ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

COLLETRAL SHARING AND PENETRATING FOR REAL-TIME VIDEO DATA IN MOBILE CLOUD

Ms.P.R.INDHUMATHI
FINAL YEAR/ CSE,
M.Kumarasamy College of Engineering,
Karur –639 113
indhuindhu09@gmail.com

Ms.S.ISWARYA
FINAL YEAR / CSE,
M.Kumarasamy College of Engineering,
Karur –639 113
ishwaryasukumar@gmail.com

Abstract-The infrastructure that allows mobile users to secures, share and search for their real-time video data. The advantages of the cloud platform and wifi facilities where mobile users can share their real-time video with their friends or families. Through the cloud while any other user without permission cannot get any information about the video even if the cloud server is hacked. The proposed algorithm produces session based key generation. A session key is a single-use symmetric key used for encrypting all messages in one communication session. Symmetric key encryption is used to provide security (A secret key is generated). The file cannot be accessible without using the secret key which is generated using Symmetric key encryption algorithm.

Index Terms: Cloud Computing, Mobile Cloud

1. INTRODUCTION

The ubiquitousness of mobile applications and devices has been part of the new market that enables mobile developers to provide new services for their users. The success of mobile applications is also driven by data feeds and services in the cloud, and hence it leads to the notion of mobile cloud computing [1]. 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, enhance the users' experience.

When incorporating the cloud, major security issues will arise, such as the leak of video data. Merely encrypting the video data in the cloud will not be a viable solution since many operations (such as data search) on the data will becirppled. Hence, a novel way to provide data protection has become necessary in this situation.

2. CONTRIBUTION

In this article, we propose an infrastructure that allows mobile users to secure,share and search for their real-time video data. Mobile users can choose the 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 an information (e.g. keywords) about the video data. We deploy cloud technology as the basis with some cryptographic primitives as the building blocks. Therefore, our security is guaranteed even if the cloud server is hacked or the video data is stolen. In addition we also provide secure searching within a user's own

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

video data. Our solution provides efficient and practical real-time video sharing and searching among mobile users by utilizing 5G technology in the cloud computing paradigm.

3. EXISTING PLATFORMS

Existing cloud infrastructure allows people to store their files at an affordable price or for free. The list includes: Dropbox, Box, Justcloud, Baidu pan and Google drive, among others.

All of them allow their users to specify files for sharing. Some of them allow users to make their files publicly available. Service provider specilizing in media sharing include: youtube, Vimeo for video Flicker and Photobucket for photos.

These service providers with their web addresses. Security of the stored content depends on the policy of the provider. For instance, the statement from Dropbox assured that 256-bit AES was employed to ensure the files security.

Searching is often supported global scope. For example, users can search from the videos available on Youtube. For Dropbox, how a file can be searched within the collection of the user is outside the service model of Dropbox. However, the videos made available for searching are not encrypted.

4.SKYFIRE

Skyfire Rocket Optimizer is a cloud based mobile video and media optimization technology. The target user of this optimizer is the mobile operator (e.g. 3, Vodafone etc.). The consumers of this operator consume a lot of bandwidth with the growing popularity of mobile video. To save bandwidth, the mobile operator cloud leverage video compression. This is the traditional approach Skyfire claims to provide a new solution, that can measure the experience for the users.

For example, if a user is at the edge of the cellular base station, video sent to that user should be optimized aggressively since the bandwidth is going to be limited. On the other hand, when the bandwidth is more than sufficient, there is not a pressing need for video compression for that user. By continuously monitoring the users and the network situation Skyfire Rocket Optimizer can also apply the "transcoding" for the needed users. By doing so, they claim to allow mobile operators to guarantee the best user experience for their consumers

CHALLENGES IN EXISTING

Although there are some existing platform for sharing realtime video they may not be able to achieve secure finegrained 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).

