ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 5, May 2016

Secure data transaction in the cloud using Steganography and Merkle Hash Tree

Marshall Desouza A, Arul K

Abstract—**Cloud Computing is considered as an effective information technology due to its resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers,are able to provide various services to cloud users.One of the important services provided by cloud providers is data storage and sharing.Due to the rapid increase in the use of cloud computing, security as well as the Data integrity becomes a major concern. The main aim is to store and share the data in the cloud in a secure manner.In order to overcome these issues the method used for Encryption, decryption algorithm isHuffmann and Advanced Encryption Standard algorithm. For secure data sharing Steganography technique and Merkle Hash Tree is used. In the proposed mechanism, the three Entities Users, Cloud Server & Trusted Third Party (TPA). Data Users are both Data Owners & Data Users. Every User register with the Cloud Server. Cloud will be generating Pair wise Keys, Primary & Secondary Keys for both Cloud Server & Data User. Users 1 wants to Access the data of Users 2 then Keys are Shared Keys are generated and accordingly the Data is authorized for Usage. In our modified process, an Access key is generated while Registration with Cloud. After that only Shared Keys are generated. Finally a Mutual Access key is generated by the data owner to the data user and sent via Email. Data User will have to hide that Mutual Key in an Image called Steganography and sent to the Data Owner. Data is accessed by only after Verifying Mutual Key using Desteganography.**

Index Terms—***Cloud, Trusted Third Party, Shared keys, Mutual key.***

I. Introduction

Cloud computing is an efficient information technology architecture for both enterprises and individuals. It is one of the important data storage and interactive paradigm with advantages, like on-demand self service, network access, and independent location resource pooling. Towards the cloud computing, a typical service architecture is anything as a service (XaaS), in which infrastructure, platform, software, and others are applied for interconnections. Recent studies promote the cloud computing evolve towards the service of internet.Security and privacy issues are the biggest concerns with the increase in popularity of cloud services. Conventional security approach mainly focus on strong authentication to realize that the user can remotely access its own data in the on demand mode.Along with diversity of application requirement, users may want to access and share each other authorized data fields to achieve productive benefits, which bring forth new security and privacy challenges to the cloud storage. An example is to identify the main motivation. In the cloud supply chain management which is based on storage, there are many interest groups (e.g.carrier ,retailer ,supplier) in the system. Each group has its own users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier may want to access a carrier's data field, but it's not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will reveal along with nothing obtained towards the desired data field. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It's not reasonable to thoroughly disclose the supplier's private information without any privacy consideration. In the cloud environment, a security protocol should achieve the following requirements. 1)Authentication: a legal user can access its own data field, only the authorized partial or entire data field can be identified by legal user, and any forged or tampered data field cannot deceive the legal user. 2) Data anonymity: any irrelevant entity cannot recognize the data and the communication state which is exchanged even it intercept the exchanged message through an open channel. 3)User privacy: any entity which is not relevant cannot know the user's access desire, which represent the user's interest in the another user's authorized data field. If and only if both the users have the mutual interest in each other's authorized data field, the cloud server will inform to the two users to realize access permission sharing. 4) Forward security: any adversary cannot correlate the two communication session to derive the prior interrogation according to currently captured message. In this paper, we discussed the aforementioned privacy issue to propose a shared authority based privacy-preserving authentication protocol (SAPA) to the cloud data storage, which realizes authentication and authorization without compromising a user's private information [1].

