ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMPLEMENTATION OF KEY-AGGREGATE CRYPTOSYSTEM WITH STEGANOGRAPHY FOR SECURED DATA SHARING IN CLOUD COMPUTING

S.Samyuktha*, C.Vijaya, D. Durai kumar

* M.Tech-Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

Assistant Professor, Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

Associate Professor & Head, Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

ABSTRACT

Cloud Computing is vast developing technology, the challenging problem is how to effectively share an encrypted data in cloud computing. Data owner create an account in the cloud server and then generate the public/master secret key pair. The data and data index are encrypted by the data owner. This encrypted file is hidden into an image by using steganography and then uploaded in the cloud server. The data owner can release a constant-size Aggregate Key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This Aggregate Decryption Key (ADK) can be conveniently sent to others or to be stored in a smart card with very limited secure storage. They can share the data to other users by sending his ADK to those via secured E mail. Original data, index are downloaded only after verification of ADK.

KEYWORDS: Cloud computing, Encryption, Master-secret key, Steganography, Aggregate Decryption Key.

INTRODUCTION

Cloud computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services. Social networking sites and other forms of interpersonal computing activities are used; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe the environment is. Despite all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing.

Cryptosystem in cryptography refers to a suite of algorithms needed to implement a particular security service. It achieves confidentiality and allows 2 entities to communicate over an insecure channel such that an opponent can't understand what is being communicated.

The cloud verifies the authenticity of the series without knowing the user's identity before storing data [1]. The access control scheme is provided so that only valid users are allowed to access the data. It also provides user revocation and prevents replay attacks. This scheme supports for creation, modification and reading data stored in the cloud. Authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation and storage overheads are comparable to centralized approaches. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is also protected from the cloud during authentication. The access control and authentication are both collusion resistant, meaning

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

that no two users can collude and access data or authenticate themselves, if they are individually not authorized. The disadvantage is that a single Key Distribution Center (KDC) is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment.

A privacy-preserving public auditing system for data storage security in cloud computing [4] has been proposed. They utilize the homomorphism linear authenticator and random masking to guarantee that the Third Party Auditor (TPA) would not learn anything about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also reduces the users fear of their outsourced data leakage. This scheme support scalable and efficient public auditing in the cloud computing. Specifically, it achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The disadvantage is that the Encryption does not completely solve the problem of protecting data privacy against third party auditing but just reduces it to the complex key management domain and also unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

STEGANOGRAPHY

The word steganography comes from the Greek steganos and graphy. Steganos is referred as covered or secret and graphy stands for drawing or writing. Therefore, steganography means covered writing.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them.

The data to be concealed is compressed and hidden within another file. The first step is to find a file which will be used to hide the message (also called a carrier or a container). The next step is to embed the message one wants to hide within the carrier using a steganography technique.

Computer Steganography is based on two principles.

- The first one is that the files containing digitized images or audio can be changed to a certain extend without losing their functionality.
- The second principle deals with the human inability to distinguish minor changes in image color, size or audio quality, which is especially easy to make the use of objects that contains the redundant information, it may be 8-bit, 16-bit audio or 24-bit image. The value of the least significant bit of the pixel color won't result in any perceivable change of that color.

RELATED WORK

KEY AGGREGATE CRYPTOSYSTEM

A special type of public-key encryption which is called as Key-Aggregate Cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. Each ciphertext class has the separate secret key and these keys are extracted from the data owner's master-secret key. The extracted key is called as Aggregate Decryption Key. Key Aggregate Encryption scheme has the constant size of ciphertext, aggregate key, public and master-secret key. In this scheme every key has the power for decrypting ciphertexts associated to a particular index.

A novel public-key cryptography is proposed in resilient identity based encryption for cloud storage by using aggregate keys [6]. It produces constant size ciphertexts such that it gives the efficient decryption rights for any set of ciphertexts are possible. The novelty is that one can combine any set of secret keys and make them as portable as a single key. In other words, the data owner has the Aggregate Decryption Key which is extracted from different ciphertext classes in cloud server. This compact aggregate key can be conveniently sent to others through mail or be stored in a smart card with very limited secure storage.

