ISSN 2395-1621

Data Security Using Crypto Stenography For Sharing Scalable Data

[#1]Mr.Kshirsagar Sopan B,[#2]Miss.Karad Vandana A,[#3]Miss.Chaskar Kanchan J,
[#4]Mr.Tayade Bhushan S

[1]sopankshirsagar02@gmail.com
[2]vandanakarad9096@gmail.com
[3]kanchanchaskar1993@gmail.com
[4]Bhushantayade077@gmail.com

[#1234]Student, Bachelor of Computer Engineering, SPCOE,
Dumberwadi, Otur, Pune.

ABSTRACT

Sharing any information is an important function in cloud storage. This paper we prove how to share data securely, efficiently, and flexibly with others in cloud storage. We access the private information in cloud with the help of secrete key. We describe new technique i.e. public-key cryptosystems for secure communication between data owner and third party user also .Public key cryptosystem produce constant-size cipher texts such that efficient delegation of decryption rights for any set of ciphertexts are possible. In the key aggregate cryptosystem one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. This compact aggregate key can be kindly sent to others for data access it increase data personally and security. In innovation cryptographic key generation techniques, this technique possesses unique cryptographic key aggregate cryptosystem which is helpful for secure data and privacy preserving key generation process. We propose access level policy structure such as Public and Private Access level to improve the data access mechanism in the data sharing mechanism process. Governments, military, business and Private Citizens all over the world now use stegnography and cryptography for security and privacy purpose to secure sharing information in the cloud storage . Computer forensics and another forensic methods such as digital forensics ,alternate data storage forensic etc. are used more popular in recently world due to advantages in computer systems and Authentication as well as investigation purpose in computer communication.

***Keywords*:- Database storage, data sharing, key-aggregate encryption, patient-controlled encryption, Stenography, Computer Forensic, and Authentication.**

ARTICLE INFO

Article History

Received:30th September 2015

Received in revised form :

2nd October 2015

Accepted:6th October, 2015

Published online :

9th October 2015

I. INTRODUCTION

Cloud storage is more popularity in the recently world. In everyday, we see the increase in demand for data incoming and outsourcing, which assists in the strategic management of corporative data. It is also used as a core technology behind many online services for personal as well as social applications. Nowadays, it is easy to register for free accounts for Drop box, Email, Photo album, Audio and Video files, Wuala.com, Google Drive, Amazon cloud drive file sharing and remote access, with storage size more than 20GB (or a few dollars for more than 1TB). Together with the cloud storage services and current wireless technology, users can access and share data with other members easily by uploading their data to the cloud and always all of their files and emails by a mobile phone in anytime and anywhere of the world with authentication and data security. Data

Privacy and data security for sharing scalable data is the important functionality in cloud storage. There will be lack of security for the user's data over the internet.

1. Data Availability in Cloud Storage:

The availability of data and security of data, there are a more number of cryptographic and stenographic schemes were proposed. This scheme uses a third-party user to check the availability of files on behalf of the data owner without leakage any information and added any type of unwanted data regarding the information, or without compromising the data owner's privacy. To access that availability of data third party users authentication must be needed.

2. Crypto Steganography schemes for data storage:

Cryptography is the method of gathering and sharing hidden secret data in the particular form so that only those for whom it is intended and process the required data. Cryptography is used to protect e-mail, messages, credit card and secret information and corporate data. It is technique to providing security to information by encrypting the data it into an unreadable format using some encryption algorithm. Cryptography is an effective way of protecting sensitive information that is to be stored on cloud or transmitted through internet communication media. The main goal of cryptography is that to hidden secret information from unauthorized peoples like criminal or hackers or fraud. In today's world Hackers can hack most of the cryptographic algorithms and the information can be retrieve if the attacker has required time and resources to hack the data. So a realistic goal of cryptographic algorithm is to decrypting the data to bemore difficult. Similarly, cloud users will not control the strongly dependence that the cloud server is doing a good quality work in terms of privacy and data security. A cryptographic algorithm and solution, with prove security relied on number-theoretic assumptions is more attractive. Whenever the user is not perfectly happy with believe the security of the Virtual machine or the honesty of the technical person. Those users are impulse to encryption of their data with creation of their own keys before uploading the data on the server. Steganography is the method of hidden any text, password, image or audio and video file frameworks behind an original cover file. In steganography the private data is hidden in a way that unauthorized users are unaware of the existence of the embedded data without altering the security, availability, privacy and quality of the cover file. Audio steganography is one of the popular data hiding method that embeds secret data in audio frameworks. Video Steganography is a method to hiding any kind of files into a framework of Video files. The use of the video based Steganography framework can be more effective than other multimedia files, because ofits size and memory.

