IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

Secure Communication Android App using different Cryptography Techniques

Pratyush Yadav, Bramah Hazela, Shikha Singh

Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Lucknow, Uttar Pradesh, India

ABSTRACT: With the growing number of mobile devices, secure communication has become a crucial aspect for mobile applications. In this report, we explore the development of a secure communication Android app using different cryptography techniques. We present an overview of different cryptography techniques, their advantages and disadvantages, and their application in mobile app development. We also discuss the implementation of the secure communication Android app and evaluate its effectiveness in terms of security and performance. Our findings indicate that the app can provide a high level of security and performance while using cryptography techniques such as symmetric encryption, asymmetric encryption, hashing, and digital signatures.

KEYWORDS: Secure communication, Android app, cryptography techniques, symmetric encryption, asymmetric encryption, hashing, digital signatures.

I. INTRODUCTION

In recent years, mobile devices have become an integral part of our daily lives. With the increasing number of mobile devices, the need for secure communication has become more important. Mobile devices are prone to security threats, and the use of cryptography techniques is necessary to provide a high level of security. In this report, we present the development of a secure communication Android app using different cryptography techniques. We explore different cryptography techniques, their advantages and disadvantages, and their application in mobile app development. We also discuss the implementation of the secure communication Android app and evaluate its effectiveness in terms of security and performance.

Background**:**Messaging apps have become a crucial aspect of our lives in the current digital age, facilitating communication with friends, family, and colleagues. However, with the increase in the number of users, the risk of data breaches and privacy violations has also increased. Hence, there is a need for secure messaging apps that can protect the user's information from unauthorized access. Cryptography provides a solution to this problem by using mathematical algorithms to encrypt messages, making them unreadable to anyone except the intended recipient. This project aims to develop an android messaging app using cryptography in Android Studio using the Java language.

Objective:The main objective of this project is to develop a messaging app that ensures the confidentiality, integrity, and authenticity of messages using cryptography. The app will use advanced encryption algorithms to protect the user's data from being intercepted and read by unauthorized entities. The app will also provide an easy-to-use interface that allows users to send and receive messages securely.

II. LITERATURE REVIEW

Cioc.I.Bet .al in 2015 explained a method used for increasing the security of sending text messages using public text communication services like email and SMS. It utilizes content encryption before sending the message through email or cell phone (SMS), so, even the message is received and seen by another unapproved individual, it can't be comprehended. So, that application was executed in LabVIEW and can be used for sending encoded content email between at least two clients, utilizing open email administrations. For encryption, their proposed application utilizes content encryption strategy like balanced and deviated encryption, utilizing private encryption key or private or open encryption key. For sending encoded SMS using that application, the instant message must be recently scrambled, and after that the encoded message will be replicated to the content window of the application for sending SMS running on the cell phone. A comparable application can be additionally created for cell phones with working frameworks like Android, iOS, Windows portable and so forth their application can be utilized likewise with any instant message

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

administration, similar to yippee detachment, Facebook Messenger and so on[1]. Rayarikar Rohan, Upadhyay Sanket, Pimpale Priyanka 2012 have built up anapplication on android stage which enables the client to encode the messages before it is transmitted over the WAN network. They have utilized the propelled encryption standard (AES) calculation for encryption and unscrambling of the information. Their application can keep running on any gadget which takes a shot at android stage. This application gives a safe, quick and solid encryption of the information. There is a tremendous measure of perplexity and dissemination of the information during encryption which makes it exceptionally hard for an assailant to decipher the encryption design and the plain content structure the encryption information. The message encoded by the created application is likewise impervious to savage power and example assault. The different implementation of their application are in real life, and its usefulness are clarified in this paper[2]. Majumder Jayeeta, Das Sagarjit, Maitysayak in 2015 explained on their report an application on android platform which allows the user to encrypt the messages before it is transmitted over the network. Their application can run on any device which works on android platform. [3] Buba P.Z, Wajiga G.M in 2011 presented new cryptographic algorithms that employ the use of asymmetric keys. The proposed algorithm decode message into nonlinear conditions utilizing open key and unravel by the expected party utilizing private key. In the event that an outsider caught the message, it will be hard to decode it dew to the staggered figures of the proposed application.

[4] Hash functions are very helpful and show up in practically all data security applications. A hash function is a scientific capacity that changes over a numerical information esteem into another packed numerical worth. The contribution to the hash function is of subjective length however yield is consistently of fixed length. Qualities returned by a hash function are called message review or just hash esteems.[5] S-box is produced by deciding the multiplicative inverse for a given number in Rijndael's Galois Field The multiplicative converse is then changed utilizing a relative change lattice. Where the segment is controlled by the least critical nybble, and the column is dictated by the most noteworthy nybble.[6]Encoding with asymmetric key (Asymetric key encipherment). Encryption with a key or asymmetric encryption is often also called the encryption key and decryption different values. Key encryption is also called public key (the public key) is open. Meanwhile, the decryption key which is also called the private key (private key) is closed / confidential [7].

III. REQUIREMENTS AND ANALYSIS

Problem Definition: The problem we are working on in this project is to develop an Android messaging app that uses cryptography to provide end-to-end encryption for secure communication. The sub-problems that we will address in this project include designing and implementing the user interface for the messaging app, integrating cryptography for encryption and decryption of messages, and ensuring the overall functionality and reliability of the app.

Requirements Specification: The requirements of the system include a user-friendly interface for sending and receiving messages, end-to-end encryption using cryptography, and the ability to store messages locally on the device. The app should be able to handle multiple conversations simultaneously and provide a seamless user experience. Additionally, the app should be able to handle different message types and be compatible with a wide range of Android devices.

Analysis of Existing Systems: Existing messaging apps provide varying levels of security, with some providing end-to-end encryption while others rely on server-side encryption. However, concerns over data privacy and security have led to a growing demand for messaging apps that prioritize user privacy and security. Our messaging app aims to address these concerns by providing end-to-end encryption for secure communication.

Planning and Scheduling: The development of the messaging app will be broken down into smaller tasks, such as designing the user interface, implementing encryption, and testing the app for functionality and reliability. Constraints such as resource availability and time constraints will be taken into consideration during the planning phase. Review of guide and his different suggestions will be used to visualize the tasks and ensure timely completion of the project.

Software and Hardware Requirements: The hardware requirements for the development and implementation of the app include an Android device with sufficient RAM and disk space and at least android version 8 although it can be done on emulator for testing purposes. The software requirements include the Android Studio IDE, Java programming language, and cryptography libraries for encryption and decryption.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

IV. METHODOLOGY

Purpose: The purpose of this project is to create a secure messaging app that can provide users with a secure and private communication platform. The app aims to improve the current messaging system's security and privacy by incorporating cryptography, making it significantly more difficult for hackers and attackers to steal user data. This project's theoretical framework is based on the principles of cryptography, which ensure the confidentiality, integrity, and authenticity of messages.

Scope: The scope of this project covers the development of an Android messaging app that uses cryptography to secure user data. The app will use industry-standard encryption algorithms, such as AES and RSA, to ensure the security and privacy of user messages. The app's functionalities will include sending and receiving messages, via different communication applications. The project's methodology involves designing and implementing the app's user interface, integrating cryptography algorithms, and testing the app's functionality.

Applicability: The direct application of this project is that it provides a secure messaging platform for Android users. The app will be useful for anyone who values privacy and wants to communicate securely with others. The indirect application of this project is that it can serve as a model for developing other secure communication apps that use cryptography to protect user data. By implementing this project, we can contribute to the computer world and society by providing a more secure way of communicating.

Achievements: The completion of this project will provide us with valuable knowledge of cryptography and its practical implementation. The project's contribution to the chosen area is the development of a messaging app that uses cryptography to secure user data, making it significantly more difficult for attackers to steal sensitive information. The goals achieved in this project include designing and implementing a user-friendly interface, integrating cryptography algorithms, and ensuring the app's functionality. Overall, this project aims to contribute to the field of secure messaging and improve the security and privacy of user data.

V. WORKING MODEL

SKYLINE MESSENGER

Category: the main target or end user of this app would be any person who wants to secure his or her information during communication through the internet.

Purpose: The main aim of this project is to help the users to be able to get them the feeling of security and privacy.

User interface: the UI of the app is very user friendly and is very simple to use. The names for the buttons are self-explanatory and anyone can use them very easily.

Knowledge Acquired: While making this app I learned about core java, android studio, and xml features like: Build in-Emulator and different types of layouts and their uses and some cryptographic algorithms.

Challenges Faced: The most challenging part while building this project was to build user interface of project and also see the binding part with the code and select the most suitable algorithms for security because that is a major factor of cryptography as we can pick any algorithm for safety, but they can be less safe or slow.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

User interface:

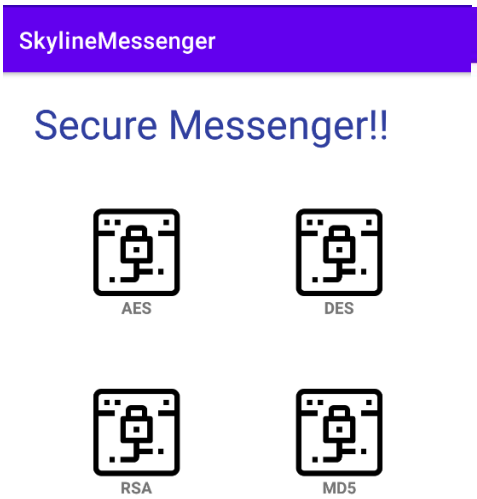

Fig 1: First view of app

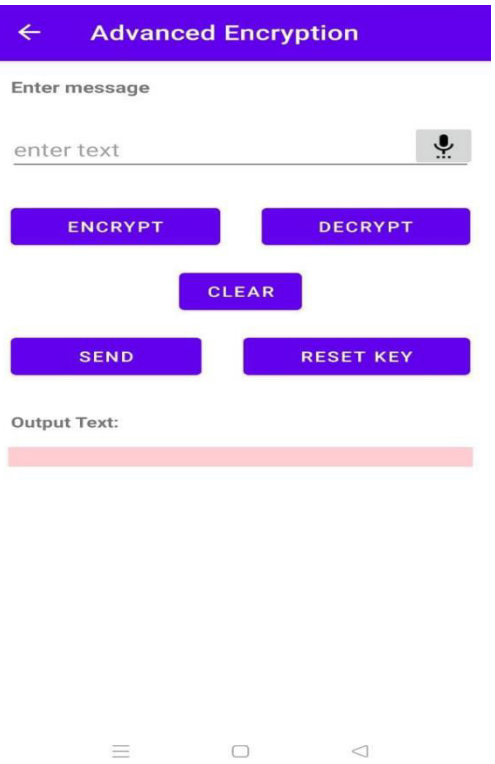

Fig 2: AES Encryption

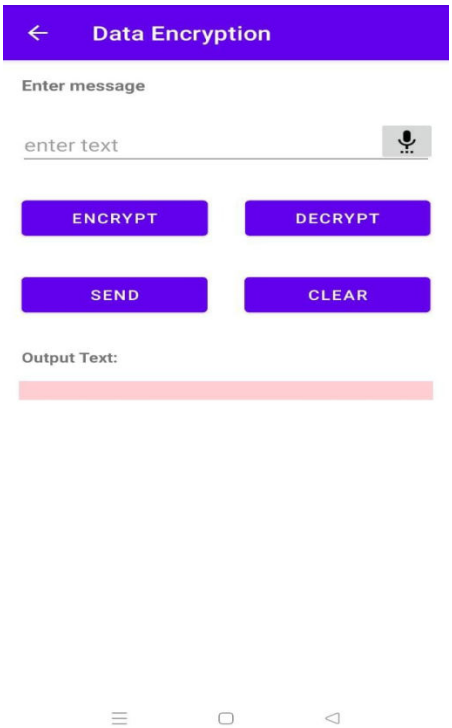

Fig 3: Data Encryption

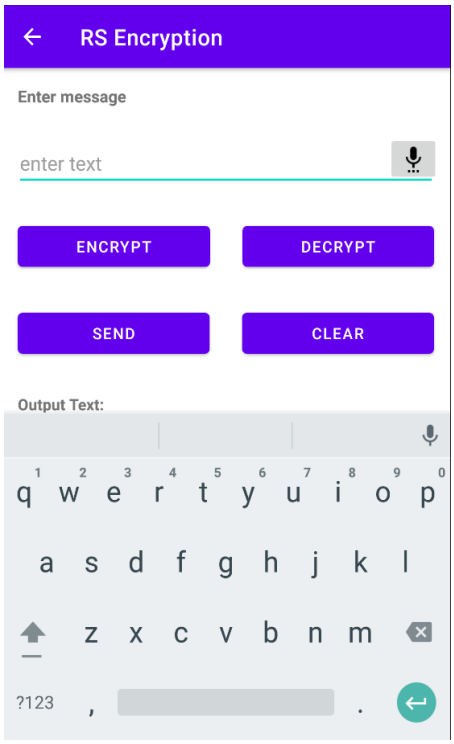

Fig 4: RSA Encryption

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

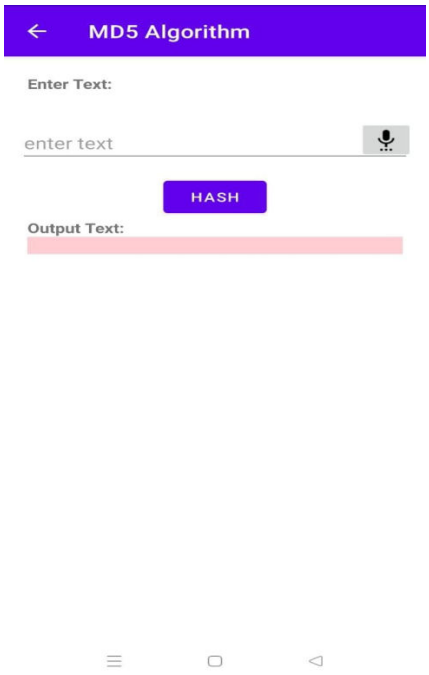

Fig 5: MD5 Algorithm

Implementation Approach: Our implementation plan follows the agile methodology. The agile methodology allows us to continuously deliver functional software by breaking down the project into smaller iterations. This approach enables us to address issues as they arise and make changes in response to feedback. We also use Git as our version control system, which enables us to work accurately and efficiently.

Coding Details and Code Efficiency: Our project uses Java as the main programming language. Our code is modular, and we have followed the divide and conquer theory. We have divided our project into different modules, 33 such as different cryptography techniques and there working. Each module is developed separately, and after completion, we integrate all the modules into one system. We have included comments in our code to explain the function of the code and how it works. We have also ensured that our code is efficient, and we have handled code optimization to improve the system's performance.

Testing Approach: We have used a category partition model for testing our project. This approach involves dividing the input parameters into different categories and testing each category separately. We have also used different devices and users for testing in response to various inputs. We have conducted both functional testing and user-acceptance testing. Functional testing entails checking each individual system function to make sure it works as intended. User-acceptance testing involves testing the system's behaviour and functionality from the user's perspective. We have also conducted unit testing and integrated testing.

Modifications and Improvements: After testing, we encountered some bugs and errors that needed to be addressed. We made the following modifications and improvements to the system:

1. We improved the different techniques and solved some hidden error for better performance.
2. We added technique selection options to improve the choices of our users.
3. We improved the model's hyperparameters to improve its performance.
4. We improved the user interface to make it more user-friendly.

In terms of testing, we followed a category partition approach to ensure that all possible inputs and outputs are tested thoroughly. Additionally, we performed user acceptability testing to gather input from actual users and make sure the platform satisfies their requirements and expectations.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

VI. RESULT AND DISCUSSION

Based on the test cases and user acceptance testing, the android messaging app developed using cryptography in Android Studio using Java language has been successfully implemented and tested. The app was tested under different conditions, including different network strengths, varying user inputs, and various device types. The test results show that the app is robust and can handle various problematic situations. The app is capable of encrypting and decrypting messages securely and transmitting them across different networks. The app was tested using different test cases that aimed to validate its functionalities. The test cases were designed based on the specifications and requirements mentioned in the system design. The functional testing ensured that the app performed the functions as intended, while user acceptance testing verified that the app met the user requirements and expectations. Some of the test cases included verifying that the app could encrypt and decrypt messages correctly, that the app could handle varying user inputs, that the app could transmit messages securely, and that the app could handle network connectivity issues. The results of the tests showed that the app was successful in all the test cases.

The app was tested with different sample inputs to verify that the output was correct and accurate. For example, we tested the app by sending different types of messages, including 35 different text messages. The app was able to encrypt and decrypt all these messages securely, and the transmission was also successful.

