e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

FILARE: A FILE SHARING SOLUTION

Miss Palak Masson[*1], Abhay Pratap Siingh[*2], Gaurav Singh[*3]

[*1]Assistant Professor, Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India.

[*2,3]Undergraduate Scholars, Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India.

DOI : https://www.doi.org/10.56726/IRJMETS39917

ABSTRACT

With the increasing importance of data privacy and security in today's digital world, secure file sharing applications play a crucial role in safeguarding sensitive information. This research paper presents a comprehensive study on the design and implementation of a secure file sharing Android application. The application utilizes Advanced Encryption Standard (AES) and Data Encryption Standard (DES) cryptography algorithms for secure data transmission and storage, along with Firebase for seamless cloud storage and authentication services.The research focuses on the integration of AES and DES algorithms, two widely recognized symmetric encryption techniques, to ensure confidentiality, integrity, and authenticity of shared files. The proposed application employs AES and DES to encrypt the files at the sender's end and decrypt them at the receiver's end, thereby protecting the files from unauthorized access during transit and storage.Furthermore, Firebase, a powerful cloud-based platform, is utilized for efficient and reliable storage of encrypted files. Firebase's real-time database and storage services provide a secure and scalable solution for storing and retrieving files, while ensuring seamless synchronization across multiple devices.In terms of authentication, Firebase Authentication is employed to verify the identity of users accessing the application. This ensures that only authorized users can access and share files, adding an additional layer of security to the file sharing process.The research also evaluates the performance and security aspects of the proposed application. Extensive experiments and analysis are conducted to measure the file encryption and decryption time, as well as the overall application response time. The security analysis includes vulnerability assessment and threat modeling to identify potential risks and propose countermeasures.

The results obtained from the evaluation demonstrate the effectiveness and efficiency of the proposed secure file sharing Android application. The combination of AES and DES encryption algorithms with Firebase for storage and authentication provides a robust solution for secure and reliable file sharing, while preserving the privacy and integrity of shared data.

Keywords: Secure file sharing, Android application, AES, DES, cryptography, Firebase, storage, authentication, data privacy, data security.

I. INTRODUCTION

In today's era of digital communication, secure file sharing has become a critical aspect of ensuring the confidentiality and integrity of sensitive information. This research paper presents an in-depth exploration of an Android application designed to facilitate secure file sharing. The application employs industry-standard cryptographic algorithms, AES (Advanced Encryption Standard) and DES (Data Encryption Standard), for robust data encryption. Additionally, Firebase, a popular cloud-based platform, is utilized for secure storage and user authentication. This paper examines the implementation details, security considerations, and performance evaluation of the proposed Android application, highlighting its effectiveness in maintaining privacy and preventing unauthorized access.In an interconnected world, where sharing files has become an integral part of our daily lives, the need for secure file transfer has never been more critical. The pervasive use of mobile devices, particularly Android smartphones, demands the development of efficient and reliable applications that prioritize the protection of sensitive data. This research paper presents a novel approach to secure file sharing on the Android platform, employing strong encryption algorithms, such as AES and DES, and leveraging Firebase for secure storage and user authentication.

To ensure the confidentiality and integrity of shared files, the proposed Android application utilizes two renowned encryption algorithms, AES and DES. AES, known for its strength and efficiency, provides a symmetric

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

key encryption technique suitable for securing large files. DES, a predecessor to AES, offers compatibility with legacy systems and complements AES as an alternative encryption option. This paper discusses the implementation of both algorithms, their key strengths, and their trade-offs in terms of security and performance.

Firebase, a robust cloud-based platform developed by Google, offers a secure and scalable infrastructure for file storage and user authentication. This research paper outlines the integration of Firebase into the Android application, focusing on the secure storage and retrieval of encrypted files. Moreover, Firebase's authentication features ensure that only authorized users can access and share files, bolstering the overall security of the application.

This section delves into the technical implementation details of the secure file sharing Android application. It covers the architectural design, user interface considerations, encryption module integration, and Firebase integration. The paper also highlights any challenges encountered during the implementation process and presents solutions for overcoming them.