3. Data sharing in cloud :

Data sharing is an important functionality in cloud storage. For example, users can access their friend's information and a subset of their personal pictures; an enterprise may allow users employees access to a portion of passionate data. In the cloud storage challenging problem is how to efficiently share or transmitting encrypted data. Users can download the encrypted data from the cloud storage and perform decryption algorithm to decrypt data, and then send that decrypted data to other people for sharing, but it may loss the quality of cloud storage. Users can able to give the access authentication of the sharing data to other people so that they can access these data from the server openly. However, finding an efficient and secure way to share partial data in cloud storage is not trivial.

Now a days Governments, military, businesses and private citizen's uses steganography and cryptography for security and privacy purpose. Combination of image, audio and video steganography is used. Computer forensic technique is used to find the parameter like frame number, height and width of data, PSNR, histogram of secrete message data before and after hiding to audio-video.

II. KEY-AGGREGATE CRYPTOSYSTEM

Sharing data or information among users is an important functionality in cloud storage. This paper explains new public-key aggregate cryptosystems that required constant-size cipher texts. The anyone user can aggregate any set of secret keys and make them as compact as a unique authentication key, but the power of all the secret keys being aggregated. This compact aggregate key can be kindly sent to users or be stored in a smart card with very limited secure cloud storage. How to a decryption key more powerful in the sense that it allows decryption of complex cipher texts, without changing its size. A another type of public key encryption ―key aggregate cryptosystem‖ in which the users decrypt a data using an identifier of cipher text called class which means the cipher texts are further categorized into different classes. The key data owner of the data contains a master-secret key, to extract secret keys for different classes of the cipher text from the cloud . Implementation of the KAC system in C with the pairing-based cryptography (PBC) Library.

SYSTEM ARCHITECTURE:

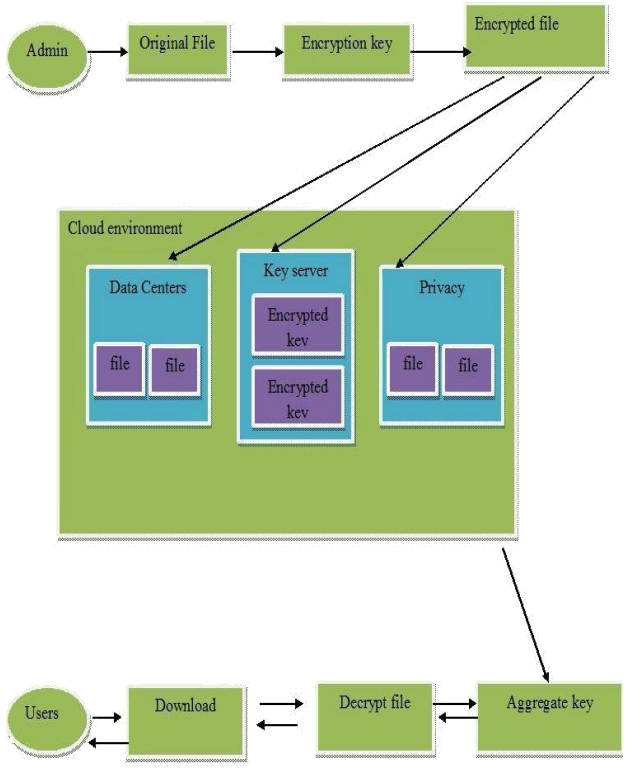

Fig 1. System Architecture For Key Aggregate Cryptosystem

Following stages of key aggregate cryptosystem:

1.**Key generation:**
Whenever we encrypt and decrypt of data and files an aggregate key is generated.

2.Encryption:
This is the stages where file is encrypted into secret form .

- Data owner essence required key from key generation and applies encryption of file and data now it generates a cipher text file.
- This file is stored in cloud storage which is unreadable for users.
- Sharing of encrypted data once file is encrypted in stored in cloud storage then the data owner the file shared in to any other user.Then the data owner share the key to the user now user can read and sometimes innovate the data based on priviliges.

a. Symmetric Key Encryption

Using symmetric key encryption, when user wants the data to be originated from a third party, other user has to give the encryptor his secret key; obviously, this is always hidden secret information.

b. Asymmetric Key Encryption

By variation, the encryption key and decryption key are different in public-key encryption. The use of public-key encryption gives more flexibility access for our applications and security information. For example, in enterprise settings, every user can upload encrypted data on the cloud storage server without the knowledge of the master-secret key.

