 2001 as a specification for the encryption of electronic data. Despite being more complex to construct, AES is still widely used today due to its superior strength than DES and triple DES [10].

Points to Keep in Mind:

1. The AES cypher is a block cypher.
2. The key can be 128/192/256 bits in length.
3. Data is encrypted in 128-bit chunks.

That is, it takes 128 bits as input and outputs encrypted cypher text in 128 bits. AES is based on the substitution-permutation network principle, which entails replacing and shuffling the input data through a series of connected processes.

III. TOP CHAT APPLICATIONS IN WORLD

We are trying to present an alternative backup encryption methodology which will enable the device to use 50% less data for backup upload and increased privacy. For us being able to understand the difference between standard methodology and the new methodology that will be presented in this article, we need to understand and know a little bit about the two industry leading chat applications.

WhatsApp

WhatsApp is one of the most popular mobile messaging applications available on a variety of devices (e.g., iOS, and Android). The service's architecture is confidential, and the information in this section comes from a variety of sources, including. The product's primary focus is message, with privacy issues coming in second. WhatsApp does not save any messages on the server; instead, the client's smartphone saves the conversation history. Along with this, WhatsApp also provides end-to-end encryption to users. If we talk about encrypted backup, WhatsApp has recently rolled out the option to opt for encrypted backup. If we see the process of encrypting the backup, WhatsApp encrypts user's chat backup file and then backup it on Google Drive. This way, WhatsApp is consuming mobile data for uploading both sender's messages and receiver's messages [11].

Telegram

In August 2013, two Russian brothers, Nikolai and Pavel Durov, launched Telegram, also known as Telegram Messenger. These brothers also founded the VK messenger, which they abandoned in 2014 owing to political difficulties. Telegram was founded in order to allow free online speech and to challenge WhatsApp's dominance. With 500 million users and a projected 1 billion by 2022, it is one of the most popular instant messaging programs. End-to-end encryption is Telegram's defining feature, however it's crucial to note that not every communication within Telegram is encrypted. For most messaging protocols, client-to-server encryption is utilized, which is less secure than end-to-end encryption but allows you to access your Telegram chats from other devices, including the web. For true end-to-end encryption, Telegram's Secret Chat feature is necessary. Although these private chats offer significantly more security, they can only be accessed from the device that sent the message [12].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

IV. TOOLS USED

Android Studio

Built on JetBrains' IntelliJ IDEA software and developed exclusively for Android development, The officially used integrated development environment (IDE) for Android application development which is also very amazing at performance is Android Studio. It will be available as a free download on Windows, macOS, and Linux in 2020, as well as a subscription-based service. It replaces the Eclipse Android Development Tools (E-ADT) as the primary IDE for native Android app development [13].

The current stable version includes the following features:

- Support for Gradle-based builds
- Refactoring for Android and fast fixes
- Performance, usability, version compatibility, and other issues are caught using lint tools.
- Integration and app-signing capabilities with ProGuard.
- Wizards based on templates for creating standard Android designs and components
- Users may drag-and-drop UI components in a powerful layout editor, and layouts can be previewed on numerous screen configurations.
- Building Android Wear apps is now possible.
- Google Cloud Platform compatibility is built-in, allowing connection with Firebase Cloud Messaging (formerly 'Google Cloud Messaging') and Google App Engine.
- In the Android studio, use the Android Virtual Device (Emulator) to execute and debug apps.

Firebase

Google's Firebase technology allows developers to create mobile and online applications. In 2011, it became a stand-alone firm. Google bought the platform in 2014, and it is now their primary app development platform [14].

Below are some of the key features of the Firebase:

- Authentication

  It accepts passwords, phone numbers, Google, Facebook, Twitter, and other methods of authentication. To manually integrate one or more sign-in methods into an app, utilize the Firebase Authentication (SDK).

- Realtime database

  Data is synced in real time across all clients and is available even when an app is turned off.

- Hosting

  Firebase Hosting is a fast web app hosting service that caches material in content delivery networks all around the world.

- Test lab

  The program is tested on Google's data centers' virtual and real equipment.

- Notifications

  No additional coding is required to send notifications with Firebase.

V. METHODOLOGY

We are going to cover the methodology in a very nice sequential manner so it is easy to understand ins and outs of the process that is going on.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

1. In this step user has started the application and signed up using his phone number as a basis for authentication after which he is directed to the Profile Setup page [15]. If the user is already registered, then just like WhatsApp, he is again directed to profile page.