A perfect decentralized access control scheme with aggregate key encryption for data stored in cloud was proposed in decentralized access control with aggregate key encryption for data stored in Cloud [2]. This scheme provides secure data storage and retrieval. Along with the security access policy is also provided for hiding the user's identity. This scheme is

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

so powerful since they use aggregate encryption and string matching algorithms which are very simple so that large number of data can be stored in cloud without any problem in a single scheme. The scheme detects any change made to the original file and if found clear the errors. They explain public-key cryptosystems which produce a set of constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts is possible. The best thing is that it is very easy to combine aggregate key into a single key, but encompassing the power of all the keys being aggregated. The data owner has the aggregate decryption key which is extracted from different ciphertext classes, but the other encrypted files outside the set remain confidential and very much authenticated. The advantage of this scheme is it provides secure data storage and retrieval and also the schemes detects any changes made to the original file stored in cloud and clear the errors if any changes found. The disadvantage of this scheme is it consumes more time for checking and recovery of every file.

A key-aggregate encryption scheme consists of five polynomial-time algorithms.

Setup

The data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

KeyGen

This phase is executed by data owner to generate the public or the master key pair (pk, msk).

Encrypt

This phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message m, and i denoting ciphertext class. The algorithm encrypts message m and produces a ciphertext C.

Extract

This is executed by the data owner for delegating the decryption power to the users by providing his Aggregate Decryption key.

Decrypt

This is executed by the candidate who has the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm takes input as public parameters pk, a ciphertext C, i denoting ciphertext classes for a set S of attributes.

For example Alice wants to upload her data on the server. First she need to Setup an account on the server with security level parameter(1) and ciphertext classes(n) and then the public(pk) and master-secret key(msk) is generated by KeyGen algorithm. The data and index are encrypted by Alice as Encrypt (pk,i,m). If Bob wants to access her data on cloud he need to know an Aggregate key. Alice's master-secret key is used to compute the aggregate key by performing Extract (msk,S). Then Bob can be able to download the data from the server by Decrypt (Ks,S,i,Ci).

Figure:

Alice shares her data with Bob

DATA USER / OWNER REGISTRATION

User application is created by which the user is allowed to access the data from the server of the cloud service provider. Here first the user wants to create an account and then only they are allowed to access the network. Once the user creates an account, then login into their account and requests the job from the cloud service provider. Based on the user's request, the cloud service provider will process the user requested job and respond to them. All the user details are stored in the database of the cloud service provider. In this project, the User Interface Frame is designed to communicate with the cloud server through network coding using the programming languages like Java/ .Net. In which the setup algorithm of key aggregate encryption scheme is used.

- Input: A security level parameter and the number of ciphertext classes n
- Output: The public system parameter

DATA UPLOAD WITH INDEX

The file uploaded by the data owner which is encrypted with AES algorithm and provided with public key. The data owner will upload the file in to

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

the cloud with an index value using public key. Index value and files are encrypted by the AES algorithm and stored in the cloud server. Every uploaded file has a link that will be sent to the cloud owner through an email. In which the setup algorithm of key aggregate encryption scheme is used. In which the encrypt algorithm is used to encrypt the message and its index values.

- Input: public key pk, an index i, and message m
- Output: ciphertext C

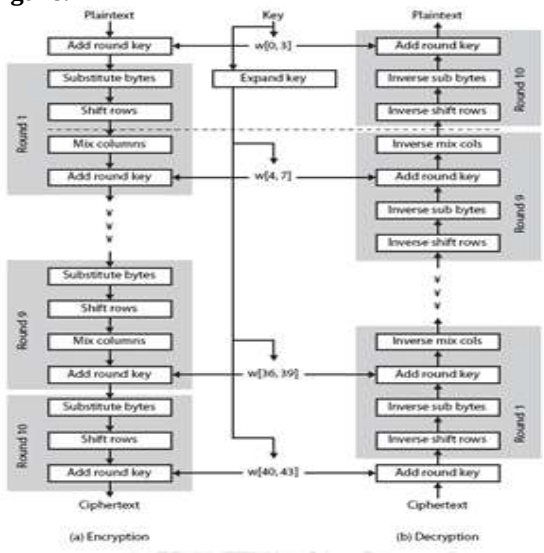
Advanced Encryption Standard

AES is a block cipher with a block length of 128 bits. The key is arranged in the form of a matrix with 4 × 4 bytes. The key matrix is expanded into a schedule of 44 words. There are 10 rounds. For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, 4) Add round key

- Byte substitution (each value of the state is replaced with S-Box value)
- Shift rows (circular left shift on each row of the state)
- Mix columns (uses matrix multiplication in GF(256))
- Add round key (bitwise XOR of current block with portion of expanded key)

For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, 4) Inverse mix columns.