5. IMPLEMENTATION

Infrastructure

Where a mobile user is connected with an external, video taking device through Wifi and the mobile device is connected through 5G with a cloud server with purposes of storage and sharing. Our security mechanism will be built on top of this network infrastructure which will be described later in this section.

CRYPTOGRAPHIC FUNCTIONS

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

We give a brief description of some cryptographic functions that are deployed in our infrastructure.

Advanced Encryption Standard (AES):

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 a message) and next runs an AES encryption algorithm AES.C ¨ AES.Enc(AESkey, m) with the key AES.key to encrypt a message m and get a ciphertext AES.C. By using the same key, the user can recover the message from its encrypted format via a decryption algorithm AES.

Searchable Symmetric Encryption (SSE)

In a SSE system, a user is allowed to generate a key SSE.key for both the encryption and the decryption of a message. By using the key, the user can encrypt a keyword index I via an encryption algorithm SSE.C ¨ SSE.Enc(SSE.key, I), and next upload the encrypted keyword index to a storage server. In the searching phase, the user (using the knowledge of the key) delivers a searchable trapdoor token tw ¨Trpdr(SSE.key w) associated with the keyword w to the server. The server checks this token with every ciphertext Check(SSE.C, tw). If the ciphertext is the encryption of the keyword w, it returns true. The user can also run a decryption algorithm with the key to decrypt the whole cipher text.

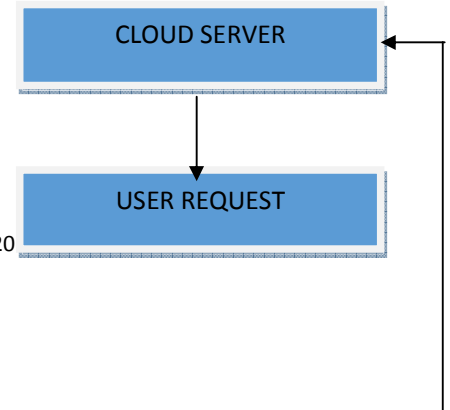
Ciphertext Policy Attribute-Based Encryption (CP-ABE)

CP-ABE is a kind of asymmetric encryption. In a CP-ABE scheme, a registered user is first issued a decryption key skAS from a trusted ABE key generation centre (KGC, in which the key is associated with an attribute set AS describing the user (e.g. male, student). To share data with other system users, the user is required to encrypt a message m under a specified access policy(e.g. male student) via an encryption algorithm ABE.C ABE.Enc(policy, m). If the attribute set of a user's decryption key satisfies the above access policy, this user then is able to gain access to the data by running a decryption algorithm with the key m ¨ ABE.Dec (ABE.C SKas).

Digital Signature In a digital signature system, a registered user is issued a signing/verification key pair (ssk, svk), with a corresponding certificate cert (which is used to guarantee the validity of the verification key and the identity of the user) issued by a certificate authority (CA). The user is able to use the signing key to make a digital signature Sign ssk(m) on a message m such that anyone holding the corresponding verification key and the message is able to verify the validity of the signature Verify Svk (s, m).

DETAILED DESCRIPTION

There are three parties in our proposed infrastructure: the mobile user (with a 5G-connected mobile device) who can upload video to the cloud with an external video-taking device; the cloud server; and the normal user (who may use a normal PC computer or mobile device but cannot upload video).The are two authorities: the key generation centre (KGC) for issuing the attribute-based user secret key, and the certificate authority (CA) for issuing the user certificate



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

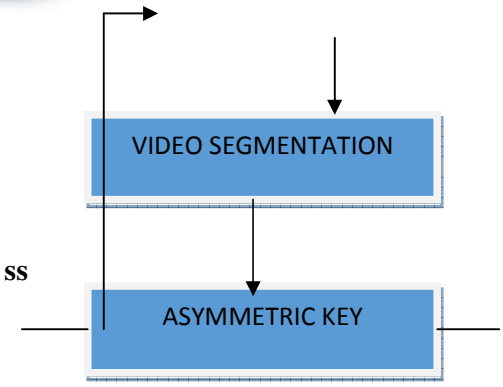


Fig1.Network Infrastructure Overview

System Setup:

The user with a mobile device downloads an app that is equipped with cryptographic functions such as AES encryption searchable symmetric encryption(SSE) cipher text policy attribute-based encryption (ABE), and digital signature.

