International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Secure Sharing and Searching of Video Data

Dipali S.Yadav[1], Prof. Kanchan K. Doke[2]
[2]*Professor* ,[1,2]*Department of Computer Engineering, BVCOE, Navi Mumbai*

Abstract: Social networking has become a part of daily life of every smart phone user. Sharing real time images and videos produces huge amount of traffic as well as data every day. Tremendous amount of video data is stored and shared through multiple web and mobile application. This has given the rise to the need of secure infrastructure to store and share the user's private videos. The proposed infrastructure that allows mobile user to securely share and search their real time video data by encrypting the data before uploading. So that, security issues like video leakage, etc. can be prevented. The mobile users can be able to share their real-time video through the cloud and only the authenticated user can get access to the shared videos. Any user who does not have rights to access the video will not be able to get any information about the video. It also allows secure searching within users own data. The access of shared video can be removed which can be used to recover the human errors which occurs while sharing the video. The security of video data is guaranteed even if the storage is hacked.

I. INTRODUCTION

The universality of mobile applications and devices has been part of the new market, which enables mobile developers to provide new services for their users. Data feeds and services in the cloud are also part of success of mobile application, and hence it leads to the notion of mobile cloud computing. The demand for the transfer of huge amounts of data will need to be supported by rapid data transfer, which will make the application very usable and hence, leads to enhance the user's experience. Sharing images and videos is becoming easier and faster each passing day. Currently, amount of images shared is much more than the amount of videos shared, due to high transfer speed required for video data. But, due to origination of 4G and 5G the demand for video sharing will increase. Increases in the transfer rate of video will also leads to increase in the amount of video data stored and shared over cloud. Higher connection speed will allow users to share large amount of video data in very short time. While dealing with the cloud, major security issues related to cloud will arise. Storing video on cloud can lead to unauthorized access and leakage of private data. Thus an infrastructure will be required for secure storing and sharing of the video data [1].

Consider a futuristic, yet very practical and realistic, scenario as follows. Bob, who is a U.S. senator, is taking a vacation with his work colleagues. But unfortunately, since he has a young family member, they do not join him on the trip. Nevertheless, Bob would like to share his experiences with his family members. To do so, Bob is equipped with a high definition and versatile camera, which he uses throughout his trip (during skiing, diving, etc.). After the scene has been recorded, it will be uploaded to the cloud via the internet, and hence having a high definition video is possible. Bob's family members, having access to the right applications and the credentials, can access within the encrypted video collections provided by Bob. As the video scenes contain some parts that Bob does not want to share with any outsiders, leaking even the keywords will be disastrous, due to Bob's reputation in the public

The proposed infrastructure that allows mobile users to securely share and search for real-time video data. Mobile users can create a set of people with whom they want to share (e.g. friends, family members). Users outside this set cannot obtain permission to access the file, or even receive any information (e.g. keywords) about the video data. We use some cryptographic primitives as the building blocks. Therefore, the security is guaranteed even if the cloud server is hacked or the video data is stolen. In addition, we also provide secure searching within video data.

II. LITERATURE REVIEW

A. *MayankArya, Chandra RavindraPurwar, NavinRajpal, "A Novel Approach of Digital Video Encryption"*
They propose a new novel scheme for digital video encryption. They represent a method to generate an encrypted video by encrypted Video-frame. Based on novel secure video scheme, an effective and generalized scheme of video encryption. It is a matrix computation scheme which uses a concept of Video-frame and xor operation.[2] Throughput and security is less in this method.

B. *AmanChadha, Sushmit Malik, AnkitChadha, RavdeepJohar, M.ManiRoja "Dual-Layer Video Encryption using RSA Algorithm".*

They proposes a video encryption algorithm using RSA and Pseudo Noise (PN) sequence, aimed at applications requiring sensitive video information transfers The audio and video components of the source separately undergo two layers of encryption to ensure a reasonable level of security. Encryption of the video component involves applying the RSA algorithm followed by the PN-based encryption. Similarly, the audio component is first encrypted using PN and further subjected to encryption using the Discrete Cosine Transform. Throughput is less in this method and memory usage is high.[3]

C. *Renle Huang, Chenyue Lu, "Research of H.264 Video Transmission Encryption Technology Based on Blowfish Algorithm"*
They put forward a H.264 video transmission encryption technology based on Blowfish algorithm. [4] Security is comparatively is less.

D. *Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study".*
they proposed algorithm that shuffles the video frames along with the audio, and then AES is used to selectively encrypt the sensitive video codewords. Using this approach unauthorized viewing of the video file can be prevented and hence this algorithm provides a high level of security. They provide less throughput.[5]

III. CHALLENGES IN EXISTING PLATFORM

Although there are some existing platforms for sharing real-time video, they may not be able to achieve secure fine grained sharing and secure searching simultaneously. These two important functions are very important to users who deal with large volume of data (e.g. large video), which will emerge in the 5G era. Thus we need to have a new infrastructure to provide secure sharing and searching for large real-time data (such as video).