Figure:



AES Structure

STEGANOGRAPHY

Steganography is the art or practice of concealing a message, image or file within another message, image or file. Generally, the hidden messages will appear to be something else: images, articles, shopping lists or some other cover text. In this module the files, index value are encrypted using the public key. The encrypt data is hidden into an image and then it will be stored in the cloud server.

ADK GENERATION

The Aggregate Decryption Key (ADK) is generated every files uploaded by the cloud owner. But this key is generated after validating the cloud owner by giving his master key (Every cloud owner has a master key while they registered in the cloud). The cloud owner generates the ADK key for every uploaded file by using this master key. KeyGen algorithm is used to generate ADK.

- Input : master-secret key mk and a set S of indices corresponding to different classes
- Output : ks defines the aggregate key for set S

USER AUTHENTICATION & DATA SHARING

The user can search the files but they cannot see the file because they need to get permission from the cloud owner even though the cloud user has his username, password and public key they need to get the permission from the cloud owner. Then the cloud owner may respond to the cloud user request by sending the ADK key and his private key to the cloud user through an email. The user can be able to see the files by entering the ADK key and private key after retrieving those keys from the owner through the email. Decrypt algorithm is used to decrypt the ciphertext.

- Input = ks and the set S, where index i = ciphertext class
- Outputs = m if i element of S

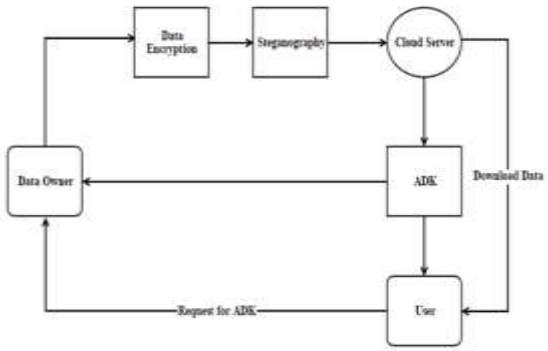
SYSTEM MODEL

This diagram describes a key-aggregate cryptosystem for secured data sharing in cloud by using steganography. The data owner can upload the files into the cloud server by apply the steganography on an encrypted data and index. The data owner's master secret key is used to generate the Aggregate Decryption Key. This key will be sent to the data owner through mail. If the user wants to access the file then they need to send the request of ADK to the data

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

owner. The data owner sends the ADK to the user through mail. The user can able to download the file after verification of ADK in the cloud server.

Figure:



System Architecture

CONCLUSION

Cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this paper, Key Aggregate Cryptosystem scheme is explained how to combine the secret keys of each cipher text classes into a single key. It is called as aggregate key. This Aggregate Decryption Key (KAC) is used to decrypt the data which is hidden into an image by means of steganography. The limitation is that a bound of maximum data to be included in image. So we can use algorithms to store more data using steganography.

REFERENCES

1. Amiya Nayak, Senior Member, IEEE, Milos Stojmenovic, Member, IEEE and Sushmita Ruj, Member, IEEE, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", 2014.
2. Mr. Ashwin Chandra C, Ms. Dharani S, "Decentralised Access Control with Aggregate Key Encryption For Data Stored In Cloud", 2014.
3. Boyang Wang, Sherman S. M. Chow, Ming Li and Hui Li, "Storing Shared Data on the Cloud via Security-Mediator".
4. Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Kui Ren, Member, IEEE, Qian Wang, Student Member, IEEE and Wenjing Lou, Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage", 2013.
5. Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records".
6. L.MohamedIrfan, S.Muthurangasamy, T.Yogananth, "Resilient Identity Based Encryption for Cloud Storage by using Aggregate Keys", 2014.
7. Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou "Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing".