RESEARCH ARTICLE OPEN ACCESS

Search and Safe Exchange of Real-Time Video on Mobile Cloud

V.Pavithra [1], S.V.Shreekeerthana [2], S.Yogapriya [3]
IV- B.Tech
Ms.T.Nithya (Sr/Gr)
Department of Information Technology
Velalar College of Engineering and Technology
Thindal -India

ABSTRACT
We propose an infrastructure that allows users of the mobile to share and search their video data on cloud secured. It is implemented using the 5G and cloud technology. The mobile users can be able to share their real-time video through the cloud and the other user can access only if the particular user authenticated. Even when the cloud server is hacked, the security for the infrastructure still remains guaranteed.

Keywords:- AES, Encryption, Decryption

I. INTRODUCTION

The major phase of telecommunication known as 5G will allow larger bandwidth. A 5G connection is 250 times faster than today's 4G LTE network. With the use of this 5G technology, the high density real- time video can be stored, retrieved and shared efficiently through the cloud platform. The major problem in cloud computing is security issue such as video data leakage. Encryption of video data will not be the only solution and hence we provide a novel data protection way to protect the video data on cloud.

II. LITERATURE SURVEY

CIPHER-TEXT POLICY ATTRIBUTE BASED ENCRYPTION

A new methodology for realizing Ciphertext-Policy Attribute Encryption (CP- ABE) is presented. This solution allows any encryptor to specify access control in terms of any access formula in the system. Three constructions are presented within this framework. The first system is proven selectively secured under the assumption that is called as Parallel Bilinear Diffie-Hellman Exponent (PBDHE). The next two constructions achieve provable security respectively by providing performance tradeoffs.

ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES)

This standard specifies the **Rijndael** algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard. The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".

A DFA-BASED FUNCTIONAL PROXY RE-ENCRYPTION SCHEME FOR SECURE PUBLIC CLOUD DATA SHARING

A general notion for proxy re-encryption (PRE) is defined. A message is encrypted in a ciphertext and a decryptor is legitimate if an associated DFA with his/her secret key accepts the string. This new approach can increase the users flexibility to delegate their rights of decryption to others. It is also proved as a fully chosen-ciphertext secure
in the standard model.

III. EXISTING SYSTEM

Existing cloud infrastructure allows people to store their files at an affordable price or for free. The list includes: Dropbox, 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 providers specializing in media sharing include: Youtube, Vimeo for video, Flickr, and Photo bucket for photos. Security of the stored content depends on the policy of the Provider. 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 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.

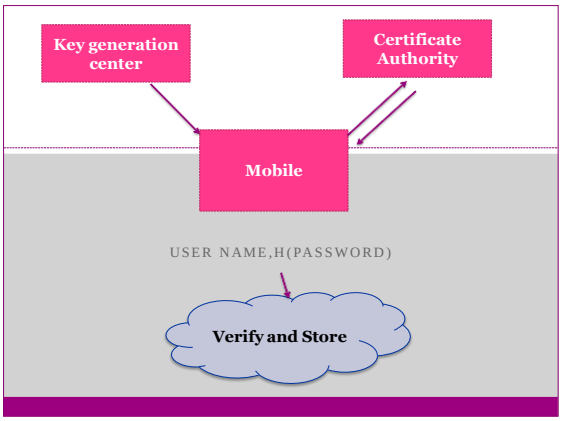
IV. PROPOSED WORK

Three parties are there in our proposed infrastructure: the mobile user who can upload video to the cloud. The video uploaded will be stored in the cloud and the normal user who may use a normal PC computer to view the video. There 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. There are several protocols in our infrastructure such as AES(Advanced Encryption Standard), SSE (Searchable Symmetric Encryption) and CP-ABE (Cipher text Policy Attribute Based Encryption).

For generating the key we use AES(Advanced Encryption Standard) algorithm . which will be verified by CA at the time of posting the request (i.e by the user who is willing to see the video) . If the key is matched then only the user will receive the file.

SYSTEM SETUP: The mobile user downloads an app that is equipped with cryptographic functions such as AES, SSE, ABE and Digital Signature.

USER REGISTRATION: In the first part of user registration, the user registers with a trusted ABE key generation center to obtain their secret key. In the second part, the user registers with a cloud server for the purpose of access control.



VIDEO UPLOAD: Before uploading the video to the cloud, the video is to be encrypted by the mobile device through several layers. Firstly, AES is used to encrypt the video data. Next, SSE is used to encrypt the respective keywords. Thirdly, ABE is used to encrypt the AES keyword under certain attributes.

VIDEO SEARCHING AND RETRIEVAL: To search the video , the owner proceeds as follows:

- The user logs in to the cloud system with the help of user name and password.
- The user retrieves the key SSE.key from the mobile and the searchable trapdoor token is generated. The user also uploads the token to the cloud server.
- The cloud server searches for this user and if there found a match for the particular keyword, the cloud server looks up the sequence number and the respective tuple is returned.
- The user verifies the signature. If it is valid, then it is decrypted.

V. CONCLUSION

The video data on the cloud platform is thus secured. The infrastructure security is guaranteed even if the cloud server is hacked. A user without the specific permission cannot get the access to the particular video data on the cloud.

REFERENCE

[1] [1] Smith's Point Analytics, "Mobile Cloud Platforms: The Backend of Mobile Apps," http://www.reportlinker.com/p01650001-summary/Mobile-Cloud- Platforms-The-Backend-of-Mobile-Apps.html, 2013.

[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] A. 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.

[6] R. Curtmola et al., "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," ACM Conf. Computer Communications Security, A. Juels, R. N. Wright, and S. D. C. di Vimercati, Eds., ACM, 2006, pp. 79–88.

[7] D. Cash et al., "Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries," CRYPTO 2013, ser. Lecture Notes in Computer Science, vol. 8042, Springer, 2013, pp. 353–73.

[8] D. Cash and S. Tessaro, "The Locality of Searchable Symmetric Encryption," Proc. EUROCRYPT 2014, ser. Lecture Notes in Computer Science, vol. 8441, Springer, 2014, pp. 351–68.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, 2007, pp. 321–34.

[10] F. Guo et al., "CP-ABE with Constant-Size Keys for Lightweight Devices," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, 2014, pp. 763–71.

[11] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol. 4, no. 3, 1991, pp. 161–74.

[12] L. Chen and J. Li, "Flexible and Scalable Digital Signatures in TPM 2.0," Proc. ACM Conference on Computer and Communications Security, ACM, 2013, pp. 37–48.

[13] K. Liang et al., "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing," IEEE Trans. Information Forensics Security, vol. 9, no. 10, 2014, pp. 1667–80.

[14] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, 2004, pp. 297–319.

[15] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," PKC 2011, vol. 6571; Springer, 2011, pp. 53–70.