IV. NETWORK INFRASTRUCTURE

The overview of our network infrastructure, as illustrated in Fig. [1], where a mobile user is connected with an external video-taking device (e.g. GoPro (gopro.com)) through WiFi, and the mobile device is connected through internet with a cloud server with purposes of storage and sharing. Our security mechanisms will be built on top of this network infrastructure [2-4]

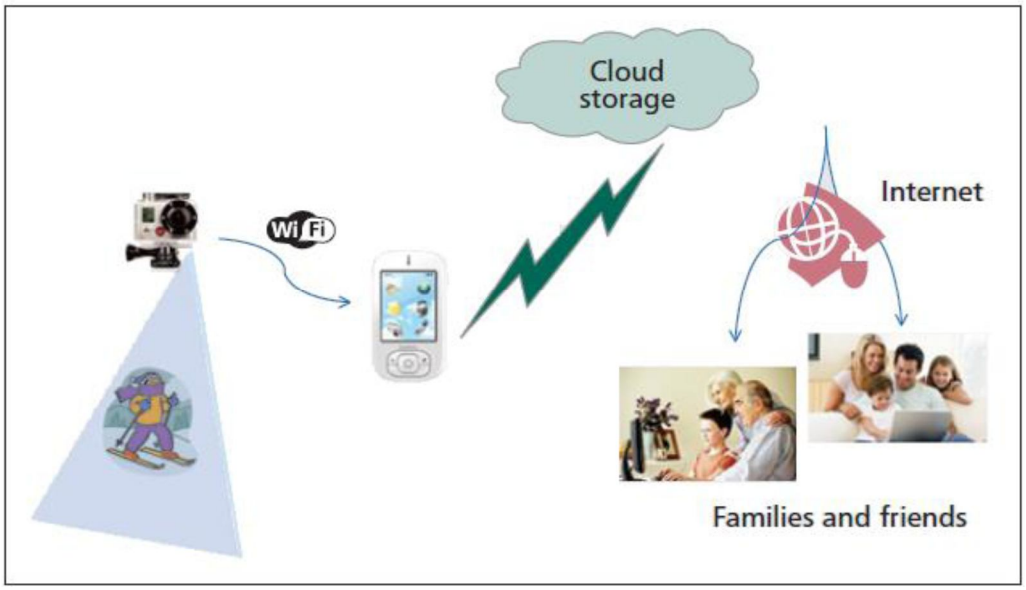

Fig. 1 Network Infrastructure

A. *Advanced Encryption Standard [AES]*
AES is a block cipher symmetric algorithm with block length 128 bits and key lengths of 128, 192 or 256. The key size of the algorithm depends on the number of rounds in algorithm
This is the most commonly used symmetric encryption scheme. In an AES encryption system, a user first generates a key AES. key (which is used to encrypt or decrypt video), and next runs an AES encryption algorithm AES.C ¨ AES.Enc(AES.key, m) with the

key AES.key to encrypt a exactly half video data m and get a ciphertext AES.C. By using the same key, the user can recover the video from its encrypted format via a decryption.[6-8]

B. Blowfish Algorithm

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. The size of block is 64 bits and the key lies at any length up to 448 bits. Encryption is done through 16-rounds. Each round performs an permutation depending on key and substitution depending on data using XOR operation and addition on 32bit words. In this user uses blowfish to encrypt the exactly half part of video data and recover data using decryption

In proposed system, our aim is to develop an application and provide user an infrastructure which will allow user to store and share their video data securely on the cloud. The video data is stored in encrypted format, which ensures security even in case the server is hacked.[9-10]

Proposed infrastructure allows user to store and share the video over cloud using smart phone. After shooting a video, user can upload the video on to the cloud using the application on smart phone. After Uploading, the application encrypts the video data to the cloud. Thus the video data which is uploaded is already in encrypted format. Blowfish algorithm and AES is used to encrypt the video data. After the encryption, the enciphered video data is stored on the cloud. Storing the enciphered data ensures more security than storing actual video data and securing with password protected account.

V. IMPLEMENTATION

A. User Registration

User first register with credentials used for authentication later. Then validate user based on stored credentials during registration

B. Video Upload

After using an external camera device to take a video, it is transferred to the user's mobile device via Wi-Fi. It uses AES and blowfish both algorithm to encrypt the video data. The details of the Upload are described below.

1) The video are divided in to 2 equal parts.
2) The first part is converted in to file format for encryption and it is encrypted with AES algorithm.
3) Second part is also converted in to file format for encryption and it is encrypted with blowfish algorithm.