2. It is the profile page activity, where the application is generating the pair of Public and Private Keys in the backend if the user is entering first time in the application. And if the user is already registered, then the keys are not again generated but the old keys are fetched from the server [16]. Yes! You heard it right, we are fetching Private key of user which is in encrypted form from the server.

3. After filling the profile information, the application asks user to enter a strong password which will be used to encrypt the private key and backups by using AES encryption [17]. Again, this step is performed only when the user is new to application, but if the user is already registered, then he is asked to enter his previous set password so that the application can decrypt the locked private key was fetched in previous step and also the encrypted backup file which will be processed in the next step.

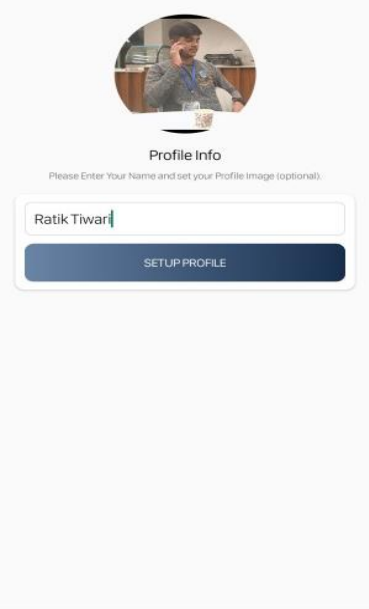

Figure 5: Profile Screen

4. Now comes the MainActivity screen which shows the list of statuses and users. This is screen which is responsible to load the encrypted backup from Firestore to the device. If the user is new to the application, then the local backup table is created to store the chats along with the required information like the chat ids and its content. After creating this local backup table in SQL file, we can finally upload the individual chat class objects after encrypting them one by one. This is the major difference between WhatsApp and our application. WhatsApp encrypts whole file and upload it in one go but we do not do the same. Encrypting the chat messages one by one by the AES key and then uploading them as individual units further decreases the possibility of the content to be hacked or cracked illegally. One major point to be noted here is that, WhatsApp is uploading both the sender's and receiver's message but, in our application, we have implemented the system to encrypt and backup only sender's side of messages, not the receiver's side. This is because the receiver's side messages are already present in our server and gets loaded when the user opens up any chat and they get decrypted by the help of Private key present the receiver's device.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

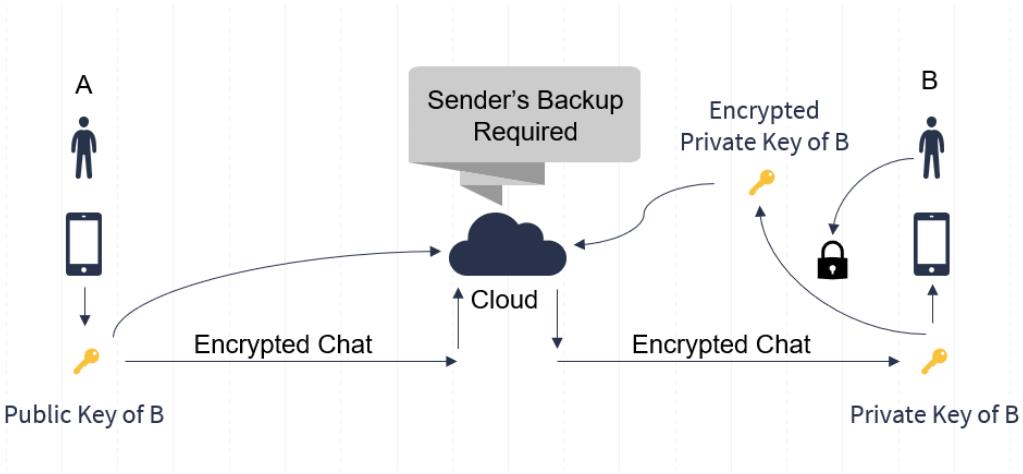

Figure 6: Data Backup Encryption Process

Figure 7: Main Screen (Status + Users List)

VI. DESIGN FRAMEWORK

In this application, we have used various object classes like User, Message, Status, etc. But in a broad to explain, all our data transactions are being handled by the Firebase Firestore and Firebase Realtime Database. Let us first see the Front-end Design Framework of the application:

