International Journal of Engineering & Technology, 7 (2.19) (2018) 94-96

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud Computing: Secure Transmission of High Definition Videos Using Cryptographic Approach

Anwar Basha.H [1*], S. Amrit Sai [2], Sanjnah.A [3], Srimathi.M [4]

[1]*assistant Professor*
Department Of Computer Science And Engineering
Srm Institute Of Science And Technology (Deemed To Be Universty), Vadapalani, Chennai, Tamil Nadu, Inida.

[2,3,4]*ug Scholar*
Department Of Computer Science And Engineering
Srm Institute Of Science And Technology (Deemed To Be Universty), Vadapalani, Chennai, Tamil Nadu, Inida.

** Anwarbasha.H@Vdp.Srmuniv.Ac.In*

Abstract

Cloud computing facilitates ubiquitous access to shared pool of configurable system resources and services over the Internet. Often due to shared access to this massive amount of data there is equal chances of risk. Transferring sensitive information in the form of text, audio or video, over the cloud one cannot guarantee the safety of the file. This paper assesses the effect of transmission of High Definition videos with the help of cloud-based servers that will improve the security of data being transmitted as well as enhance the quality of experience for end-users. We propose to share video contents to a selective group of people using the Time Domain Attribute based Access Control(TAAC) schema and generate keys using cryptographic method which gives the much needed protection to access these videos. Further stegnographic approaches are practised to maintain the data confidentiality.

Keywords: *Cloud computing, video content sharing, time-domain attribute-based access control (TAAC), watermarking, cryptography*

1. Introduction

It is a common practise to share a single file to a large number of people in any organisation. It takes lesser time for a text file to load compared to an image or a video file and it occurs due to the size of the file and quality. In order to ensure a smooth transmission of these files for a higher audience, cloud computing is chosen as a medium[1].
It offers storage, backup and a wide range of services which helps to virtually eliminate capital expenditure. As much as advantageous it is, there exists a certain of risk factors attached to it. Companies understand that data loss means a business is at risk. Even if a monetary value is not assigned to the data, the negative effects are significant. Often there is an underlying security issue, as to what if the supposed content lands in the hands of someone that is not authorised to view it. Privacy and security of data can exist only when the risk factors are analysed and can be prevented to some extent. Data security and accuracy should not compromise on the Quality of Experience for the end-users. A balance between the two is found as we propose cryptographic methods to protect the data, stegnography to copyright the data and (insert algorithm used to maintain the quality of the data).

2. Cloud Computing Overview

2.1 Introduction and Services offered by Cloud

Cloud computing delivers computing services such as setting up of hardware services, platform for developing software, maintenance of servers, storage and recovery of large amount of data, handling large set of databases, transmission of data, analysing data to extract patterns, hosting websites and blogs and streaming audios and videos. The major advantage of using cloud as a medium for transmission is to eliminate the capital expenses of buying hardware and software equipment, offers quick service on demand, sustain over latest generation of efficient hardware and ensures disaster recovery in case of data loss. We use different ways to deploy cloud computing resources. Public cloud which is owned and operated by a cloud service provider and manages all supporting infrastructure. In this case the security might get compromised. Hence the concept of private cloud is introduced where the resources are exclusively used by a single organization[2,5].

2.1 Data Security in Cloud

The worldwide cloud computing market is expected to grow to $191 billion by 2020, according to analyst firm Forrester, up from $91 billion in 2015, all within a matter of five years. The same firm has surveyed the major risk factor such as storing data without controls such as encryption, or lack of multi-factor authentication to access the service. An analysis has found that 21% of files uploaded to cloud-based file sharing services contain sensitive data including intellectual property, contracts and confidential details.

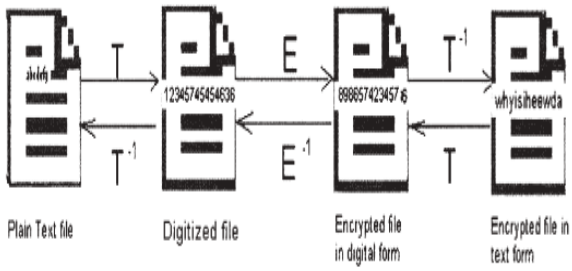

Fig 1 Data Security model in cloud

3. High Definition Videos Over Cloud

All over the world, everyday multiple videos are being uploaded and downloaded simultaneously. As of 2017 it is found that people now watch one billion hours of video per day. High Definition videos which offer greater resolution and quality than any normal videos take more time to load. To transfer the High Definition videos over the cloud, the data owners will upload the video in the cloud server for which a key will be generated and distributed to 'n' number of users. The security of the uploaded video is not guaranteed since a single key is used throughout the duration in which the video is present at the server. When the video contents are outsourced to the cloud, it is not easy to achieve the fine-grained access control. The data owners of the video contents will not be able to control their own data in the server. Due to this, the video becomes vulnerable to attacks. In this paper, we propose to introduce a factor which might reduce the lack of privacy. We upload the video in the cloud server which will generate multiple keys which will expire after a particular time period. A cryptographic approach ensures a provably secure time domain attribute based access control (TAAC) scheme, which holds the cipher text and keys, that only users who hold the sufficient information can decrypt the video[5].