After it combine both the part, one is encrypted with blowfish and other is encrypted with AES, and upload the encrypted video to the cloud and stores the whole video in encrypted format in to cloud database.

C. View List

It will show all the video presented in database. Following three actions can be performed on this.

1) *Download:* user can download his uploaded video from cloud directly he details of the Download are described below.
a) Cloud retrieve the two part of video from database
b) Download the file on mobile device.
c) Decrypt the first part using blowfish decryption algorithm.
d) Decrypt second part using AES decryption algorithm.
e) Combine both part to form original video file.
f) Video file is available on mobile on mobile
2) *Sharing:* If the video owner wants to share one of his/her videos with their friends or another set of people.
3) *Delete Access:* we can remove access of the user with whom we have shared the video. User first login then it search for a video in view list, then it select video and then select the recipient whose access he want to remove.

D. Shared

It will show all the video which is shared with user by some other user.

1) User first login and open View shared list. It will contain all videos, which is shared by other with user.
2) User then select the particular video which he want to download and video is downloaded on user's mobile.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

VI. RESULTS

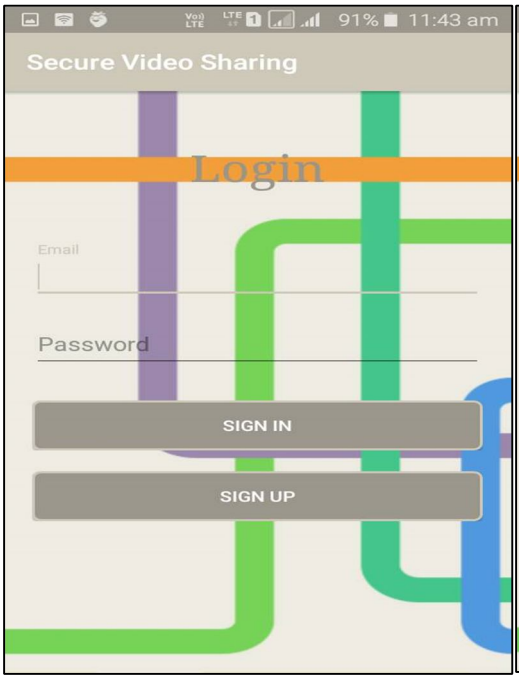

Fig 2: Login Page

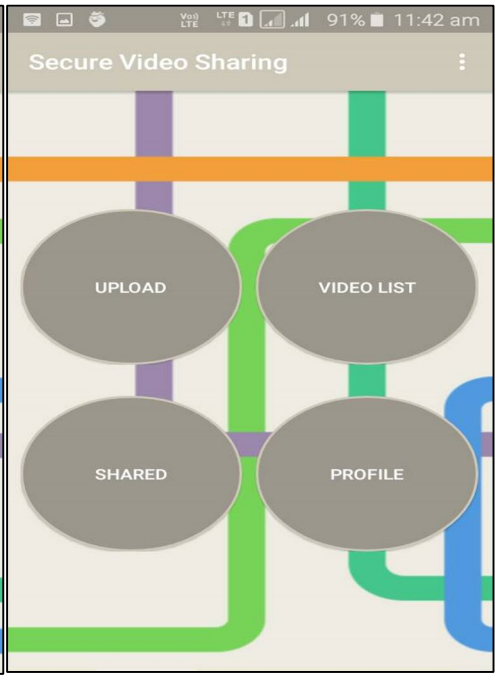

Fig 3: Home Screen

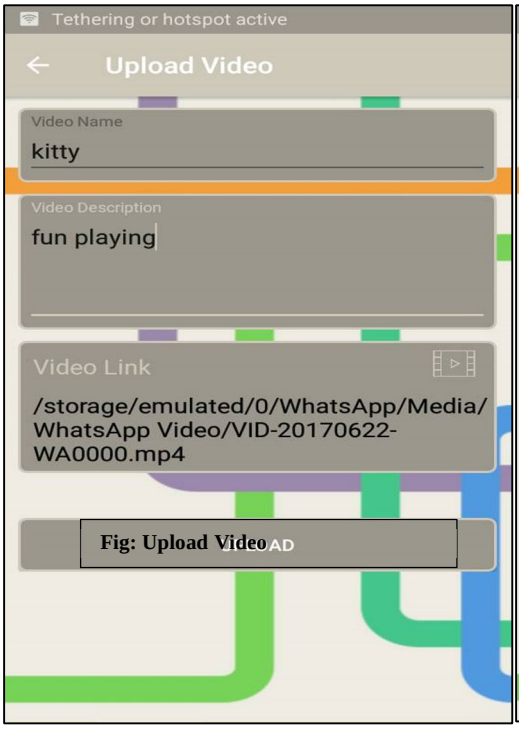

Fig 4: Upload Video

Fig 5: Video Upload Result

Fig: Upload Video

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

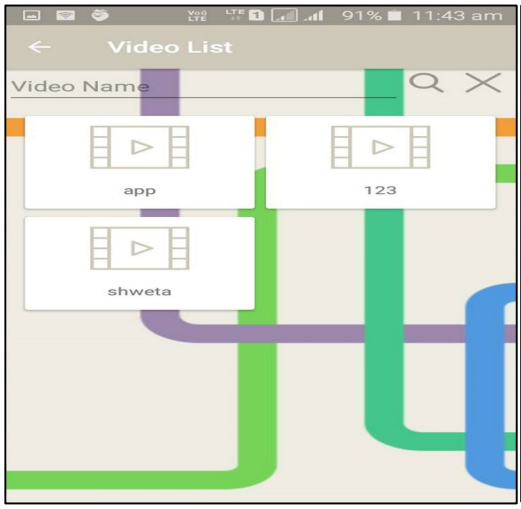

Fig 6: Video List

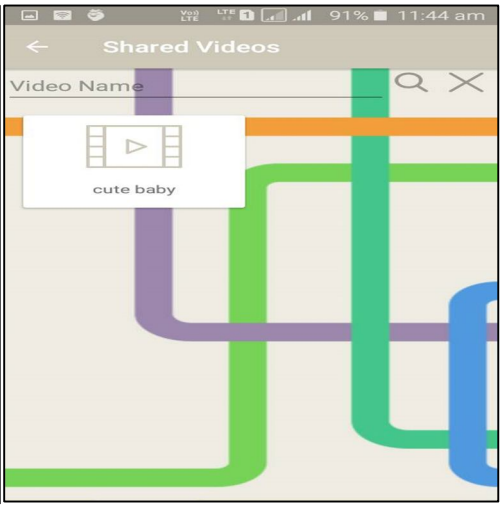

Fig 7: Shared Video

Fig 8: Sharing and Deleting Video

Table 1. Encryption Time Table

Video Size (MB)	Half AES +half blowfish			Dual Layer with AES and Blowfish
	AES	BLOWFISH	TOTAL	
2	121	413	534	1175
3	237	445	684	1608
4	265	898	1163	2846
5.4	570	1253	1723	4446

Table 2. Decryption Time Table

Video Size (MB)	Half AES +half blowfish			Dual Layer with AES and Blowfish
	AES	BLOWFISH	TOTAL	
2	213	295	508	988
3	415	592	1007	2048
4	522	763	1285	2699
5.4	728	1669	2397	7597

VII. CONCLUSION