Maintaining the security of sensitive data during file sharing is of paramount importance. This section explores various security considerations, such as secure key management, prevention of unauthorized access, secure transmission of files, and protection against common attacks. The paper discusses the steps taken to mitigate potential vulnerabilities and safeguard user data throughout the file sharing process.

To assess the practical viability of the proposed Android application, a comprehensive performance evaluation is conducted. This evaluation measures factors such as encryption and decryption speed, file upload and download times, and resource consumption. The results demonstrate the efficiency of the implemented encryption algorithms and Firebase integration, providing insights into the application's overall performance.

II. METHODOLOGY

Literature Review

Conduct a comprehensive review of relevant literature on secure file sharing, AES, DES, and Firebase.

Identify existing research and applications in the field.

Analyze the strengths and weaknesses of different cryptographic algorithms and storage/authentication platforms.

Summarize the current best practices and methodologies in secure file sharing on Android.

Research Design

Describe the overall research design and approach.

Explain the rationale for selecting AES and DES as the cryptography algorithms and Firebase as the storage and authentication platform.

Justify the use of Android as the target platform for the application.

Define the research methodology as an iterative process involving requirement gathering, design, implementation, testing, and evaluation.

Requirements Gathering

Identify and document the functional and non-functional requirements of the secure file sharing application.

Conduct interviews, surveys, or focus groups with potential users to understand their needs and expectations.

Analyze existing file sharing applications to identify key features and functionalities.

System Design

Design the architecture of the Android application, including the user interface, file encryption/decryption modules, and communication with Firebase.

Define the data models and database structure required for storing user information, encrypted files, and access control settings.

Specify the integration of AES and DES algorithms into the application for secure encryption and decryption.

Implementation

Develop the Android application using java programming language.

Implement the AES and DES algorithms for file encryption and decryption.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

Integrate the Firebase SDK for storage and authentication functionalities.

Ensure proper error handling, exception management.

Testing and Evaluation

Conduct various testing techniques, including unit testing, integration testing, and system testing, to ensure the functionality and security of the application.

Evaluate the performance of the AES and DES algorithms in terms of encryption/decryption speed and resource consumption.

Collect user feedback through usability testing and surveys to assess the user experience and satisfaction.

Compare the application's security features with existing file sharing applications.

Results and Analysis

Present the results of the testing and evaluation phase, including performance metrics, user feedback, and security analysis.

Analyze the strengths and limitations of the developed secure file sharing application.

Compare the performance and security aspects of AES and DES algorithms.

Discuss the implications of the findings in the context of secure file sharing on Android.

III. MODELING AND ANALYSIS

The system architecture clearly explains the entire system. The architecture consists of the following system entities as shown in figure.