II. Related Work

In [2],Dalit Naor, Moni Naor, and Jeff Lotspiech deal with

Marshall Desouza A, *Computer Science and Engineering, Saveetha Unoiversity, Chennai, India,*
Arul K, *Computer Science and Engineering, Saveetha University, Chennai, Chennai, India.*

the matter of a middle sending a message to a gaggle of users specified some sub set of the users is taken into account revoked and will not be ready to acquire the content of the message. We concentrate on the unsettled receiver case, where the users do not (necessarily) update their state from session to session. We gift a framework known as the Subset-Cover framework, which abstracts a selection of revocation schemes as well as some antecedently best-known ones. We offer decent conditions that guarantees the protection of a revocation formula during this category.We describe to express Subset-Cover revocation algorithms; these algorithms are terribly versatile and work for any range of revoked users. The schemes require storage at the receiver of and keys severally (is the total range of users), and in order to revoke users the specified message lengths are of and keys severally. We additionally offer a general traitor tracing mechanism that will be integrated with any Subset-Cover revocation theme that satisfies a “bifurcation property”. This mechanism doesn't need Associate in Nursing a priori sure on the amount of traitors and will not expand the message length by abundant compared to the revocation of a similar set of traitors.The main improvements of those ways over antecedently prompt ways, when adopted to the unsettled state of affairs, are: (1) reducing the message length to regardless of the coalition size while maintaining one decoding at the user’s finish (2) offer a seamless integration between the revocation and tracing in order that the tracing mechanisms doesn't need any amendment to the revocation formula.

In [3],Yanli Ren and Dawu Gu Constructing identity based schemes is one of the new topics of current cryptography. Hierarchical identity primarily based cryptography is a generalization of identity based secret writing that mirrors associate structure hierarchy. It allows a root public key generator to distribute the employment by delegation public key generation and identity authentication to lower-level public key generators. Currently, there is no hierarchical identity based mostly secret writing theme that's totally secure within the customary model, with short public parameters and a tight reduction. In this paper, we propose associate anonymous ranked identity primarily based secret writing theme based on the q-ABDHE downside that's totally secure within the customary model. The cipher text size is independent of the level of the hierarchy. Moreover, our scheme has short parameters, high efficiency and a tight reduction.

In [4],Dan Boneh and Craig Gentry describe two new public key broadcast secret writing systems for unsettled receivers. Both systems sq. live all secure against any sort of colluders. In our first construction every cipher texts and private keys sq. live of constant size (only two cluster elements), for any subset of receivers. The public key size during this method is linear among the entire variety of receivers. Our second system is a generalization of the first that encompasses a trade off between cipher text size and public key size. For example, we attain a collusion resistant broadcast system for n users where every cipher texts and public keys sq. live of size O(pn) for any set of receivers. We discuss several applications of these systems.

In [5],LeonardoB.Oliveira, Diego Aranha, Eduardo Morais, Felipe Daguano, Julio Lopez, and Ricardo Dahab did intense analysis in the space of security and cryptography in Wireless detector Networks (WSNs) still contains a spread of open problems. On the other hand, the advent of Identity-Based Encryption (IBE) has enabled an outsized vary of recent science solutions. In this work, we argue that IBE is ideal for WSNs and contrariwise. We discuss the action between the systems, describe how WSNs can take advantage of IBE, and present results for computation of the John Orley Tate pairing over resource strained nodes.

In [6], Sherman S. M. Chow, Jian Weng, Yanjiang Yang and Robert H. Deng described proxy re-encryption (PRE) permits a semi-trusted proxy to convert a cipher text originally meant for Alice into one encrypting the same plaintext for Bob. The proxy only desires are-encryption key given by Alice, and cannot learn anything concerning the plaintext encrypted. This adds flexibility in various applications, such as confidential email, digital right management and distributed storage. In this paper, we study one-way PRE, which the re-encryption key solely permits delegation in one direction however not the opposite. In PKC 2009, Shao and Cao proposed a one-way PRE assumptive the random oracle. However, we show that it is at risk of chosen-ciphertext attack (CCA). We then propose Associate in Nursing economical one-way PRE theme (without resorting to pairings). We gain high potency and CCA-security victimization the “token-controlled encryption” technique, under the procedure Diffie-Hellman assumption, in the random oracle model and a relaxed but cheap definition.

In [7], Matthew Green and Giuseppe Ateniese described,in a proxy re-encryption scheme a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob while not seeing the underlying plaintext. A number of solutions are planned within the public-key setting. In this paper, we address the downside of Identity-Based proxy re-encryption, where ciphertexts area unit remodeled from one identity to another. Our schemes are compatible with current IBE deployments and do not need any further work from the IBE trusted-party key generator. In addition, they are non-interactive and one in all them permits multiple re-encryptions. Their security is based on a regular assumption (DBDH) within the random oracle model

In [8], Kaoru Kurosawa and Le Trieu Phong construct identity-based secret writing (IBE) and inner product encryption (IPE) schemes underneath the choice linear (DLIN) or bilaterally symmetrical external Di_e-Hellman (SXDH) assumptions. Their private user keys square measure leakage-resilient in many situations. In particular, In the bounded memory outflow model, our basic schemes reach the maximum-possible leakage rate o(1). In the continual memory leakage model (FOCS '10), variants of the above schemes relish outflow rate at least twelve o(1). Among the results, we improve upon the work of Brakerski et al. by presenting adaptively secure IBE schemes.

In [9], Ran Canetti and Susan Hohenberger described in a proxy re-encryption (PRE) theme a proxy is given special data that permits it to translate a ciphertext below one key into a ciphertext of constant message below a unique key. The proxy cannot, however, learn anything concerning the messages encrypted below either key. PRE schemes have many sensible applications, including distributed storage, email, and DRM. Previously planned re-encryption schemes achieved solely linguistics security; in distinction, applications often need security against chosen ciphertext attacks. We propose a definition of security against chosen ciphertext attacks for PRE schemes, and present a theme that satisfies the definition. Our construction is efficient and primarily based solely on the Decisional linear De-Hellman assumption in the commonplace model. We additionally formally capture CCA security for PRE schemes via each a game-based definition and simulation-based definitions that guarantee universally composable security. We note that, simultaneously with our work, Green and Ateniese planned a CCA-secure PRE, discussed herein.

In [10], Cheng-Kang Chu, Jian Weng, Sherman S. M. Chow, Jianying Zhou and Robert H.Deng, described a proxy re-encryption (PRE) theme supports the delegation of secret writing rights via a proxy, who makes the ciphertexts decryptable by the delegatee. PRE is useful in numerous applications like encrypted email forwarding. In this paper, we introduce a a lot of generalized notion of conditional proxy broadcast re-encryption (CPBRE). A CPBRE scheme permits Alice to generate a re-encryption key for a few condition specied throughout the coding, such that the re-encryption power of the proxy is restricted to it condition only.This enables lot of fine-grained delegation of secret writing right. Moreover, Alice can delegate secret writing rights to a set of users at a time. That is, Alice's ciphertexts can be re-broadcasted. This saves lots of computation and communication cost. We propose a basic CPBRE theme secure against chosen-plaintext attacks, and its extension which is secure against replayable chosen-ciphertext attacks (RCCA). Both schemes area unit unifacial and evidenced secure in the customary model. Finally, we show that it is straightforward to unifacial RCCA-secure identity-based proxy reencryption from our RCCA-secure CPBRE construction.

III. Proposed work

Cloud Computing is considered as an effective information technology due to its resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs),are able to provide various services to cloud users. One of the important services provided by cloud providers is data storage. By utilizing the cloud, the users can store the data and maintain it. Encryption and decryption algorithm are used to preserve the data files in the cloud. Cloud Storage is used to store the user's data and enjoy the high quality applications and services from a computing resources with no burden in local data storage and maintenance but the user will not have physical possession of outsourced data makes the data security as well as data integrity in cloud computing a difficult task. Due to the rapid increase in the use of cloud computing security as well as the Data integrity becomes a major concern. In order to overcome these issues Merkel Hash tree as well as Advanced Encryption Standard Algorithms are used in the proposed method. The Data owner will register with the cloud .After the user registration the cloud will generate a primary key, secondary key and access key to the data owner. The primary key and secondary key is used to generate the shared key by the cloud. The data owner login with the username and password. After login the data owner upload the image and text file. The data owner add the index key for the particular text file. While uploading Merkel Hash tree is used to split the data into many different parts with unique hash value assigned to each and every part of the data and it is also used to check whether the data which is present in the cloud storage is modified or deleted using the original data which is present in the owners database. The data which is present in the text file is encoded using Huffmann algorithm. The data user will also register with the cloud and the cloud service provider will generate separate primary key, secondary key, access key for data user also. The data user will search for a file in the cloud using the keyword. If data owner is having a particular file then data user will sent a request to the data owner to access the file. The cloud ask for the access key from the data user to check the data user liability. After the authentication of the data user the request will be sent to the data owner. Data owner will check the data user's request and if data owner accepts the request the cloud service provider will generate a mutual access key with the help of both the data owner and data user's primary key as well as secondary key. The mutual access key along with the decryption key is sent to the data user's email. The data user download the mutual key image file and it is decrypted using decryption key. The data user will enter the mutual key with the help of mutual access key the data can be shared between data owner and data user.

A. *Advantages*

- By providing the Public, Private key, access, key only the registered user will be allowed to access the data.
- Trusted party auditor will be allowed to audit the data. It will improve the trustworthiness within the user.
- Multiple level of batch auditing process is used in Merkle Hash Tree Algorithm to audit the data.

IV. Overall process design

Cloud Computing is considered as an effective information technology due to its resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSP),are able to provide various services to cloud users.One of the important services provided by cloud providers is data storage. By utilizing the cloud, the users can store the data and maintain it.Encryption and decryption algorithm are used to preserve the data files in the cloud.Cloud Storage is used to store the user's data and enjoy the high quality applications and services from a computing resources with no burden in local data storage and maintenance but the user will not have physical possession of outsourced data makes the data security as well as data integrity in cloud computing a difficult task.Due to the rapid increase in the use of cloud computing security as well as the Data integrity becomes a major concern.In order to overcome these issues Merkel Hash tree as well as Advanced Encryption Standard Algorithms are used in the proposed method.The Data owner will register with the cloud .After the user registration the cloud will generate a primarykey, secondary key,and access key to the data owner.The primary key and secondary key is used to generate the shared key by the cloud.The data owner login with the username and password.After login the data owner upload the image and text file.The data owner add the index key for the particular text file.While uploading Merkel Hash tree is used to split the data into many different parts with unique hash value assigned to each and every part of the data and it is also used to check whether the data which is present in the cloud storage is modified or deleted using the original data which is present in the owners database.the data which is present in the text file is encoded using Huffmann algorithm.The data user will also register with the cloud and the cloud service provider will generate separate primary key,secondary key,access key for data user also.The data user will search for a file in the cloud using the keyword.If data owner is having a particular file then data user will sent a request to the data owner to access the file.The cloud ask for the access key from the data user to check the data user liability.After the authentication of the data user the request will be sent to the data owner.Data owner will check the data user's request and if data owner accepts the request the cloud service provider will generate a mutual access key with the help of both the data owner and data user's primary key as well as secondary key.The mutual access key along with the decryption key is sent to the data user's email.The data user download the mutual key image file and it is decrypted using decryption key.The data user will enter the mutual key with the help of mutual access key the data can be shared between data owner and data.

