Android Video Encryption and Sharing

[1]Rishidharan B, [2]Pradeep C, [3] Ajay P

[1,2,3]Student
[123]Information Security and Digital Forensics,
[1]Dr.M.G.R. Educational and Research Institute, Chennai-600095, India

Abstract: Multimedia data security is becoming important with the continuous increase of digital communications on the internet. The encryption algorithms developed to secure text data are not suitable for multimedia application because of the large data size and real time constraint. The technology has improved a lot in the field of Video sharing, the market trends and advancement in video techniques are growing rapidly nowadays. While sharing video through a network there are many risks in security. Since a more number of searching steps are required to obtain the desired results from the Internet sources. To avoid malicious applications we are designing and developing an application which provides security for transferring the data, it encrypts and decrypts the data to maintain the security. This system "Android video encryption" overcomes this problem and provides users the better opportunity to share the desired information and to scale up with upcoming market trends and technologies in a user-friendly manner. Android video encryption is actually an android application, which shares the video through any online network, through which the users have assurance of their video. The focus is on developing an android application for secure sharing of video through the internet. This can help people to share video easily through network architecture, since this system uses the AES algorithm and Blowfish encryption technique to ensure security.

Keywords: Encryption, Android, Video

INTRODUCTION

The growing popularity of digital images and videos in various applications has highlighted the need for enhanced security and privacy measures. With an increasing number of Android phones being activated every day, a large volume of videos are being shared among users. To protect this data, encryption algorithms such as DES and RSA are being widely used for text and binary data. However, these algorithms may not be suitable for videos, as they often have large volumes of data and require real-time processing. The "Android video encryption and sharing " project is similar in functionality to the YouTube application, allowing users to upload and store source videos in an encrypted database using AES and Blowfish algorithms. These videos can then be decrypted using the same algorithms.

PURPOSE

The objective of video encryption initiatives is to safeguard the security and confidentiality of digital video content. Videos frequently contain confidential or private information, and it is crucial to secure this data from unauthorized access, theft, or misuse. Encryption transforms regular text into encrypted text, making it challenging for unauthorized individuals to read the original information. In this project, the source video is transformed using encryption algorithms such as AES or Blowfish, and stored in a database. This helps to secure the data from being accessed or stolen by unauthorized parties, even if the database is hacked. Furthermore, encryption ensures that the video information remains private and cannot be viewed or used by unauthorized parties, thereby preserving the privacy rights of the video owner.

EXISTING SYSTEM

Before the development of the Android video encryption app using AES and Blowfish algorithms, the existing system for encrypting videos on Android devices was limited. The following are the limitations of the existing system:

1. Lack of Security: The existing system for encrypting videos on Android devices did not provide adequate security for sensitive video content. Videos could be easily intercepted and decrypted without proper encryption.
   Inefficient Encryption: The existing system for encrypting videos was slow and inefficient, making it unsuitable for large video files.
2. Limited Encryption Options: The existing system offered limited encryption options, with only a few encryption algorithms available for use.
3. User-unfriendly: The existing system was difficult to use, with a complex interface that was not user-friendly.

LITERATURE SURVEY

This section is dedicated for some papers related to video encryption algorithms and the improvement or modification on it.

- "Performance of encryption techniques for real time video streaming" published in 2009 in IEEE proposes. The idea of this paper is based on this system of three data types are encrypted that are text, video, audio using AES algorithm.[1]
- "Video encryption using AES algorithm" in 2014, This paper adds information about the system which include encryption, authentication, and digital signatures.[2] For video, the method has been adopted to protect unwanted interception and viewing of any video while in transmission over the over the networks using AES. Using only AES is not much secure from brute force attack. [2]
- "To provide security to MPEG video using MAES, AES, AES and MAES algorithms are used". This paper states that they have proposed their work in "Modified AES Based Algorithm for MPEG Video Encryption" in 2014 IEEE publication.[3]

