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 6, June 2016

Data Security in KAC Using Standard Encryption Technique

Sunil S.khatal[1], K.S.Kahate[2]

M. E Student, Dept. of Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, India[1]

Asst. Professor, ME Co-Ordinator, Dept. of Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, India[2]

ABSTRACT: Cloud computing is an architecture for succeeding generation. It has more facilities though have risks of attacker who can access the data or leak the user's information. Cloud users and service provider's authentication is needed. The issue arises whether loud service provider is uncompromised, data will leak if any one of them in compromised. The cloud preserving the privacy and also maintaining user's information. There are many cloud users upload there data without providing much privatedetails to different users. Another way for sharing encrypted data is Attribute-Based Encryption. ABE encrypt the data with attributes which are equivalent to users attribute rather than only encrypting every part of data. In ABE attributes description is considered as set so that a particular key which is matched with attribute can decrypt the cipher text. The user key and the attribute are matched if it matches it can decrypt a particular cipher text.A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for other users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using private key.

KEYWORDS: -Database storage, data sharing, keyaggregate encryption, patient-controlled encryption, Stenography, Computer Forensic, and Authentication.

I. INTRODUCTION

Cloud storage is nowadays very popular cloud storage system. Cloud storage is storing of data off-site to the physical storage which is maintained by third party application. Cloud storage is saving of digital data in logical pool and physical storage time multiple servers which are managed by third party. Third party is responsible for keeping data available and procurable and physical environment should be protected and running at all time. Hence of storing data to the hard drive or any other local storage, we save data to remote storage which is procurable from anywhere and anytime. It reduces pursuit of carrying physical storage to everywhere.

A. Data Privacy in DatabaseEnvironment:

Considering data secrecy in cloud computing environment, a traditional way to assure data privacy is to rely on the server to enforce the access control after authentication, which means any unexpected privilege increase will expose all data. Data from other users can be hosted on different virtual machines (VMs) but reside on a single physical machine. Data in a target VirtualMachine could be stolen by instantiating other Virtual Machine co-occupant with the target one.

B. Data Availability in Database Server :

Regarding accessibility and privacy of files, there are a many number of cryptographic schemes were proposed. This scheme allowing a third-party auditor to check the procurable of files on behalf of the data owner without leaking any information regarding the information, or without compromising the data owner's privacy.

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 6, June 2016

II. RELATED WORK

The paper discusses the conjunction of cryptography with adaptive steganography for audio video sequence with messy algorithm as the encryption algorithm. As the encryption increases the PSNR value gets increased.The author discusses other methods for audio steganography and LSB method is found to be more secure. The paper discusses LSB audio steganography with location identification and it provides best audio quality and robustness.The paper discusses the advanced messy algorithm for the encryption and decryption purpose and it consumes less time and fewer complexes. This portion broadly reviews the state-ofthe- art of proving security to the data stored on the cloud storage. Other approaches were proposed by more scholars and few of them are mentioned below. A system was proposed by to generate a tree hierarchy of symmetric-keys by using repeated evaluations of pseudorandom function block-cipher on a fixed private. The concept can be generalized from a tree to graph. In other system data owner encrypts the data, public key, data index and then uploads to the cloud server. Data owner creates aggregate decryption key using its master-secret key, and shares the data to different users by sending its ADK to users via a secure E-mail on the other side the data user decrypts the data in this process steganography used. Other technique discusses a special type of encryption called as key-aggregate cryptosystem which allows user to share their data partly across cloud and produces constant-size cipher text.

In this technique user provide a fixed-size aggregate key for another cipher text classes in cloud storage, but the other encrypted files outside the class remain confidential**.** A more group key management accomplishes a hierarchical access manage by applying an integrated key graph also handling the group keys for another users with multiple access authorities. Centralized key management scheme uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It
derive an integrated key graph for each user.Information security using data hiding audio video steganography with the help ofcomputer forensic techniques provides best hiding power we have worked on hidingimage and text behind video and audio file and extracted from an AVI file using 4 least consequence bit insertion methods for video steganography and phase coding audio steganography.