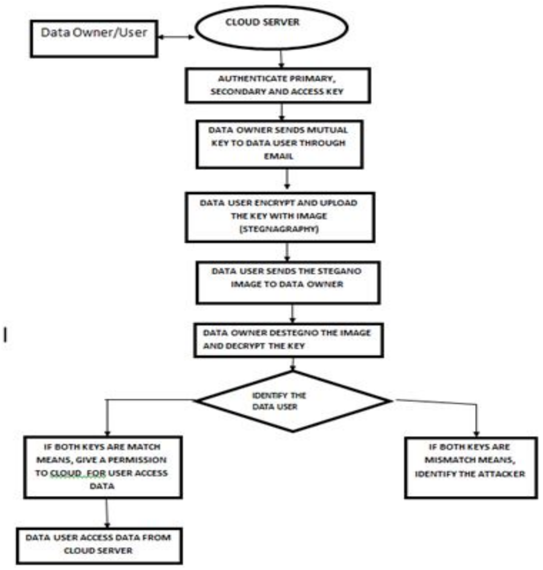
Data Owner/User
CLOUD SERVER
AUTHENTICATE PRIMARY, SECONDARY AND ACCESS KEY
DATA OWNER SENDS MUTUAL KEY TO DATA USER THROUGH EMAIL
DATA USER ENCRYPT AND UPLOAD THE KEY WITH IMAGE (STEGNAGRAPHY)
DATA USER SENDS THE STEGANO IMAGE TO DATA OWNER
DATA OWNER DESTEGNO THE IMAGE AND DECRYPT THE KEY
IDENTIFY THE DATA USER
IF BOTH KEYS ARE MATCH MEANS, GIVE A PERMISSION TO CLOUD FOR USER ACCESS DATA
IF BOTH KEYS ARE MISMATCH MEANS, IDENTIFY THE ATTACKER
DATA USER ACCESS DATA FROM CLOUD SERVER

Fig 1 overall process design

V. ALGORITHM

A. Merkle Hash Table

Step 1: A file is split up into n number of data blocks.
Step 2: Each data block is hashed and these hashes of data blocks are the leaves in hash tree.
Step 3: Nodes further up in the tree are the hashes of their respective children.
Step 4: Final hash value in a single node becomes a top hash value [11].

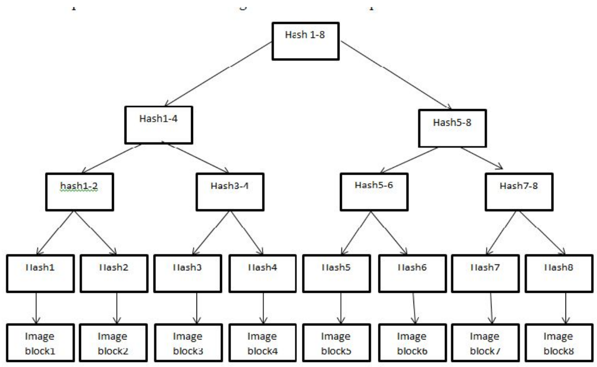

Fig 2 Example of Merkle Hash Tree

B. Huffmann Coding and Encoding

Step 1. Create a leaf node for each unique character and build a min heap of all leaf nodes (Min Heap is used as a priority queue. The value of frequency field is used to compare two nodes in min heap. Initially, the least frequent character is at root)
Step 2. Extract two nodes with the minimum frequency from the min heap.
Step 3. Create a new internal node with frequency equal to the sum of the two nodes frequencies. Make the first extracted node as its left child and the other extracted node as its right child. Add this node to the min heap.
Step 4. Repeat steps 2 and step 3 until the heap contains only one node. The remaining node is the root node and the tree is complete [12].

C. Steganography

Embedding phase is as follows
The embedding process is .
Input: Image file and the text file
Output: Text embedded image
Procedure:
Step1. Extract all the pixels present in the given image and store it in an array called Pixel-array.
Step2. Extract all the characters present in the given text file and store it in the array called Characterarray.
Step3. Extract all the characters which is present in the Stego key and store it in an array called Key- array.
Step4. Choose the first pixel and pick the characters from Key- array and place it in the first component of pixel. If there are more characters present in Keyarray, then place rest in the first component of next pixels, otherwise follow Step (e).
Step5. Place some of the terminating symbol to indicate the end of key. '0' has been used as the terminating symbol in the algorithm.
Step6. Place the characters of Character- Array in each first component (blue channel) of the next pixels by replacing it.
Step7. Repeat step 6 till all the characters which is present has been embedded.
Step8. Again place some of the terminating symbol to indicate the end of data.
Step9. Obtained image will hide all the characters which is present in the input.