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

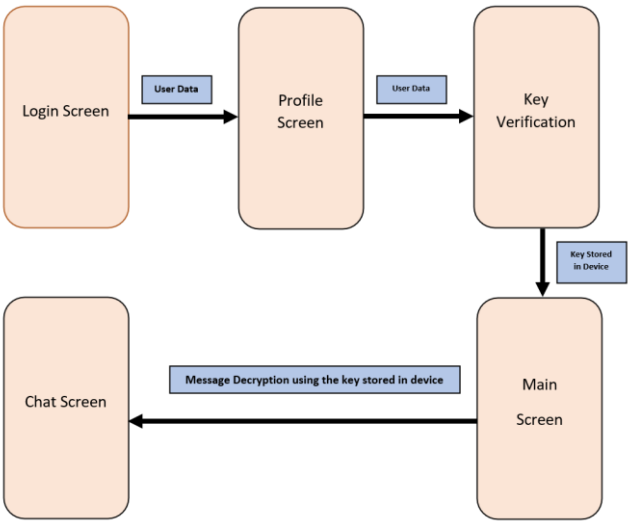

Figure 8: Front-end Design Framework

Now let us see the Backend Design Framework of the Application:

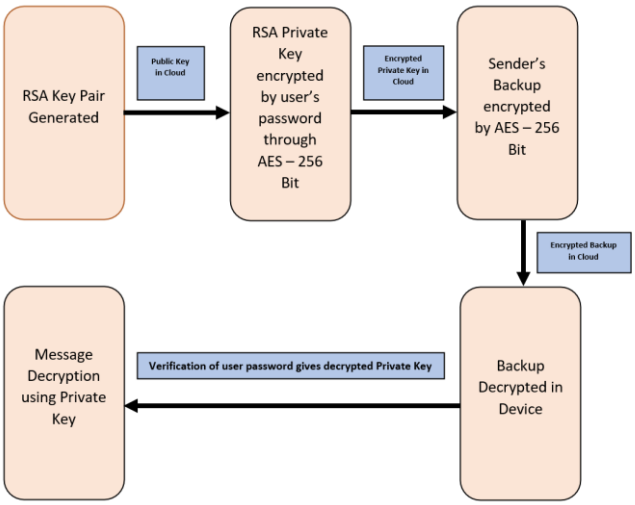

Figure 9: Back-end Design Framework

VII. FUTURE SCOPE

As a result, the application we have developed meets the requirements that we defined at the start of development. We are successfully able to send and receive messages without a third party being able to read conversations in the transition phase of message being sent from person A to person B. We would like to emphasize on the point that this application which we have developed is a basic prototype which can be the base of very huge applications providing tons of different services to user having an element of securely encrypted backups with data efficient properties. And we would like to suggest some innovations that can be carried out in order to make this prototype even more sophisticated.

1. Use of Machine Learning Algorithms to auto reply to the messages being received at the receiver's end. We can use Natural Language Processing (NLP) to reply to the messages [18]. Also, the model will be correcting itself by time and the outputs will be more in accordance with the nature of person using the application.

2. Implementation of safe and secure payment gateways for our application. Payment Gateway is a type of software that allows users to pay to some account within the application. Nobody could make an internet transaction without a Payment Gateway. The good news is that such gateways allow for the verification of client data as well as support for major financial systems such as MasterCard, Visa, and others. We have not implemented a payment gateway in our application just like the WhatsApp does because we are working on the application having debug mode activated in Firebase services which did not let us use the gateway for users.

3. Addition of admin panel for the admins of the group. Admin can be an authorized person to monitor and manage the chat groups in the application. This concept is not yet implemented by any of the major messaging providers. Admin panel can have features like disable messaging for certain participants, muting some participants, separate private lobby for admin and participants, and many more features can be added.

4. We can use Augmented Reality to present the Display Picture of a user in a new and better way. This will show pictures in a more 3D and realistic manner. We can use Google's ARCore Platform for building such an experience [19]. ARCore allows your phone to perceive its surroundings, interpret the world, and interact with information through a variety of APIs. This again is an area of deep research and application of graphical concepts.

VIII. CONCLUSION

WhatsApp and other messaging applications are very secure now and there may be no need for security additions but the storage of messages in backup file and then uploading of that backup on the server still weak and has some scope of improvement. This weakness can be overcome by providing added security in this case using Data efficient AES encrypted array of individual backup packets method. Talking about learnings, we've discovered that the vast amount of data created by Android devices needs proper backend and database operation knowledge in order to provide better backup security. We also discussed some of the most important aspects of our application architecture, how they function, and what are some of the improvements that can be made. The most recent studies and reports on the subject of Android and Encrypted chatting have also been addressed in the above study. In all, we assessed Android application development, Cryptography algorithms, industry standards of securing chats and backups and our development methodology including the possibility of innovations.