III. PROPOSED WORK

A. Key Generation with Aggregate Cryptosystem:

In key-aggregate cryptosystem (KAC), users encrypt a message is not only under a publickey, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into another classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for other classes. Most importantly, the extracted key have can be an aggregate key which is as compact as a private key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.With our example, Alice can send Bob a single aggregate key through a secure e-mail. Bob can download the encrypted data's from Alice's Box.com space and then use this aggregate key to decrypt these encrypted data. The sizes of ciphertext, public-key, and master-secret key and aggregate key in KAC schemes are all of constant size.

B. Symmetric-Key Encryption with Compact Key:

An encryption scheme which is originally proposed for concisely converting huge number of keys in broadcast scenario. The construction is simple and we broadly review its key derivation process here for a concrete description of what are the desirable properties we want to achieve. The derivation of the key for a set of classes is as follows. A composite modulus is select where a and b are two huge random primes. A master secret key is select at random. Everyclass is associated with a distinct prime. All of theseprime numbers can be put in the public system parameter. A fixedsize key for set can be created. For those who have been delegated the access rights for S′ can be created. Hence, it is designed for the symmetrickey setting. The content provider necessary to get the corresponding secret keys to encrypt 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 6, June 2016

IV. SYSTEM ARCHITECTURE

Encryption keys also came with two flavors symmetric key or asymmetric key. Using symmetric encryption, when Alice wants the data to be originated from a third party, she has to give the encryption her private key; obviously, this is not always desirable. By contrast, the encryption key and decryption key are different in public-key encryption. The use of public-key encryption gives most flexibility for our applications. For example, in enterprise settings, each employee can upload encrypted data on the cloud storage server without the knowledge of the company's master-secret key. hence, the better solution for the above problem is that Alice encrypts files with distinct public-keys, but only sends Bob a single decryption key.In this system each ciphertext is labeled by the encryption with a group of descriptive attributes. Each nonpublic secret is related to AN access structure that species which sort of ciphertexts the key will decrypt. We tend to decision such a theme a Key- Policy Attribute-Based secret writing, hence the access structure is per the non-publickey, whereas the ciphertexts area unit merely labeled with a group of descriptive attributes.

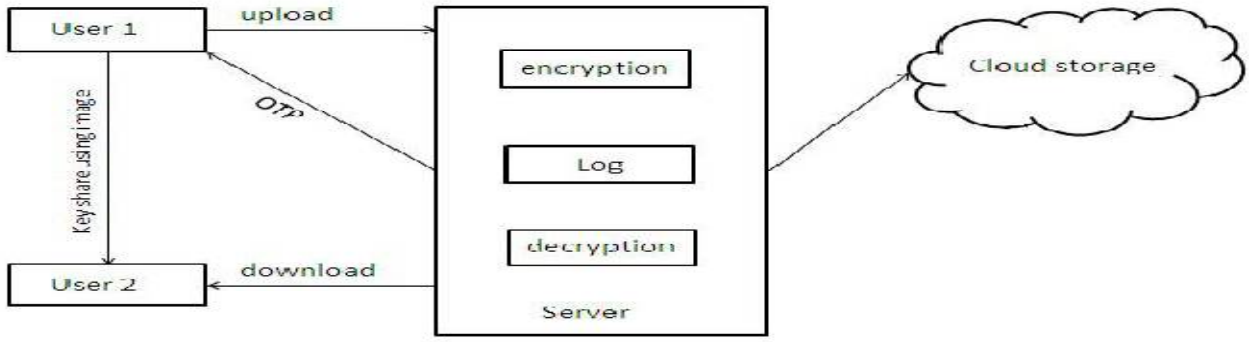

Figure 1. Using KAC for data sharing in cloud storage

Advantage:

A. Security of Data
B. Key Aggregation System
C. Application of data hiding in audio-Video.
D. OTP (Online Transaction Processing).
E. Three Tier Architecture forAcknowledgement.

