Providing Security for Storing and Sharing Video Data in Cloud

Prayas Gajbhiye
ME Student, Department of Computer Engineering
Dhole Patil College of Engineering,
Pune, India
Email: prayasgajbhiye09@gmail.com

Arati Dandavate
Head of Department, Dept. of Computer Engineering,
Dhole Patil College of Engineering,
Pune, India
Email: aratidk@gmail.com

***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. In this paper, we propose an infrastructure which allows users to store and share their video data securely over cloud. 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. The security of video data is guaranteed even if the storage is hacked.

Keywords-*secure Encryption, Video upload, Video Sharing, Secure Storage*

*****

I. INTRODUCTION

The launch of Apple's iPhone and App Store in 2008 and then the boom in android market has seen the rise in use of mobile devices and applications. The services provided by cloud have also played a huge role in success of mobile applications. 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, with the inception of 4G and 5G [2, 3], the demand for video sharing will increase. Increase in the transfer rate of video will also see the 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 less time. Incorporating 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.

In this paper we have proposed an infrastructure which allows user to share their video data securely over cloud using mobile application. The user with access rights will only be able to access the shared video. Any other user who does not have permission to access video will not be able to get any information about the video. Even if someone hacks the cloud server, the security is guaranteed as the video data is stored in encrypted format. If someone gets access to the encrypted videos, one cannot decrypt it since the key will not be in cloud. Thus the security is maintained for the video data throughout the life cycle.

II. LITERATURE REVIEW

Qiao and Nahrstedt [5] proposed The Video Encryption Algorithm (VEA) for securing video files which primarily focused on the selective encryption of I-frame. The algorithm includes the creating two indexed sequences of bits, odd and even sequenced bits. These two sequences are then operated with XOR operation. Any symmetric encryption methodology is then applied selectively to either the even sequence or the odd sequence. The sequence obtained by appending the sequence obtained by XOR operation and the enciphered sequence would be the enciphered data. The proposed Video Encryption Algorithm (VEA) is effective for low quality videos. It takes half time as that taken by naively applied methodology. But it consumes large amount of time for enciphering of high quality videos [6].

Wen et al [7] proposed an approach for selectively enciphering the video data. The data fields are distinguished into two parts. Data fields can be either be carrying information or not. The data fields carrying information can be of fixed length or variable length. Fields carrying information are only taken into account for encryption. The proposed approach then suggests applying different encryption methods, like DES, depending on length of fields, fixed or variable, while maintaining the format compliance. The proposed approach is effective but introduces some amount of overhead.

K C Ravishankar and M G Venkateshmurthy [8] proposed a method for region permutation. It scrambles various regions of the image based on symmetric key. It disorders the image and hampers the visibility of the image. Regions interchange the positions due to permutation. Though the algorithm distorts the image and introduces disorder, it is easy to trace back the original image if the key is known.

III. PROBLEM DEFINITION

Providing an infrastructure to ensure that the video data of user is securely stored and shared over cloud by adding an encryption layer between mobile application and cloud.

IV. IMPLEMENTATION DETAILS

A. *Proposed System Architecture*

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

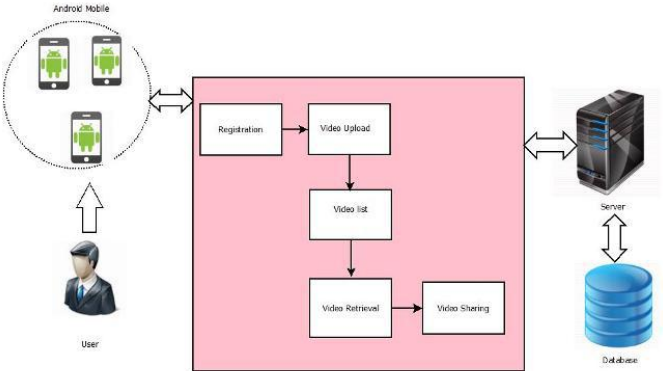

Figure 1. System Architecture

Any user who has a video and want to store it or share it with another user, he can do so using proposed infrastructure. Security is an important aspect in both the functionalities. 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.