User Registration

User registration consists of two parts. In the first part, the user registers with a trusted ABE key generation centre (KGC) to obtain their attribute user secret key which is used for video sharing purposes. In the second part, the user registers with the cloud server for access control purposes. They are described as follows:

A user (mobile user or normal user) first registers to a trusted ABE KGC, which in turn offers an attribute set AS describing him/herself (e.g. male, student, British ,Alice's friend, Bob's family) and the corresponding decryption key skAS associated with the attribute set to the user. The user stores the decryption key.

A mobile user further registers him/herself with the cloud. The detail procedures are NO ribed as follows: A mobile user obtains a signing/verification key pair (sskreg, svkreg) and a digital certificate cert (which contains the user identification and the verification key) from the CA.

The user signs the username USERNAME and the login password PASSWORD as sreg Signsskreg(USERNAME||H(PASSWORD)),a nd finally uploads the tuple (USERNAME, H(PASSWORD), sreg, cert) to the cloud server where H is s target collision resistant hash function.The cloud server validate cert extract the svkreg from the cert, and verifies the signature as Verify svkreg(sreg, (USERNAME||H(PASSWORD)). If all verifications are valid, the server stores the tuple (USERNAME, H(PASSWORD), cert) in its backend storage system.

Next the user generate a SSE encryption/decryption key as SSE.key and stores SSE.key in the mobile device. At the end of the registration, every user (mobile or normal) gets his/her attribute-based decryption key skAS (with the associated attributes). A mobile user (who can upload video to the cloud) additionally gets a certificate cert (together with a signing/verification key pair), a searchable encryption/ decryption key SSE.key, and a username/password for the access to the cloud.

VIDEO UPLOAD

After using an external camera device to take a video, it is transferred to the user's mobile device via Wifi. The user further remarks the video by using some keywords as searchable indexes (e.g. date, location information, personal identification etc.). Before uploading the video to the cloud, the mobile device needs to encrypt the video in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

several layers. First, it uses AES to encrypt the video data. Then it uses SSE to encrypt the corresponding keywords. Finally, it uses ABE to encrypt the AES key under some desired attributes (e.g. Alice's family). The details of the protocol are described below.

In order to encrypt a video data V, the user first generates a one-time AES encryption/decryption key and uses this key to symmetric encrypt the video data V as (AES.keyV, V). Next the user uses SSE.key (generated at the registration stage) to encrypt the corresponding keyword index IV = {I1, … , In} as SSE.CV = SSE.Enc(SSE.key, IV).