Proposed infrastructure allows mobile users to store and share their video data securely over cloud. User can securely share their videos in encrypted format with other users. The infrastructure is secure from eavesdrop attack. Even if attacker is able to get access to video, he will not be able to watch it as the video will be in encrypted format. Security is guaranteed even in case the cloud storage is hacked, as the video data present on the cloud will be in encrypted format.

In the next major phase of telecommunication standard i.e. 5G, video data of large size could be transferred in very less time, due to larger bandwidth availability. More algorithms and combinations of different algorithms and techniques can be added to overcome security risks in mobile cloud computing.

REFERENCES

[1] Joseph K. Liu, Man Ho Au, Willy Susilo, Kaitai Liang, Rongxing Lu, and Bala Srinivasan, "Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud" , IEEE March/April 2015.
[2] MayankArya, Chandra RavindraPurwar, NavinRajpal, "A Novel Approach of Digital Video Encryption" International Journal of Computer Applications (0975 – 8887) Volume 49– No.4, July 2012
[3] Aman Chadha, Sushmit Malik, Ankit Chadha, RavdeepJohar, M.ManiRoja "Dual-Layer Video Encryption using RSA Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015
[4] Renle Huang, Chenyue Lu, "Research of H.264 Video Transmission Encryption Technology Based on Blowfish Algorithm" 2015 4th International Conference on Computer Science and Network Technology (ICCSNT 2015).
[5] Ajay Kulkarni, SaurabhKulkarni, KetkiHaridas, Aniket More " Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study" International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013.
[6] Alahmadi et al., "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard," IEEE Trans. Inf. Forens. Security, vol. 9, no. 5, 2014, pp. 772–81.
[7] Dhananjay M. Dumbere, Nitin J. Janwe, "Video Encryption using AES Algorithm" ICCTET'14.
[8] United States National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, 2001.
[9] Avinash M Ghorpade, Harshavardhan Talwar , " The Blowfish Algorithm Simplified " IJAREEIE volume 5, Issue 4, April 2016.
[10] Ajay kulkarni, saurabhkulkarni, ketkiharidas, aniket more, "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study" International Journal Of Computer Applications, Volume 65- No 1, March 2013.