Advantages:

- Applicability of KP-ABE scheme is to sharing of audit-log information and broadcast encryption .
- Multi-Identity Single-Key Decryption scheme is more efficient in decryption.

3.Decryption:

Any user who access the encrypted file from cloud is first applied with decryption when decryption is compared with extracted key from hierarchical structure then decryption is performed an original information get**.**

III. DATA SECURUTY BY USING AUDIO AND VIDEO FILES

Steganography is the method of hidden any personal information as like password, text and image, audio and video aback original cover file. Original text message is converted into cipher text by using secret aggregate key and then hide into the LSB of original images. The proposed system provided audio-video cryptosystem and steganography which is the synthesis of image steganography and audio steganography using Forensics Techniques as a resource of authentication. The main aim is to hiddenprivate and secret information behind theimage and audio file or video file. As video is the application of more static frames of image audio and video files, we can select particular any frame of video file and audio file for hidden our secret and private data. Appropriate algorithm such as LSB is using by image steganography appropriate parameter of security and authentication as like as PSNR, histogram are obtained at receiver and sender side which are precisely identical, hence data security can be increased. This paper focus the idea and plan of computer forensics technique and its using of video steganography in both investigative and security.

1.Methodology

- **LSB Technique:**

One of the latest techniques studied in the information and personal data hiding in digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file and video file is replaced with binary equivalent of secret and private message.‖ Least significant bit (LSB) coding is the easier method to embed information in a digital audio signal. By substituting the least significant bit of each and every sampling point with a binary text message, LSB coding permit a large amount of data is an encoded. Among many different data hiding techniques proposed to embed private as well as secret data within an audio video file, the LSB data hidden technique is one of Secret data into digital signals in a noise free environment, which entirely embeds the secret text message-bits in a subset of the LSB techniques of the audio and video stream. The following steps are:

a. Receives the audio and video file in the form of bytes and transmitted in to bit pattern.
b. Every character in the text message is transmitted in bit pattern.
c. By replacing the LSB bit from audio with LSB bit from character in the text message.

This proposed system provided a best and useful method for hiding the secrete data from hackers and sending it to the destination in a safe manner. This does not significant the size of the any file similar after encoding and is also correct for any type of audio and video file format

AES Encryption Process:

The encryption methods a set of particularly derived keys which is called as round key. You can take the following steps to encrypt a 128-bit block:

To keep t round the keys from the cipher key.

Firstly the state array with the block data i.e. plaintext, Cipher text

Added the initial round key to the starting state array.

Perform nine rounds of state manipulation.

Perform the tenth and final round of state manipulation.

Copy the final state array out as the encrypted data i.e.

cipher text, plaintext.

When cipher text message is processed based on bit the loop will for 9, 11, and 13 if there are 128, 192, 256 bit respectively and final round is different.

The final round has certain processes:

• Sub byte

• Shifting rows

• Mixed columns

• Added round key

IV. RELATED WORK

The paper canvass the conjunction of cryptography with adaptive steganography for audio and video sequel with chaotic algorithm as the encryption algorithm as the encryption increased the PSNR value also gets increased. The author discussed different process for audio steganography and LSB method is founded to be more and more secure. The paper discussed by LSB audio the simple methods. This mainly allows for insertion of steganography with location identification and it provides best audio quality and robustness. The paper also explains by the advanced chaotic algorithm for the encryption and decryption purpose and it consumes minimum time and fewer complexes. This section compact review the state-of-the-art of proves security to the data storing on the cloud storage. Different approaches were proposed by more scholars and few of them are mentioned down. A method was proposed by to generating a tree hierarchy of symmetric-keys by using evaluations of pseudorandom function/block-cipher text on a fixed secret. The conceptof the key aggregation can be generalized from a tree to graph.

In another system information of data owner encrypts the data, public key, data index and then uploading on the cloud server. Data owner generated aggregate decryption key by using its master-secret key, and shares the information of data to other users by sending its ADK to users via a secure E-mail on the other side the data user decrypts the data information, in this process steganography was used. Another technique can explain a special type of encryption called as key-aggregate cryptosystem which permitted user to share their own data partially across cloud storage and produced constant-size cipher text. In this technique user provide a constant-size aggregate key for different cipher text categories in cloud storage, but the other encrypted files outside the categories remain confidential.

Other process for sharing encrypted data is Attribute-Based Encryption (ABE). It is as like as to encrypt the data with attributes which are equal to users attribute rather than only encrypting every part of information data. In ABE attributes description can be considered as set so that only a particular aggregatekey which is matched with attribute can decrypt the ciphertext. The user key and the attribute are same if it same it can decrypt a particular ciphertext. When there are k attributes are overlay amongst the ciphertext and a private or secret key the decryption is permitted.

A multiple group secretes or private key management accomplishes a hierarchical access control by applying an integrated secretes or private key graph also handling the group secrete keys for different users with multiple access authorities. Centralized key managing techniques usage tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it.

V. EXISTING SYSTEM

The key-aggregate encryption process consists of five polynomial-time algorithms as follows. The data owner generated the public system parameter with the Setup algorithm and engenders a public/master-secret3 key combination through the KeyGen. Encryption of the messages to be stored on to the cloud storage can be done with the Encrypt algorithm. The master-secret key thus generated can be used to form the aggregate key in the Express process. The generated aggregate key can be sent to depute securely as an email or through portable devices. Finally, any client with an aggregate key can decrypt the data associated with this key receive though the process called as Decrypt.

1. **Setup:** This is a randomized algorithm that takes no input other than the implicit security parameter.

2. **KeyGen:** Randomly generate a public/master secret key pair (pk,msk).

3. **Encrypt (pk,i,m):** Encrypts the data m using the public Key and the index i of the cipherclass and outputs C.

4. **Extract (msk,S):** This process results an aggregate key when we input the set of indices of the cipher class along with the master secret key.

5. **Decrypt :** Decrypt is the process done by the one who receives the aggregate key obtaining the message m if and only if i ε S.

The paper discusses the different audio steganography process such as echo hiding, parity hiding, phase coding and their comparison. The author can be explains how an image can be hide in AVI video using 4LSB method. Security techniques are used to find the parameters such as frame number, height and width of the image, PSNR and histogram of the image before and after hiding. If all the verification of these parameters is find to be correct the data is send to receiver or user.

VI. PROPOSED SYSTEM

A. Key -Aggregate Cryptosystem:

In key-aggregate cryptosystem (KAC), users encrypt a text message not only under asymmetric or public-key, but also under an identifier of cipher text called as class. That means the cipher texts are further categorized into different classes. The key owner control a master-secret called master-secret key, which can be used to express secret keys for different classes. More importantly, the expressed key have can be an aggregate key which is as concise as a secret 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, A1 can send B1 a single aggregate key through by a secure e-mail. B1 can download the encrypted photos or images from

A1's InBox.com space and then used this aggregate key to decrypt these encrypted data. The sizes of cipher text, public-key and master-secret key and aggregate key in KAC schemes are all of constant in size.

B. Symmetric-Key Encryption with Compact Key:

An encryption scheme which is originally proposed for concisely converting large number of keys in broadcast scenario. The construction is very simple and we briefly review its key derivation method here for a real description of what are the desirable properties we want to achieve. The derivation of the key for a set of classes (which is a subset of all also possible cipher text classes) is as follows. A mixed modulus is chosen where A and B are two large random primes. A master secret key is chosen at random. Every class is associated with a distinct prime. All these prime numbers can be put on the public system parameter. A constant-size key for set is generated.

For those who had been deputing the access rights for S' can be generated. Howsoever, it is designed for the symmetric-key setting instead. The content provider needs to get the corresponding secret or private keys to encrypt data, which is not appropriate for many applications. Because process is used to generate a secret value rather than a combination of public/secret keys, it is unclear how to reduce the key size for achieving authentication in symmetric-key encryption. However, sharing of decryption power is not a concern in this process.

C. Attribute-Based Encryption:

Attribute-based encryption (ABE) allows every cipher text to be associated with an attribute, and the master-secret key holder can express a secret key for a policy of these attributes so that a cipher text can be decrypted by this secrete key if its associated attribute conforms to the policy. For example, with the secret key for the policy (1 ∨ 3 ∨ 6 ∨ 8), one can decrypt cipher text labeled with class 1, 3, 6 or 8. However, the major concern in ABE is collusion-resistance but not the concision of secret keys. Indeed, the size of the key often grows linearly with the number of attributes it synchronized, or the cipher text-size is not constant .In this system each cipher text is tagged by the encryptor with a group of descriptive attributes. Each and every nonpublic secret is related to access structures that species which sort of cipher texts the key will decode. We notice to decision such a theme a Key-Policy Attribute-Based secret writing (KP-ABE), since the access structure is per the non-public key, whereas the cipher texts area unit merely tagged with a group of descriptive attributes. Cloud computing is conceive as architecture for succeeding generation. It has many facilities though have a risk of attacker who can access the data or to drop out the user's identity. While setting a cloud users and service providers authentication is needed. The contribute arises whether loud service provider or user is not compromised. The data will drop out if any one of them in compromised. The cloud should be very simple, preserving the privacy or secret and also maintaining user's identity.

Computer Forensics And Authentication:

Phase coding feats the human audio systems insensitivity to relative phases of different spectral components.

- The basic idea is to share the original audio file into blocks.
- Then embed the whole message data sequence into the phase spectrum of the first block.
- One drawback is low payload because only first block is used for secret message embedding.
- The secret message is not distributed over the entire file so it can be easily removed using cropping attack.

The phase coding algorithm can be explained in the following procedure:

- The original sound signal is segmented to express the header.
- The rest portion is broken up into little segments.
- The size of this will be equal to the message to be encoded.
- A discrete Fourier transform is applied to every segment to create a matrix of phases.
- The secret message is inserted in the phase vector of the first signal segment as follows:

Using new phase matrix sound signal is reconstructed by applying inverse DFT

Key Space Analysis:

Large key space is very much important for an encryption algorithm to avoid the Brute Force attack. For this purpose we use the triple key chaotic algorithm for both information data and image encryption and decryption. The triple key provided can be used not only as a tool for encryption but can be used as a tool for embedding both images and information data in video and audio file components. The data hidden key provided in audio embedding can be used as a tool of authentication.

Audio-video analysis:

The advantage of the proposed system is that the quality of the audio and video files may not be compromised even after embedding. Since location based LSB substitution can be done in audio file, the quality and robustness is not at all disturbed, in the case of video file frames also after embedding and combining the secret image the quality of the video is not disturbed. One disadvantage is that the exact secret image cannot be retrieved since only 4MSB bits are embedded into the frame, but the overall complexion of the image can be obtained which is the best advantage of 4LSB substitution.

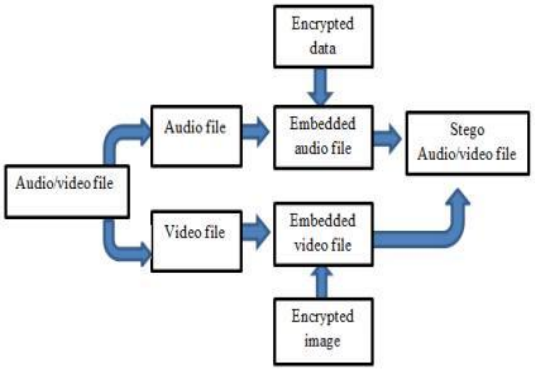

Fig 2. Block diagram of encryption text information with Authentication Audio and Video.

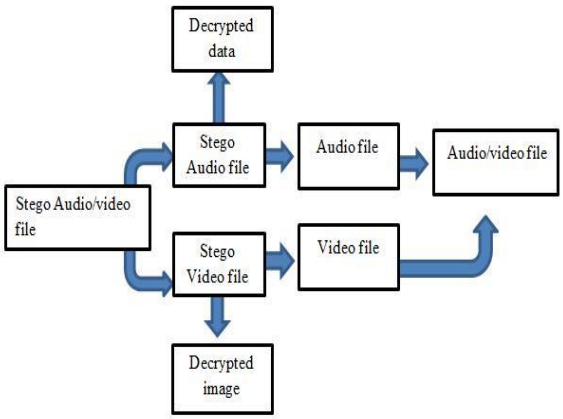

Fig 3. Block diagram of decryption text information with Authentication Audio and Video.

VII. SYSTEM ARCHITECTURE

Encryption keys always come with two flavors —symmetric (private) key or asymmetric (public) key. Using symmetric encryption, when A1 wants the data to be originated from a third party, B1 has to give the encrypted his Private or secret key; obviously, this is not also desirable. By contrast, the encryption key and decryption key are different in asymmetric-key encryption. The use of public-key encryption gave more and more flexibility for user applications. For example, in enterprises settings, every user can upload encrypted data on the cloud storage server without the knowledge of the company's master- secret key. Therefore, the best option for the above problem is that A1encrypts any files with distinct asymmetric (public) keys, but only sends B1 a single (constant-size) decryption key. Since the decryption key should be sent via a secure communication channel and kept private and secret, this key size is also desirable.

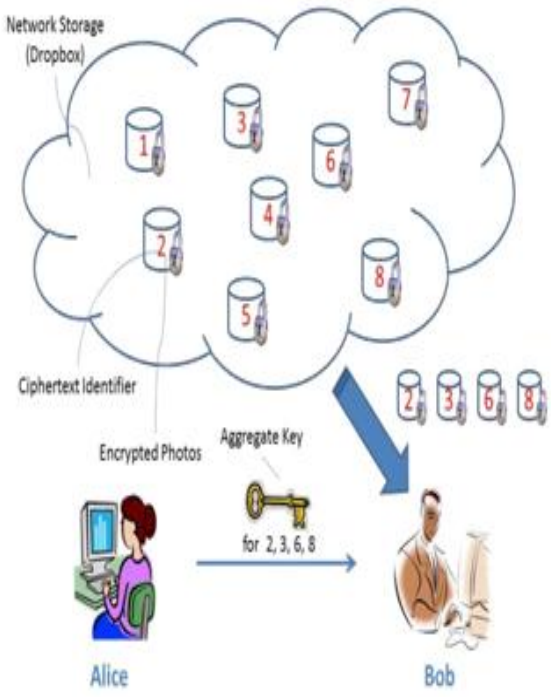

Fig 4. Using KAC for data sharing in cloud storage

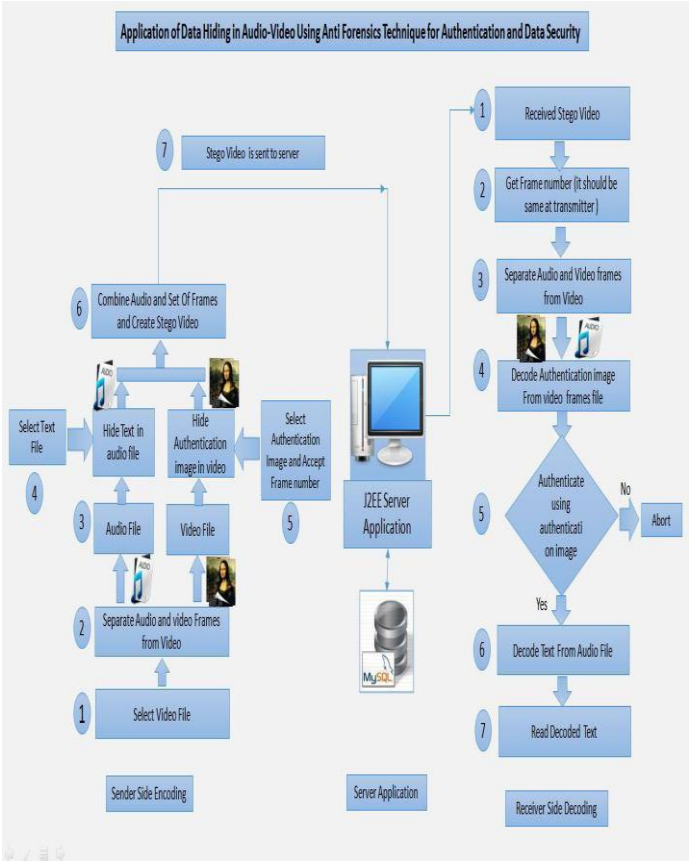

Fig 5. Architecture of Data Hiding In Audio, Video Using Anti Forensic Technique for Authentication Data Security.

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 R, ―Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm‖. International Journal of Engineering Inventions e-ISSN: 2278-7461,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 and Technology (NCRISET), 16th Nov.-2014, Pune, India,ISBN: 978-93-84209-65-0.

[6] Athira Mohanan, Reshma Remanan, Dr. Sasidhar Babu Suvanam, Dr. Kalyankar N V, Audio - Video Steganography Using Forensic Technique for Data Security, International Conference On Emerging Trends In Engineering And Management (Icetem14) 30-31, December 2014, Ernakulum, 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