Apart from securing the video, sensitive data are hidden through such videos. The existence of data is hidden as stegnographic methods are performed which is also frequently used as a digital watermark to determine if an image, video or audio is stolen. A combination of fragile and robust watermarking coupled with cocktail watermarking ensures that complementary roles are simultaneously embedded into the host file. We can also determine the worst likelihood that the better watermark among the two can be extracted. This ensures that the best outcome is always retained.

3.1 Existing System

In the existing system, cloud based video conferencing is done in order to enhance the quality of experience. To make sure that there is no buffering or delay during the process of video conferencing a number of servers and cloud Routers are used. A large number of servers and cloud routers and are erected in many places such that the increase in the amount of the users may not affect the quality of experience of the number of users. Here a limit is set to the number of users entering the server such that if the number of users exceed the limit the users are moved to the next server. This is done because if the number of users exceed the limit, the increase in the users will lead to the high traffic conditions leading to the buffering of the video during the video conferencing and there may be breakage in the pixels during the video conferencing and the quality of video will decrease due to it. To avoid all these conditions a large number of servers and cloud routers are used. Another major issue is that the security level is low and there may be some Data loss. To overcome this issue the cryptographic approach and the TAAC schema are used.

4. Proposed System

To improve the quality of video for the user, prevent the loss in the Data being transmitted over the cloud and to secure the data, the following system is proposed. In this System a 'n' number of servers are used and a certain limit is set to each server. When the server limit exceeds, the user is shifted to the next server and shifted back to the same if the number of users decrease in the former server. To prevent data leakage and enhance the security TAAC scheme, a Cryptographic approach (CP-ABE) and RSA is used for key generation process.

This System is categorised into the following modules:

1. Public Channel Creation
2. Secure Channel Creation
3. Division of video using TAAC scheme
4. Hiding of Data

PUBLIC CHANNEL CREATION: A public channel is created in the cloud for the transmission of video. Here the video is transmitted by the Data owner and any user can access the video with the use of a common Decryption Key and view it. The security level in this is low as a common key is used for the decryption process.

SECURE CHANNEL CREATION: In this module, a time section is created such that the key can be entered by the user within a specific time of key generation. When the user exceeds the time limit for entering the key the video cannot be viewed. This is done in order to enhance the security by protecting it from the attacks from unauthorised users and avoid data leakage.

DIVISION OF VIDEO USING TAAC SCHEME: Here, the video that is uploaded over the cloud is divided into N part. Keys are generated by using the random key generation (RSA). For N parts of the video, N keys are generated. The user provided with a certain key can only access one section of the video assigned for him to view. The user has to access the video using the key before a certain period of uploading the video else the key will expire and the user cannot access the video.

DATA HIDING: In data hiding, a video is encrypted and data's such as video, text or files are hidden in a video using a stegnographic approach. Watermarking is used for authentication and authorisation of the video.so the user with the certain key can decrypt the video or file and view it. Data is hidden in the video in order to prevent from the external attacks. Thus it helps in Data protection.

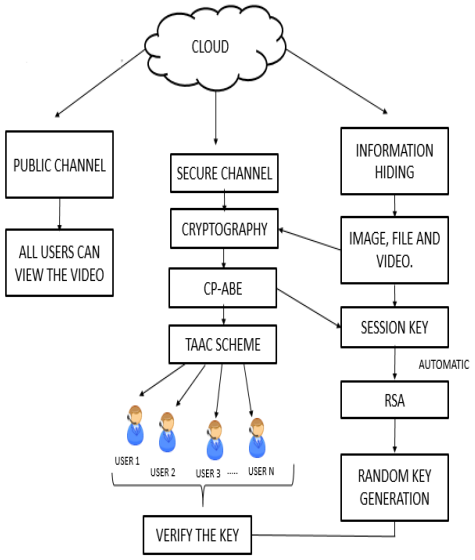

Fig 2.0 Proposed Model

5. Conclusion

In this paper we have improved the quality of experience of a video by using servers and also enhanced the security level by using the cryptographic approach and also reducing the data loss.

References

[1]. Richard Clegg, Raul Landa, David Griffin, Miguel Rio, Peter Hughes, Ian Kegel, Tim Stevens, Peter Pietzuch, Doug Williams, "Faces In The Cloud", 2017, pp:1-1

[2]. Chun-Shien Lu, H.Y.M.Liao, "Multipurpose Watermarking For Image Authentication And Protection", 2001, pp: 1579-1592.

[3]. E.I.Lin, A.M.Eskicioglu, R.L.Lagendijk, E.J.Delp, "Advances In Digital Video Content Protection",2005, pp: 171-183

[4]. F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn, "Information Hiding – A Survey", 1999, pp: 1062-1078

[5]. Chun-Shien Lu, Shih-Kun Huang, Chwen-Jye Sze, Hong-Yuan Mark Liao, "Cocktail Watermarking For Digital Image Protection", 2000, pp:209-224

[6]. S. Roy, M. Chuah,"Secure Data Retrieval Based on Cipher text Policy Attribute-Based Encryption (CP-ABE) System for the DTNs"

[7]. Gang Liu, Yafei Dai, Zhenhua Li, Yan Huang, "Cloud download: using cloud utilities to achieve high-quality content distribution for unpopular videos"