The application encrypts the video data even before uploading on to the cloud. Thus the video data which is uploaded is already in encrypted format. 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.

User can share the uploaded video with other users, using the application. The receiver also needs to have smart phone to be able to download and watch the video. The sender while uploading the video mentions the user with whom he wants to share the video. The notification is sent to the receiver along with the key. The receiver then can download the enciphered video data from cloud, decrypt the same using the shared key and watch the shared video.

B. *Mathematical Model*

System S = {Secure Sharing Video}

S = {S1, I, E, F, O}

S1 = {Secure sharing server}

I = {Plain video data}

E = {Encrypted video data}

F = Function

O = Output

d1 = *EncryptAES (I)*

d2 = *Upload (E)*

d3 = *Share (E)*

d4 = *Download (E)*

d5 = *DecryptAES (E)*

D = {d1,d2,d3,d4,d5}

To upload video

Input: I {Plain video data}

Output:

O1 = *EncryptAES (I)*

Upload (O1)

To download video

Input: E {Encrypted video data}

Output:

O1 = *Download (E)*

DecryptAES (O1)

V. RESULT

A. *Home Screen:*

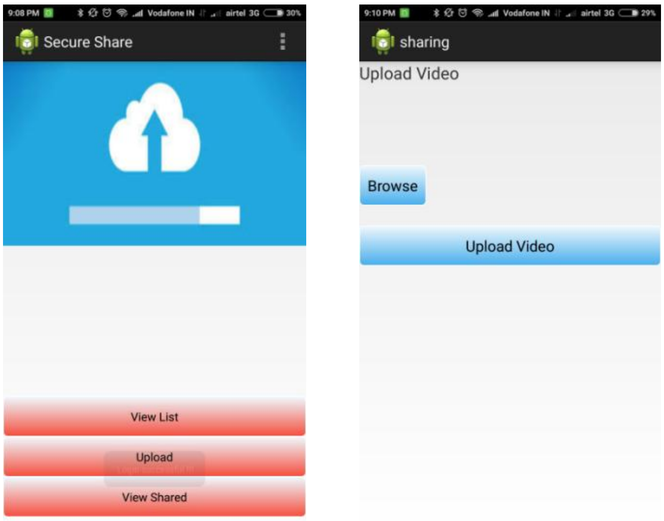

Figure 2. (a) Home Screen (b) Upload Screen

User sees the Home screen after successfully logging into application. He can choose to one of the following actions:

1. View list of uploaded videos
2. Upload new video from mobile
3. View list of videos shared with hi.

B. Upload Video

User can choose from the video to upload from his storage. The uploaded video will be then available for sharing with other users.

VI. CONCLUSION AND FUTURE SCOPE

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 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] CNET, “Ericsson Hits Crazy-Fast 5Gb/s Wireless Speed in 5G Trial,” http://www.cnet.com/news/ericsson-tests-out-crazy-fast-5-gbps-wirelessspeed/, July 2014.

[3] Computer Weekly, “Samsung Claims 5G Speed Record,” http://www.computerweekly.com/news/2240232676/Samsung-claims-5G-speed-record, Oct. 2014.

[4] United States National Institute of Standards and Technology (NIST), “Announcing the Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, 2001.

[5] L. Qiao and K. Nahrstedt, “A new algorithm for MPEG video encryption,” Proceedings of the 1st international conference on imaging science, systems and technology (CISST ’97), Las Vegas, NV, July 1997, pp. 21-29.

[6] C.-P. Wu and C.-C. Kuo, “Efficient multimedia encryption via entropy codec design,” Proceedings of SPIE security and watermarking of multimedia content III, Volume 4314, San Jose, CA, January 2001.

[7] J. Wen, M. Severa, W. Zeng, M. Luttrell, and W. Jin, “A format-complaint configurable encryption framework for access control of video,” IEEE Transactions of circuits and systems for video technology, Vol.12, No. 6, June 2002, pp.545-557.

[8] K C Ravishankar and M G Venkateshmurthy, “Pixel Compaction and Encryption for Secure Image Transmission”, National Conference on Intelligent Data Analytics and Pattern Discovery -2007, BIT Sathyamangalam, March 15-16, 2007