- "Encryption using two algorithms" in 2014. In this paper the authors described the technique to encrypt the data and messages in mobile devices transmitted over network .This technique is developed under android platform and used two algorithms for encryption data , the first used symmetric AES and the second used asymmetric ECC , in sender and receiver sides are used the appropriate keys for encryption and decryption of the data .and he claims the system are achieving confidentiality ,authenticity ,and integrity of massage and data.[4]
- "Video Encryption Using AES Algorithm" in 2014. This paper used Advanced Encryption Standard (AES) Algorithm for Video encryption. AES algorithm is also compared with a modified algorithm of the Data Encryption Standard (DES). The results referred that encryption and decryption time in AES is better.[5]
- "A Modified AES for Mobile Devices" in 2015. This thesis modified the AES to encrypt data mobile phone. He takes different cases to show result of system between classical AES and modified AES in terms of computational complexity and security. The platform used in mobile and programming language is the Android Studio. The author claims the adjust AES encryption algorithms have many advantages which are; robust encryption, fast encryption and decryption process, and easy implementation.[6]
- "Video Frame Encryption Algorithm using AES" in 2016, their methodology focuses on security and privacy of digital video. They have used mpeg video compression, encryption and decryption technique. These proposed in IJERT about this system needs some improvement, as AES alone is not much secure now-a-days.[7]

PROPOSED SYSTEM

In this app the user can select a video and encrypt the video file and upload the encrypted file in the form of cipher text in the server. By uploading the encrypted videos the user can share the video by clicking my list in the app the he can select a video and he can share the encrypted video file to other users then the other user can decrypt the video by clicking the cipher text.

System Architecture

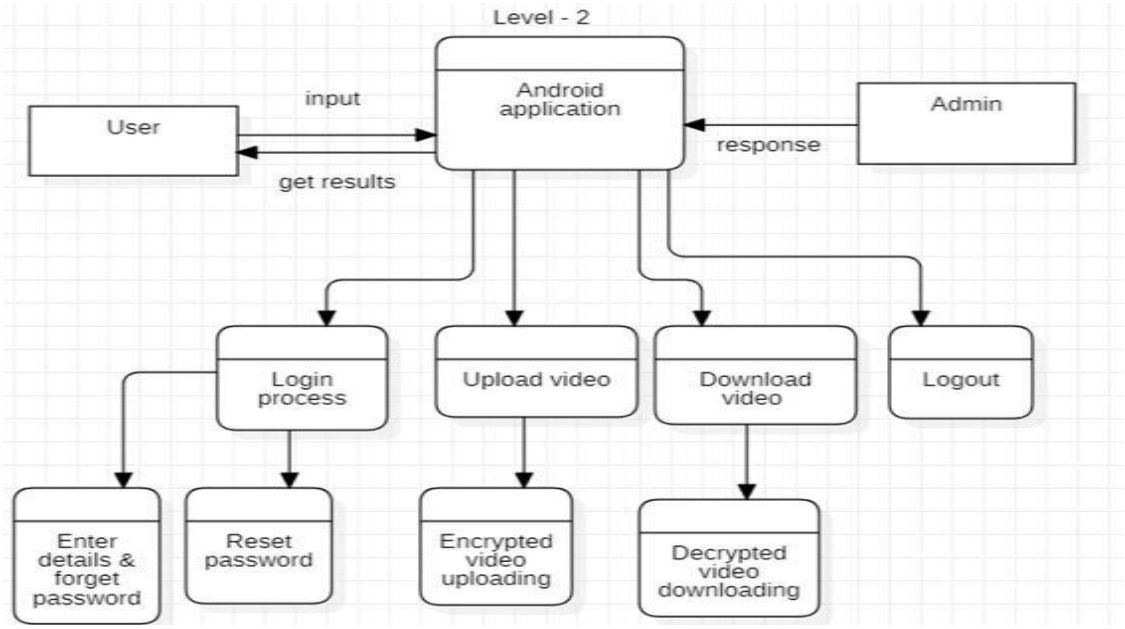

Fig: 1 System Architecture

METHODOLOGY

Uploading the video:

Upon successfully logging in or completing the registration process, the user will have the option to choose a video file from their device and upload it or share it with others. The video will then be transformed into a series of bytes and saved in a document format, providing a secure digital storage solution for the video.

Fig: 2 Uploading the Video

Division of video file:

In Java, the split function is utilized to segment a file into two components, streamlining the encryption process. When it comes time to decrypt the file, the steps are reversed, and the two pieces are merged back together and converted into the video format.

