ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud: A Survey

Prayas Gajbhiye[1], Arati Dandavate[2]

M. E Student, Dept. of Computer Engineering, Dhole Patil College of Engineering, Pune, India[1]

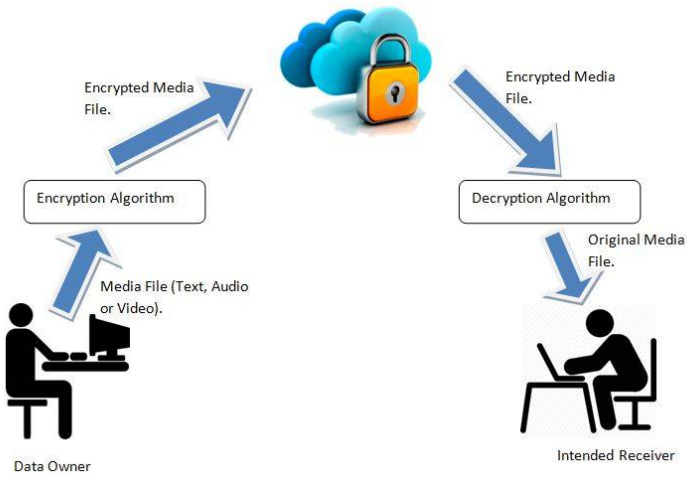
HOD, Dept. of Computer Engineering, Dhole Patil College of Engineering, Pune, India[2]

ABSTRACT: 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. 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.
The next major phase of the mobile telecommunication standard, known as 5G, will allow larger bandwidth. With the availability of 5G technology, sharing real-time high density video can be offered efficiently via the cloud platform. When incorporating the cloud, major security issues will arise, such as the leak of video data. To provide the solution to these security issues different algorithm and techniques has been introduced but every algorithm and technique has its own merits and demerits. In this paper we have done the survey of different cryptographic algorithms.

KEYWORDS: Encryption, Decryption, Public key, Secret key.

I. INTRODUCTION

The basic architecture of a cloud is shown in figure 1. The actors of the system are, the user who wants to upload and share the data called as data owner and the other user with whom, the data is being shared. The data owner uploads the data to the cloud. This data is encrypted using encryption algorithms. The encrypted data i.e. cipher text is stored securely in the cloud. The data owner shares the key with the intended receiver of data. The receiver can then decrypt the cipher text and get the original data.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Cloud computing is used in tremendous amount in different fields. Large amount of data is generated in daily life. To store this huge amount of data we use cloud computing services. Cloud computing provides different types of services to the user. While storing the data on cloud there are number of issues.

Cloud computing is used in tremendous amount in different fields. There are many service providers which provide cloud services to the clients. Knowingly or unknowingly, cloud storage has become part of everyone's daily life. When user stores any file, text, audio or video, it is stored on the cloud. The person, who wants to retrieve it, then downloads it from the cloud. During this process of storing and retrieving, security measures come into picture. There are multiple proposed solution and techniques which are used to secure storage and transmission of user data. Cryptography is the most commonly used technique. It is process which converts the user's file into an unreadable format and then stores it. While retrieving, the encrypted unreadable file is converted back to original format.

Cryptography is classified into types, symmetric algorithm and asymmetric algorithms. Symmetric algorithms are AES, DES, IDEA, TDES, and Blowfish, while RC6. RSA and ECC are asymmetric algorithms. Symmetric algorithms uses same key for encryption as well as decryption, known as Secret Key. Asymmetric algorithms use two keys, Public and Private. Public Key is used for encryption while Private Key is used for decryption.

Combination of multiple cryptography algorithms are used for enhancing security [1]. Different security models can be created using different combinations of same algorithms. These newly formed security model overcomes issues of cloud security like secure data storage, secure data transmission and secure data access. Different algorithms are used to maintain authenticity of data. Only valid user should be able to access the data stored on cloud. This can be achieved using MD5 algorithm. In the proposed system, multiple algorithms are applied at multiple level, thus it becomes difficult for unauthorized person to access the data of the user.

Proposed system uses different algorithms to store, share and search video securely over the cloud platform. The metadata about the video is also encrypted. Many algorithms have been proposed by researchers to overcome data security issue. TDES and Diffie Hellman key exchange algorithm are used to solve these issues. Diffie Hellman key exchange algorithm is used to securely exchange keys through unsecure communication channel. Signature is used for authentication purpose. AES is used to encrypt the actual message. It also generates the key which can be shared with authenticated user to access the encrypted message.

Cloud computing offers on-demand services. In cloud deployment models different combination of algorithms are used to achieve data confidently, integrity and authentication. Data is stored in different deployment model of cloud computing according to the security requirement of the user. [2] Cloud can be public, private, community or hybrid. The security level depends on type of deployment model.