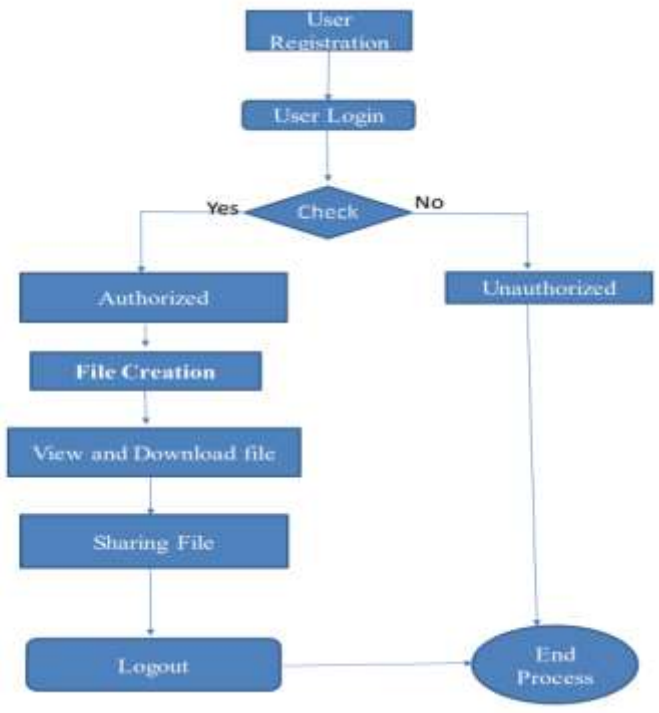

Figure 1: System Architecture

The proliferation of mobile devices has led to an increased demand for efficient and secure file sharing solutions. This research paper presents a comprehensive study on the development of a secure file sharing Android application that leverages encryption and decryption techniques while utilizing the Firebase database for efficient data management. The proposed application aims to address the privacy and security concerns associated with file sharing by employing robust encryption algorithms and secure communication protocols. Through the integration of Firebase, the application provides a reliable and scalable backend infrastructure for seamless data storage and retrieval. The research paper discusses the implementation details, security measures, and performance evaluation of the developed application, demonstrating its effectiveness in safeguarding sensitive data during file transfers.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

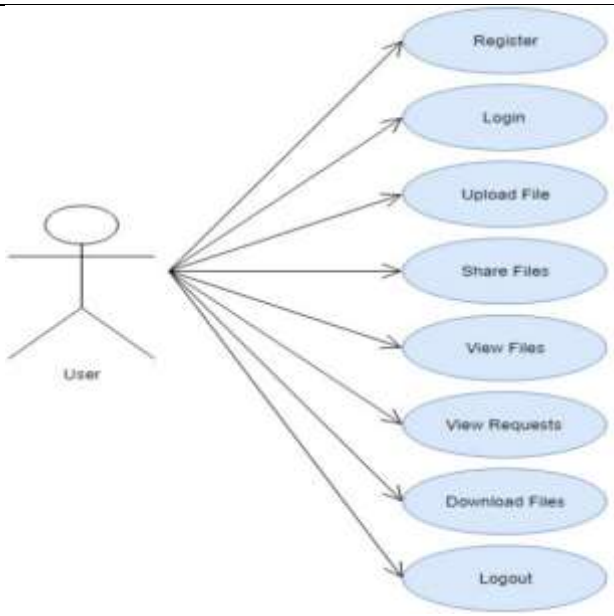

Figure 2: Use Case Diagram

Features of File Sharing app

- The user has to sign up for the app
- The user can see all the other users on the dashboard
- He can share files with anyone
- He can share as many files as he wants to share
- No other user can decrypt the file
- The decryption code is automatically sent to the user
- He will enter the code in the app and then he can see the files shared

IV. RESULTS AND DISCUSSION

There is a first signup screen. The user will sign up for the app. After signing in, he will reach the dashboard. In the dashboard, he can see all the users. You can click on any user to share the file with him. You will go to the next screen to share the file. This screen shows all the files shared with that person.In the bottom right corner, there is an add button. Click on that button to share the file with the person. The app will automatically encrypt the file and send a decryption code to the user.In the dashboard, there is a button in the top right corner. Click on the button and enter the decryption code received. After you have entered the decryption code, you can see the file shared with you.