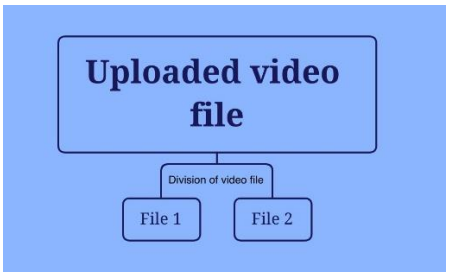

Fig: 3 Division of video files

Encryption Process:

The encryption process involves two distinct algorithms, AES and Blowfish. The video is split in half, with one portion being encrypted using AES and the other portion using Blowfish. In order to use Blowfish, the input must be in byte format, so it is converted accordingly. The AES algorithm uses a block size of 128 bits and a key size of 192 bits, while the Blowfish algorithm uses a block size of 64 bits and a key size of 192 bits. These keys are securely stored in a database, with the Firebase database being used for this purpose.

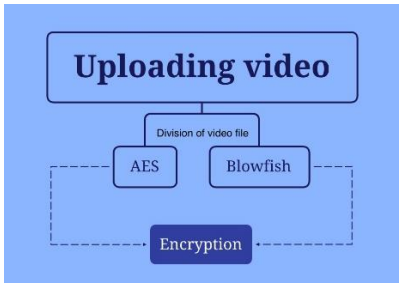

Fig: 4 Encryption Process

Storing the encrypted file into database:

Following the encryption process, the video data is securely deposited into a database for safekeeping. This information, now in a encrypted format, can be easily retrieved and accessed at a later time.

Decryption Process:

The decryption process involves undoing the steps taken during the encryption phase. Firstly, the encrypted video data that was stored in the database is retrieved. The Ciphertext is then processed through the Blowfish algorithm using the same key as before, transforming it back into its original format. The next step is to pass the newly decrypted data through the AES algorithm using the key that was used in the initial encryption. This process is repeated until the entire video is decrypted and the user is able to download the combined and fully restored video.

ADVANTAGE OF PROPOSED SYSTEM

- Easy to use.
- User Friendly application.
- Encryption and decryption process takes less time compared to the existing system.
- Multilevel algorithms makes it harder to crack even if the data got intercepted

CONCLUSION

Although an important and rich variety of video encryption algorithms have been used, most of the algorithms defined are not completely secured. This application allows users to send files or data in the video format to other android devices in a secure network. In this way, applications can still access the data without reaching for the user's sensitive information.

REFERENCES

1. Wail S. Elkilani, Hatem M. Abdul-Kader says in their work “Performance of encryption techniques for real time video streaming” published in 2009 in IEEE proposes. In this system three data types are encrypted that are text, video, audio using AES algorithm.
2. Dhananjay M. Dumbere, Nitin J. Janwe worked on development of encryption technique. In their proposed work “Video encryption using AES algorithm” published in IEEE in 2014 they mentioned that these system include encryption, authentication, and digital signatures.[4] For video, the method has been adopted to protect unwanted interception and viewing of any video while in transmission over the over the networks using AES. Using only AES is not much secure from brute force attack.
3. Ms. Pooja Deshmukh, Ms. Vaishali Kolhe says, “To provide security to MPEG video using MAES, AES, AES and MAES algorithms are used.” They have proposed their work in “Modified AES Based Algorithm for MPEG Video Encryption” in 2014 IEEE publication.
4. N.Mayur, S.Avinash, B.Pratik, and M. Chetan, “Secure and Reliable Data Transfer on Android Mobiles Using AES and ECC Algorithm,” International Journal of Innovative Technology & Adaptive Management (IJITAM) www.ijitam.org 2014[Online].Available:http://www.ijitam.org/d oc/ v11c4.pdf.
5. M. Dhananjay, J. Nitin , “ Video Encryption Using AES Algorithm,” In Proceedings of the IEEE International Conference on Current Trends in Engineering and Technology (ICCTET), pp.332- 337, 2014.
6. F. Hadi, “A Modified AES for Mobile Devices,” MSc thesis in Computer Sciences University of Technology, 2015.

7. Keshav S. Kadam, Prof. A.B.Deshmukh proposed “Video Frame Encryption Algorithm using AES” in 2016, their methodology focuses on security and privacy of digital video. They have used mpeg video compression, encryption and decryption technique. These proposed in IJERT about this system needs some improvement, as AES is not much secure now a days.
8. Ms NehaKhatri – Valmik and Prof. V. K Kshirsagar ,"Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83, Apr. 2014.