Though asymmetric algorithms offer higher level of security than symmetric algorithm, performance-wise symmetric algorithm are better than asymmetric algorithms. RSA is used to solve key distribution problem. AES solves the problem of data confidentiality. The proposed hybrid system offers higher level of security with better performance.

In a SSE system, a user is allowed to generate a key for both the encryption and the decryption of a message. By using the key, the user can encrypt a keyword index via an encryption algorithm and next upload the encrypted keyword index to a storage server. CP-ABE is a kind of asymmetric encryption. In a CP-ABE scheme, a registered user is first issued a decryption key from a trusted ABE key generation center (KGC), in which the key is associated with an attribute set describing the user.

II. RELATED WORK

The hybrid security model has been proposed by Joseph K. Liu, Man Ho Au, Willy Susilo, Kaitai Liang, Rongxing Lu, and Bala Srinivasan. The security is provided by using combination of different algorithms at different levels. Proposed consists of user registration, video uploading, sharing and searching. Different algorithms are used at different stages to perform these tasks securely.

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 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.

The user with a mobile device downloads an app that is equipped with cryptographic functions such as AES encryption [3, 4], searchable symmetric encryption (SSE) [5-7], cipher text policy attribute-based encryption (ABE) [8, 9], and digital signature [10, 11]. User registration consists of two parts. In the first part, the user registers with a trusted ABE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

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.

III. PROPOSED ALGORITHM

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. 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 smartphone. 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.

IV. 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. PERFORMACNE REVIEW

As mentioned earlier, different algorithms have advantages and disadvantages over other. Thus, we have performed a performance evaluation for symmetric and asymmetric algorithms to analyze the different service.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Table 1 . Performance Analysis Table for Cryptography Algorithms

Sr. No.	Algorithms and Techniques	Advantages	Disadvantages
1	AES and RSA	1. High speed 2.High system performance 3.Secuirty	1. RSA is more time consuming
2	RSA ,MD5 and Blowfish	1.Authentication 2.Intgrity 3.Data confidentiality	1.In Blowfish algorithm static key is used every time
3	RC6	1. Less Memory space 2.Fast Encryption 3.Data recovery	1. Less Secure
4	Blowfish, AES ,IDEA and SHA1	1. Better Security 2.Confidentiality 3.Non-repudiation 4.Availabilty 5Privacy 6.Integrity	1.Less secure as compare to asymmetric algorithms 2.Key distribution problem
5	Digital signature ,AES and Diffie Hellman Key Exchange Algorithm	1. Integrity 2. Confidentiality 3 Authentication	1.less Efficiency
6	RSA ,Digital signature and MD5	1.Data security 2 Data integrity 3Authentication	1.Consumes maximum time
7	Diffie Hellman key Exchange and TDES	1.Confidentiallity 2.Authentication	1. Week key 2. Time consuming
8	Dynamic Merkle Hash tree and AES	1.Better security 2.Data confidentiality	1.Less secure as compare to RSA algorithm
9	Blowfish	1.High availability 2.Data integrity 3.Confidenltiy 4.Data authentication	1.Less secure
10	SHA-1 and Grid based technique	1.Multilevel integrity 2.Confidentility 3.User Authentication	1.less efficiency

The T able 1 helps to analyze which algorithms are better than the others. Depending on the requirement of security level user can choose any combination these algorithms.

VI. CONCLUSION AND FUTURE WORK

Symmetric algorithms are gives better performance in terms of speed as compare to asymmetric algorithm. Asymmetric algorithms provide better security as compare symmetric algorithm.AES algorithm gives better security as compare to RC6 and Blowfish algorithm. AES algorithm require minimum amount of time for encryption and decryption as compare to RSA. In future we will add more algorithms and combinations of different algorithms and techniques to over security risks in cloud computing.

REFERENCES

[1] B. Nayak, Sudhansu Ranjan Lenka,"Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm", IJCST ,Volume 2 Issue 3, pp.60.-64,June-2014

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

[2] R. Pal Singh, "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques", SSRG International Journal of Mobile Computing & Application , volume 2, Issue 3 ,pp.38-44,June 2015
[3] United States National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, 2001.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, 2007, pp. 321–34.
[9] 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.
[10] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol. 4, no. 3, 1991, pp. 161–74.
[11] 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.

BIOGRAPHY

Prayas Gajbhiye [B.Tech (I.T)] is a student of Dhole Patil College of Engineering, Pune. He is in second year of Computer Engineering and will receive his Master of Engineering degree in July, 2016.

Prof. Arati Dandavate [M.E (CSE)] is currently working as HOD, Computer Engg. Dept., at Dhole Patil College of Engineering, Pune. She has 15 years of teaching experience and 2 years of IT experience.