ACKNOWLEDGEMENTS

I take this opportunity to acknowledge all those who have guided me during this project. I express my earnest gratitude towards **Mr. Azhar Ahmed**, my project guide for his valuable encouragement and guidance. His motivation and suggestions were invaluable in the project work. I am grateful for his most cooperative attitude and suggestions, without which I would not have been able to do this work. I would also like to express my gratitude to the faculty members for their kind assistance and cooperation during the development of my project.

IX. REFERENCES

[1] J. K. Riley, "Liking the Lies: An Analysis of Hoaxes on Facebook and What They Mean for the Contextual Framework of Viral Message Spread | Response," 2017. [Online]. Available: https://responsejournal.net/issue/2017- 06/article/liking-lies-analysis-hoaxes-facebook-and-whatthey-mean-contextual-framework.

[2] J. Evans and A. Rzhetsky, "Machine science," Science, vol. 329, no. 5990. pp. 399–400, 2010.

[3] E. Winarko and A. Cherid, "Recognizing the Sarcastic Statement on WhatsApp Group with Indonesian Language Text," in International Conference on Broadband Communication, Wireless Sensors and

Powering (BCWSP), 2017, pp. 1–6.

[4] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, Viber and Telegram which is Best for Instant Messaging?" Int. J. Electr. Comput. Eng., vol. 6, no. 3, p. 909, 2016.

[5] P. Kallas, "Top 15 Most Popular Social Networking Sites and Apps [February 2018] @DreamGrow 2018," 2018. [Online]. Available: https://www.dreamgrow.com/top-15- most-popular-social-networking-sites/. [Accessed: 31-Mar2018].

[6] WhatsApp Official Documentation, https://scontent.fdel63-1.fna.fbcdn.net/v/t39.8562-6/271639644_1080641699441889_2201546141855802968_n.pdf?_nc_cat=108&ccb=1-5&_nc_sid=ad8a9d&_nc_ohc=KcPwTrBL1xMAX-OE5GK&_nc_ht=scontent.fdel63-1.fna&oh=00_AT_g27Zjw7OoHu2KSvuCdPA27dM9gYo4utuhTx_638Ejbg&oe=6273CBFD

[7] The Many Faces of End-to-End Encryption and Their Security Analysis - Mohamed Nabeel, https://www.researchgate.net/publication/319633280_The_Many_Faces_of_End-to-End_Encryption_and_Their_Security_Analysis

[8] RSA Public Key Cryptography Algorithm – A Review, Shireen Nisha - University of Fiji, Mohammed Farik - University of Fiji

[9] RSA Algorithm in Cryptography, Mohit Gupta, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[10] Toa Bi Irie Guy-Cedric, Suchithra. R., "A Comparative Study on AES 128 BIT AND AES 256 BIT", International Journal of Scientific Research in Computer Science and Engineering Vol.6, Issue.4, pp.30-33, August (2018).

[11] WhatsApp, Wikipedia, https://en.wikipedia.org/wiki/WhatsApp.

[12] Telegram, Wikipedia, https://en.wikipedia.org/wiki/Telegram_(software)

[13] Android Studio, https://developer.android.com/studio

[14] Firebase, https://firebase.google.com/

[15] Ranganath Manohar Rane, Tilak Maharashtra Vidyapeeth Department of Computer Science; Sandesh Suresh Kadam, Tilak Maharashtra Vidyapeeth Department of Computer Science, "A Research Paper on Firebase Authentication", Paper ID: IJSRDV9I50021, Published in: Volume: 9, Issue: 5, Publication Date: 01/08/2021, Page(s): 55-56.

[16] Li Dongjiang; Wang Yandan; Chen Hong, "The Research on Key Generation in RSA Public-Key Cryptosystem", DOI: 10.1109/ICCIS.2012.348

[17] Omer K. Jasim Mohammad, "Innovative Method for enhancing Key generation and management in AES-algorithm", https://arxiv.org/ftp/arxiv/papers/1504/1504.03406.pdf

[18] Moneerh Aleedy, "Generating and Analyzing Chatbot Responses using Natural Language Processing", January 2019, International Journal of Advanced Computer Science and Applications 10(9), DOI:10.14569/IJACSA.2019.0100910

[19] TD Pamungkas, "Android-based augmented reality media and the curiosity about mathematics", October 2020, Journal of Physics Conference Series 1663(1):012016, DOI:10.1088/1742-6596/1663/1/012016