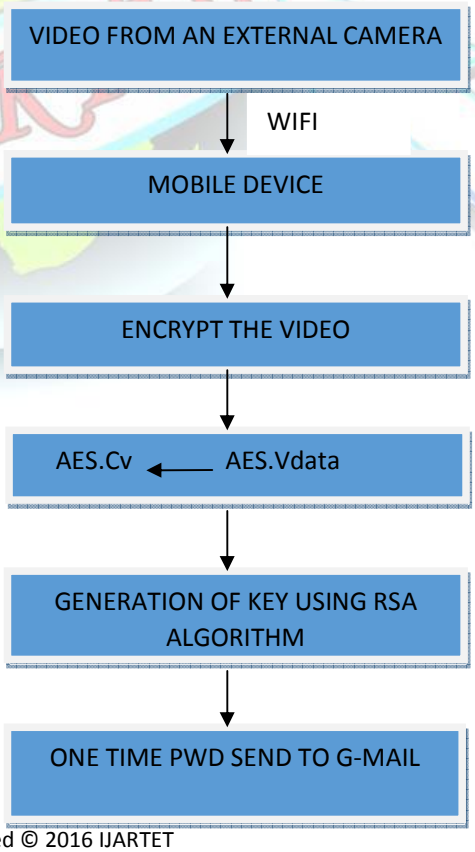
In order to securely share the encrypted data with other users, the mobile user deploys ABE to encrypt the one-time AES key AES.keyV as (policy, AES.keyV), where policy is an access control formula. policy always includes USER=USERNAME. For example, if the user has a username Alice, the policy can be set as USER=Alice OR Alice's family (that means user Alice or any user with the attribute Alice's family can decrypt). In this way, the user does not need to store any AES symmetric key as he/she can always retrieve every key from decrypting the attribute based cipher text from the cloud .The user signs the above encryptions as sV ¨ Signsskreg(AES.CV||SSE.CV||ABE.CV).

The user eventually logs in to the cloud by using his/her username and password, and uploads the tuple (AES.CV, SSE.CV, ABE.CV, sV).If the verification on Verifysvkreg(AES.CV||SSE.CV||ABE.CV, sV) is valid, the cloud stores the tuple in the storage under the username USERNAME of the user. There is also a sequence number d for this entry. That is this is the dth video of the user whose username is USERNAME.

VIDEO SEARCHING AND RETRIEVAL

In order to search for and retrieve a particular video (with a keyword), the video owner proceeds as follows.

The user logs in to the cloud system by using the username/password.The cloud server searches all SSE.CV for this user (with username USERNAME). If there is a match for the keyword w (by executing the algorithm Check(SSE.CV, t)), the cloud looks up the corresponding sequence number d for this entry and returns the corresponding tuple (AES.CV, SSE.CV, ABE.CV, sV).The user verifies the signature Verifysvkreg (AES.CV||SSE.CV|| ABE.CV, sV). If it is valid, he/she uses skAS to decrypt ABE.CV and gets AES.keyV ¨ ABE.Dec(skAS, ABE.CV). Then he/she uses AES.keyV to decrypt AES.CV and gets V ¨ AES.Dec(AES.keyV, AES.CV).



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

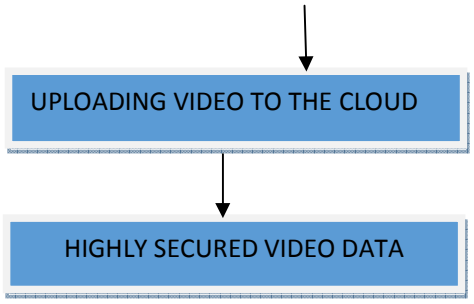


FIG.2 UPLOADING THE VIDEO TO THE CLOUD

VIDEO SHARING

If the video owner wants to share one of his/her video with their friends or another set of people (with some unique attribute) they can do the following:

The video owner searches for the video entry V that he/she wants to share (by using Video Searching and Retrieval).

The user asks the cloud to open the corresponding web page for public access such that the web page contains URLs for the download of the tuple (AES.CV, SSE.CV, ABE.CV, Sv) and cert of the user.1

Those users with whom the video wants to share can access the web page to download all tuples and cert and execute the following steps to retrieve the video: – Verify cert and extract the public key svkreg. –If the verification on Verifysvkreg

(AES.CV||SSE.CV|| ABE.CV, sV) is valid, use skAS to decrypt ABE.CV to get AES.key ¨ ABE.Dec(ABE.CV). –Use AES.key to decrypt AES.CV to get V AES.Dec(AES.CV).

6. RELATED WORK

We analyze the efficiency of our protocol. We use the benchmark result from Geek bench and the API from JPBC for simulation.

The mobile device we used is HTC M8. We deploy the signature scheme from [14] and the ABE scheme from [15] for the analysis.

Our protocol, the cloud server is only required to verify a digital signature in each phase. It can be done in 0.02 seconds according to the benchmark result from JPBC for a desktop computer with Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz, 3 GB Ram, Ubuntu 10.04.

For the user side, we analyze the efficiency for user registration, video upload, and video retrieval phases. In the user registration phase, the mobile device requires 0.151 second. In the video upload phase, we deploy AES CBC mode so the streaming video can be processed.

The maximum processing speed for AES is 293.9 MByte/s, which is much larger than the video bit rate (the maximum bitrate for 1080p Blue ray Disc is just 40 Mb/s).

when the whole video has been generated, the AES encryption will be almost done. The time for SSE is negligible when compared to ABE. Thus we only consider the time for ABE encryption.Assume the video data size is 2 Gbytes. It takes 2.97 seconds to generate the hash using SHA-1 and 0.15 second to generate the signature. Overall, it takes less than 4 seconds to complete.

In the video retrieval phase, again we assume the video data size is 2 G and the policy contains four attributes. It takes 2.97 seconds to generate the hash using SHA-1; 0.71 seconds to verify the signature; 4.5 seconds to ABE decrypt; and 6.97 seconds to AES decrypt. Overall, it takes less than 16 seconds to decrypt the video.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

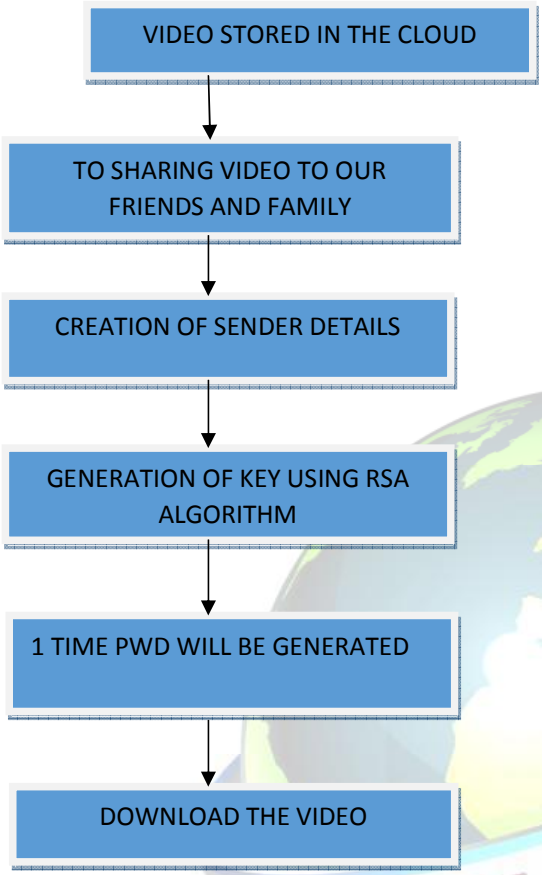


FIG.3 DOWNLOADING THE VIDEO FROM CLOUD

we have proposed an infrastructure for secure sharing and searching for real-time video data. It is particularly suitable for mobile users by deploying wifi connection and a cloud computing platform. Our security is guaranteed even if the cloud server is hacked since data is now protected by cryptographic encryption algorithms. In addition, we also provide secure searching functionality within a user's own video data. We believe our proposed infrastructure is practical to be deployed.

REFERENCE

[1]Secure Key for Authentication and Secret Sharing in Cloud Computing,Santosh Lomte,Shraddha Dudhani,2015

[2]Cloud-based Mobile Video Streaming Techniques,Londhe, Dejan Kovachev ,2015

[3]Mobile video streaming and sharing in social network using cloud by the utilization of wireless link capacity ,H. Schwarz , M. Wien,2014

[4]A Framework of Adaptive Mobile Video Streaming and Efficient Social Video Sharing in the Cloud,Xiaofei Wang, Min Chen,2013