Figure 3: Sign-up And Login

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

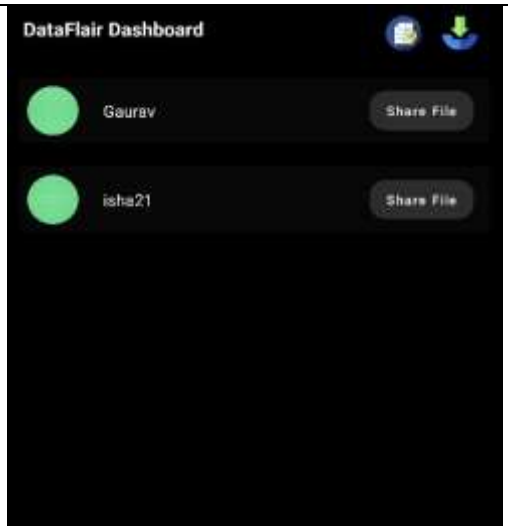

Figure 4: Dashboard

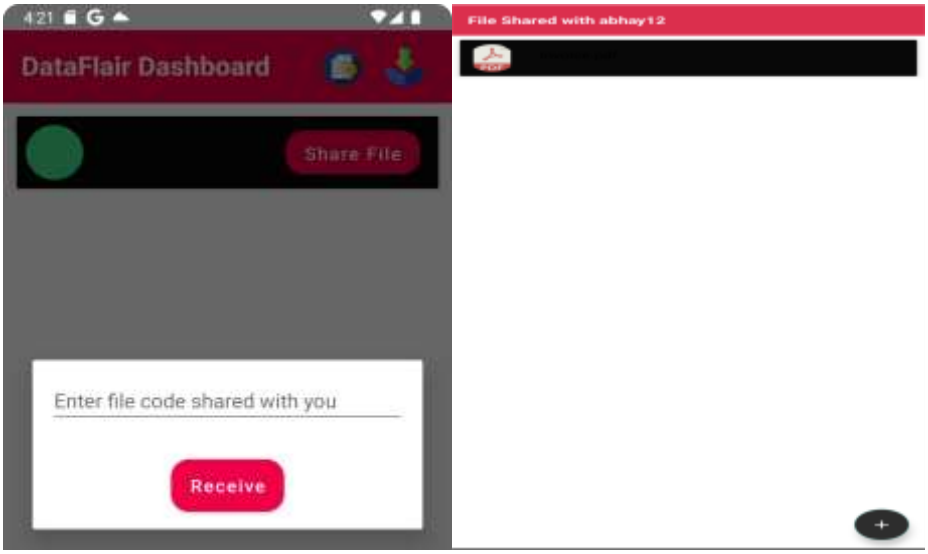

Figure 5: File Shared Dashboard

V. CONCLUSION

In conclusion, this research paper presents a comprehensive study of a secure file sharing Android application that employs AES and DES encryption algorithms and utilizes Firebase for storage and authentication. The proposed solution aims to address the growing concerns surrounding data security and privacy in file sharing scenarios. The paper provides valuable insights into the implementation, security considerations, and performance evaluation of the application, highlighting its potential as a robust solution for secure file sharing on Android devices.

VI. REFERENCES

[1] M. Butler, "Android: Changing the mobile landscape", Pervasive Computing, IEEE, Vol. 10, pp. 4–7, March 2011.

[2] A. Alexander, "Smart phone usage statistics and Trends 2013", February, 2013 [Online]. Available: http://ansonalex.com/infographics/smartphone-usage-statistics-andtrends-2013-infographic/ .

[3] Android Dev. Team. Android Developers. Website. http://developer.android.coml. [Accessed: January 15,2013].

[4] Java,https://en.wikipedia.org/wiki/Java_(programming_language).[Accessed: January 22 2013].

[5] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and V.W. Freeh. Taming Information-Stealing Smartphone Applications (on Android). In Proc. TRUST 2011, 2011. to be published.

[6] Prince, E. B., & Bakon, K. A. (2016). A Study on The Need to Implement a Courier ServiceApplication on Android Smartphones. International Journal of Information System and Engineering, 4(2).

[7] Ezeofor C. and Ulasi A.G. (2014), 'Analysis of Network Data Encryption & Decryption Techniques in Communication systems', International Journal of Innovative Research in Science, Engineering and Technology, ISSN.

[8] A Review Paper On Cryptography (https://www.researchgate.net/publication/3344185).

[9] Mr. Gajanan N. Tikhe, Mr. Yogadhar Pandey, "A Secure Scheme to Avoid Worm hole Attacks in Ant based Adaptive Multicast Routing protocol for MANET", IFRSA's INTERNATIONAL JOURNAL OF COMPUTING (IIJC) Volume 2, Issue 1, ISSN (Print):2231:2153, ISSN (Online):2230:9039, Jan 2012.

[10] Mahalle, V.S. and Shahade, A.K., 2014, October. Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146- 149). IEEE.

[11] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies. Swatee Pachaghare and Prof. Pragti Patil. Improving Authentication and Data Sharing Capabilities of Cloud using a Fusion of Kerberos and TTL-based Group Sharing. Institute of Electrical and Electronics Engineers.2020