Videozen: Video Encryption and Decryption using AES and Blowfish

Tejaswini Sawant[1], Sagar Soni[2], Dhwani Tank[3], Dr. Dipti Patil[4]
[1,2,3]*Department of Computer Engineering, Universal College of Engineering, Mumbai, India*
[4]*Professor, Department of Computer Engineering, Universal College of Engineering, Mumbai, India*

Abstract **- 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 network there are many risks of insecurity. Since a more number of searching steps are required to obtain the desired results from the Internet sources.**

To avoid malicious application 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 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.

Index Terms **- Video encryption, Advanced Encryption Standard (AES) algorithm, Blowfish algorithm, encryption and decryption.**

I.INTRODUCTION

The wide use of digital images and videos in various applications brings serious attention to security and privacy issues today. There are so many android phones activating each day and through that phone's so many videos are shared to each other. So data encryption is a suitable method to protect the data. Till, now various encryption algorithms have been proposed and widely used like DES, RSA etc most of them are used for text and binary data. [2]

It is difficult to use them directly in video encryption as the data in videos maybe of large volumes many a times and it requires real time operations. The sharing and surfing of Real Time Video project is quite similar to YouTube application in some functionality. The source video is uploaded by the user itself which undergoes through various process which takes care of video security. In this system, video will be saved in encrypted form and stored in database. Encryption in form of AES and Blowfish algorithm and decrypted also in the same form.

II.LITERATURE REVIEW

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]

III.METHODOLOGY

A. Uploading the video file:

After login / registering user needs to select the video file from their feed and upload it or can share which they want to share. This video will be converted into bytes and stored in document format.

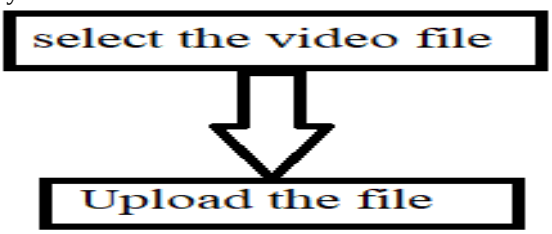

Fig: 1 Upload the file in Videozen

B. Division of file:

Using split function in java we have divide the file into two parts, for the ease of encryption process. While in decryption, this whole process is followed in reversed and the whole file is combined together and convert to video format.

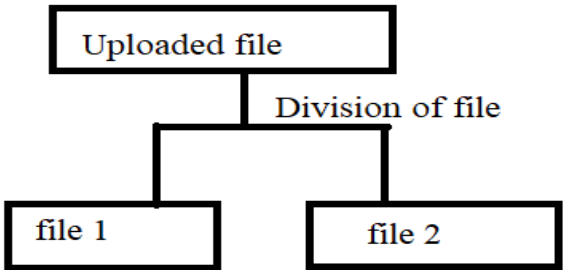

Fig: 2 Division of video files.

C. Encrypting Process:

The encryption process undergoes two different algorithms that is AES and Blowfish. The first half of the video undergoes into AES and other part of the video undergoes into Blowfish. As we know, blowfish accepts inputs in bytes format for this purpose we converted input in bytes format. We have used AES with block size of 128 bits and key size for AES is 192 bits and for blowfish block size is 64bits and key size is 192 bits. This keys are stored in database. Firebase database is used for storing the data.

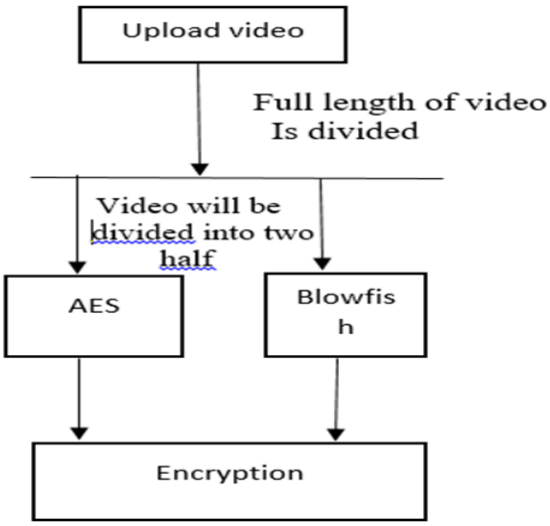

Fig: 3 Encrypting the video files

D. Storing this encrypted file into database:

The files or the data of the video format after the encryption process are stored into the database.

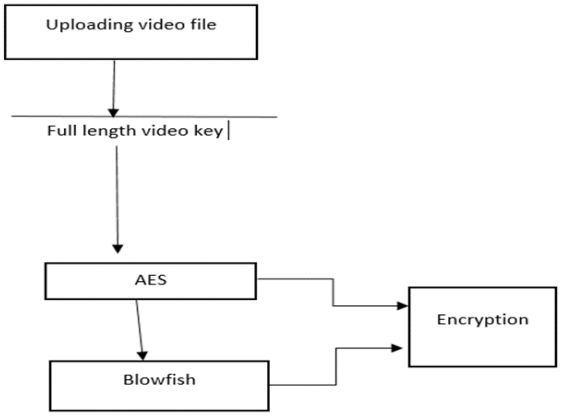

Fig: 4 Storing the file in database

E. Decryption Process:

After the encryption process, the divided parts of the video are combined together to make to bring back the video into the original length. The reverse process of the encryption is carried out for decryption. In Decryption, the whole process is followed in reverse order. Initially, the Ciphertext is passed through Blowfish algorithm in bytes format using the same key. Then, that file is passed through AES algorithm using the key of AES which was used initially for encrypting the file. Then this file is divided in two parts among which one is passed through AES and Blowfish algorithm. After this whole decryption process the Users can download the whole combined video.

IV.SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure behavior and more views of the system, organizing in the way that supports reasoning about the structure of the system which comprise the system components the relationship between them and provides a plan for which product can be produced and the system developed that will work together to implement overall system. The fig. 5 is the architecture diagram of the Android application. The inputs are in the form of video through user interface in the form of normal video or we can say plaintext. Video can be of any size. The user interface receives the video and then forwards it to the main process of encryption in application. Before encryption it is converted into text file format and then passed for division, further process. In this application, in 1st stage the text file undergoes the process of division followed by encryption. Preprocessing steps include video encryption using AES algorithm and blowfish algorithm and key of same size. Here video is divided into two parts, where one part is encrypted using AES algorithm with key and another is encrypted using Blowfish algorithm with their key. This generates a text file which is stored on server.

In 2nd stage whole file is combined and again passed from AES and then from blowfish for encryption whose ciphertext is stored in database. Ciphertext is generated this generated CP encrypts by using Blowfish algorithm. Text file is generated after this, which is stored in server. Decryption is the reverse process of encryption where all the process are repeated. application (Videozen). For decryption the whole steps is followed in reverse order, where the ciphertext is passed through the blowfish using the same key.

The user needs to create their account.

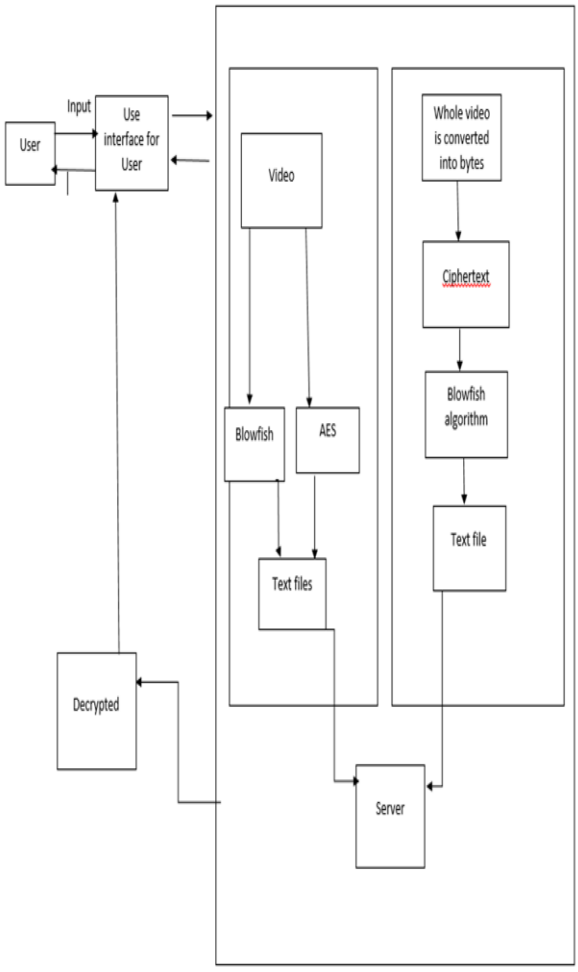

Fig: 5 System Architecture

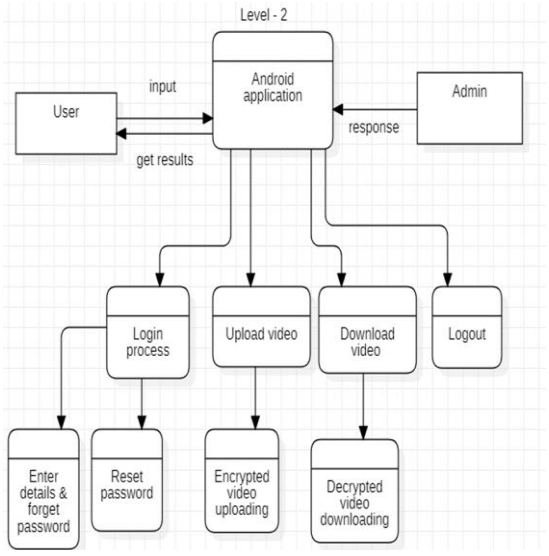

Fig: 6 Data flow diagram

V.ALGORITHMS USED

We are using a combination of AES and Blowfish algorithms for more security reasons.

- AES:

The Advanced Encryption Standard (AES) is a symmetric block cipher used to protect the classified information in the system. It includes three block ciphers: AES-128, AES-192 and AES 256. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES-256 a 256-bit key length to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.[4][5][7]

Symmetric, also known as secret key, ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know and use the same secret key. The government classifies information in three categories:

Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths. Round varies according to key size. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final

output of ciphertext. [2][3][7]

- Blowfish

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. It is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. It works with keys up to 448 bits in length.[8]

VI.RESULT

	AES	Blowfish	Combination (AES + Blowfish)
Speed	Slow in speed	Faster	Faster in speed when both used combinedly.
Time	Less time	More time	Takes less time for small size video encryption.
Security	Security is depends on key size	In this also, security depends on key size. If we are using bigger size key then it is more secured.	In our combination if we are using key of less size for the algorithms, then also it provides more security and not vulnerable to any types of attacks.
Key size	128- 256 bits	64 -448 bits	AES – 192 bits, Blowfish – 128 bits
Structure	Substitution and permutation	Feistel	Substitution & permutation + Feistel
No. of rounds	10	16	Combination (10 + 16)
Complexity	Less complex	More complex	More complex makes it more secure.

VII.CONCLUSION

In this paper, we have proposed a methodology where by using the two algorithms AES [2][3][5][6][7] and Blowfish [8] by integrating them and implemented an attempt to present a video encryption sharing

application for the Android based mobile devices. 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 file or data in the video format to other android devices in a secure network. In this way, application can still access the data without reaching for user's sensitive information. This application can be useful in many real time events and applications for an enhanced user support. It is observed that the decryption process takes more time relatively as compared with the encryption process, which is acceptable because of the nature of the algorithms besides this the algorithms are implemented in limited resources.

The main advantage of this system is achieving the protection for data of video in android devices such as confidentiality for the secure end-to-end user communication and for simple user interface so that it is easy for users to interact.

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/doc/ 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.