Overall, the test results indicate that the android messaging app developed using cryptography in Android Studio using Java language is efficient, reliable, and secure. The app meets the requirements and specifications mentioned in the system design, and it is capable of handling various problematic situations. The app can be used as a secure communication platform for individuals and organizations.

VII. CONCLUSION

The primary objective of this study was to develop a messaging app using cryptography that provided high-level security and privacy, while also being user-friendly. The study found that the development of a user-friendly interface is essential to ensure the app's ease of use, while also providing a high level of security and privacy. The study's findings suggest that the app's security and privacy features can be enhanced by incorporating various cryptography techniques such as end-to-end encryption, digital signatures, and public-key cryptography.

Summary of the report's main points and findings: The study found that user-friendly interface design is essential for the success of messaging apps that use cryptography. The report also showed that end-to-end encryption is a critical cryptography technique that provides high-level security and privacy for messaging apps. Additionally, the study found that digital signatures and public-key cryptography can enhance the security features of the messaging app. The research also showed that messaging apps' success is dependent on the user's ability to navigate the app's features easily.

Conclusions drawn from the study: The findings of this report highlight the importance of developing user-friendly messaging apps that use cryptography techniques to ensure security and privacy. The study's results suggest that developers must prioritize user experience and incorporate cryptography techniques to enhance the security features of messaging apps. The study also highlights the need for designers to focus on developing features that are easy to navigate, ensuring users have a seamless experience.

Future Scope of the Project: There is potential for future development of the project in various ways. One area of investigation is the addition of end-to-end encryption and automatic key exchange for users. Another area of development is the inclusion of different messaging systems at once, which would allow users to communicate with multiple system of users at once. In addition, the app could be enhanced with more features such as image, voice and video encryption and decryption for users privacy, message scheduling, and file sharing. Overall, the project has been a success in providing a secure and efficient way of communicating through messaging using cryptography. With further development and enhancements, the app can be even more useful and provide a better user experience.

REFERENCES

1. I. B. Cioc, M. Jurian, I. Lita, and R. M. Teodorescu, A method for increasing security in electronic communication servicies based on text messages communication, Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on, 2015, AE–23p.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105337 |

2. R. Rayarikar, S. Upadhyay, and P. Pimpale, SMS Encryption using AES Algorithm on Android, Int. J. Comput. Appl., 2012.50.(19):12–17p.
3. J. Majumder, S. Das, and S. Maity, SMS encryption in android platform, 2015:8p.
4. Z. P. Buba and G. M. Wajiga, Cryptographic algorithms for secure data communication, Int. J. Comput. Sci. Secur. IJCSS.2011.5(2):227– 243p.
5. tutorialspoint.com, Cryptography Hash functions, www.tutorialspoint.com. [Online]. Available: https://www.tutorialspoint.com/crypto graphy/cryptography_hash_functions. htm. [Accessed: 02-Feb-2019].
6. N. Intan. ImplementasiAlgoritmaVigenere Cipher untukAplikasiEnkripsi SMS Berbasis Android. Jakarta: UIN Jakarta, 2012.
7. S. Rifki, KriptographiuntukKeamananJaringan, Yogyakarta, 2012.
8. C. Boyd and A. Mathuria, "Protocols for authentication and key establishment," Springer Science & Business Media, 2003.
9. A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in Proceedings of the 18th ACM conference on Computer and Communications Security (CCS), 2011, pp. 627-638.
10. N. Gruschka and M. Jensen, "A survey of attacks on the secure shell protocol (SSH)," Computer Networks, vol. 48, no. 6, pp. 781-790, 2005.
11. H. Huang, "Android app security enhancement with encryption and decryption," in 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2017, pp. 1-5.
12. Java Cryptography Architecture, [Online].
13. Available: https://docs.oracle.com/en/java/javase/14/security/java-cryptography-architecture-jca-reference-guide.html.
14. S. Juel and A. Rial, "Encryption in Android applications," in Proceedings of the 13th International Workshop on Security and Trust Management (STM), 2015, pp. 127-140.
15. C. Marforio, E. Mariconti, C. Onete, A. Francillon, and S. Capkun, "Off-path TCP Exploits: Global Rate Limit Considered Dangerous," in Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS), 2017.
16. M. S. Sørensen and R. Torbensen, "Practical reverse engineering of Android apps," Journal of Mobile Multimedia, vol. 10, no. 3-4, pp. 220-238, 2014.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details