V. RESULT ANALYSIS

FIGURE 2. USER REGISTRATION

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 6, June 2016

Figure 3. Owner Login

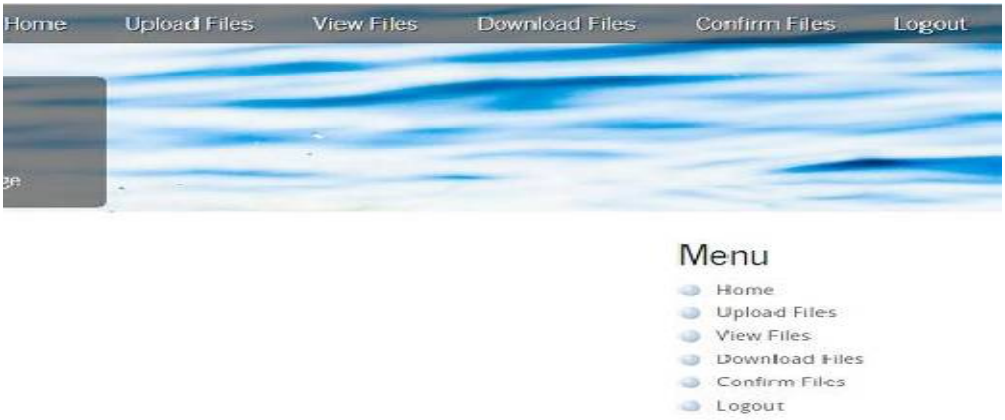

Figure 4. File Operations

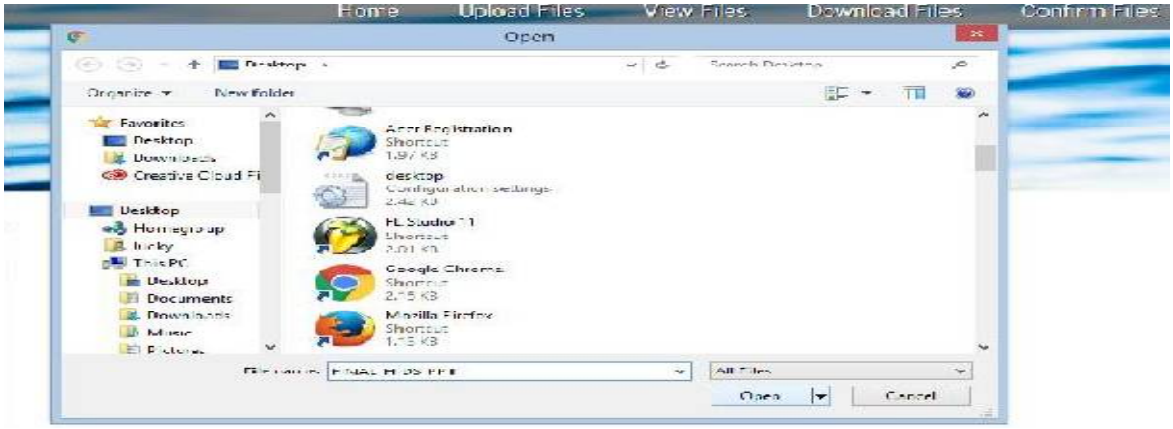

FIGURE 5. FILE DOWNLOAD

VI. CONCLUSION AND FUTURE WORK

Steganography is the system of hiding any private information or any secret information like password, single key text and image, audio behind original cover file in cloud storage. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio- video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is toHide secret information behind image and audio of video file.

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 6, June 2016

As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

REFERENCES

1. Cheng-Kang Chu ,Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage‖, IEEE Transactions on Parallel and Distributed Systems. Volume: 2 5, Issue: 2. Year: 2014.
2. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
3. J. Benaloh, ―Key Compression and Its Application to Digital Fingerprinting,‖ Microsoft Research, Tech. Rep., 2009.
4. Praveen, P, Arun, RAudio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm, International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 4, Issue 2 (August 2014) PP: 01-07.
5. Savkar Tushar, Dhanak Prasad,Jadhav Gaurav, Salunke Sachin,Application Of Data Hiding In Audio- Video Using Anti Forensics Technique For Authentication And Data,National Conf. on Recent Innovations in Science Engineering & Technology(NCRISET), 16th Nov.-2014, Pune, India, ISBN: 978-93-84209-65-0.
6. AthiraMohanan, Reshma Remanan, Dr. Sasidhar Babu Suvanam, Dr. Kalyankar N V, Audio – Video Steganography Using Forensic Techniquefor Data Security, International Conference On Emerging Trends In Engineering And Management (Icetem14) 30 – 31, December 2014, Ernakulam, India.
7. Ms. V.Sarangpure; Mrs. R. B. Talmale;Ms. M. Domke, Survey paper - Audio-Video Steganography Using Anti Forensics Technique, International Journal of Research (IJR) Vol-1, Issue-9, October 2014 ISSN 2348-6848.