Extraction phase
The extraction process is as follows.

Inputs: Embedded image file
Output: Secret text message
Procedure:
Step1.Consider the three arrays .Let the arrays be Character Array,Key array and Pixel array.
Step2.Extract all the pixels which is present in the given image and store it in an array called Pixel-array
Step3.Now, start scanning pixels from the first pixel and extract the key characters from first (blue) component of the pixels and place it in the Keyarray. Follow Step3 up to the terminating symbol, otherwise follow step 4.
Step4.If this key which is extracted matches with the receiver key, then follow Step 5, otherwise terminate program by displaying the message "Key is not matching".
Step5.If the key is valid which is entered by the receiver, then start scanning the next pixels again and extractthe secret message characters from the first (blue) component of next pixels and place it in the Character array. Follow Step 5 till the terminating symbol, otherwise follow the step 6.
Step6.Extract the secret message from the Characterarray [13].

VI. IMPLEMENTATION

A. User Registration

In this module we are going to create an user application by which the user is allowed to access the data from the Server. Here the user wants to create an account and after that only they are allowed to access the Network. Once the User create an account, they are allowed to login into their account to access the application. Based on the User's request, the Server will respond to the User. All the details of the User will be stored in the Database of the Server. In this Project, we will design the User Interface Frame to Communicate with the Server.

B. Cloud Deployment

Cloud Data Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the User information to authenticate the User when they login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Data Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job

C. TPA Deployment

Once parity added bits is added,the data will be given to the Trusted Parity auditor. The Trusted Parity Auditor will generate the signature using change and response method. The data will be audited in this module, if any changes occurs it will provide the intimation regarding the changes.

D. Shared key and Access key generation

In this module we develop a shared key and Access key,access key is generated to access the data, after that if you want to share it will provide the shared key for getting access from the cloud owner

E. Owner –mutual key generation

In this module we develop a mutual key for getting access from the cloud owner, when the cloud users want to access the files like download, then he/she has to get the permission from the cloud owner ,the cloud owner will verify the mutual key.

F. Steganography

Steganography is the art of hiding the message within another so that hidden message cannot be seen by the others. The key concept behind steganography is that message to be sent to others is not seen by the casual eye. Text is used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication.Hide the sentence into an image is called as steganography[.

G. Authentication

In this module we designed the cloud user to interact with the cloud owner .so In this module the user will search the files that is he/she can search the files but he cannot see the file because they need to get permission from the cloud owner by using the mutual key, and to share data validate the shared key

VII. CONCLUSION

Cloud computing seems to be one of the most important technology in upcoming decade. So it is necessary to identify the security issues of cloud computing time to time and addressing those security issues. This paper identified a new challenge to achieve the data security and secure data transmission in cloud computing. Authentication is introduced to guarantee data confidentiality and data integrity. Data security is achieved with the help of huffmann encoding and decoding algorithm.Secure data transmission is achieved with the help of steganography algorithm. The issue which is present in the existing system is data security and secure data transmission.With the help of Huffmann and steganography algorithm the issues can be rectified in the proposed system.

REFERENCES

[1] MHong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing," January 2015, Volume:26 Issue:1, pp 241 – 251, 2015

[2] Dalit Naor, Moni Naor, and Jeff Lotspiech, "Revocation and Tracing Schemes for Traceless Receivers,"December 2008, Volume 13, Issue 6, pp 665-669, 2008

[3] YanliRen and DawuGu, "Efficient hierarchical identity based signature scheme in the standard model," December 2008, Volume 13, Issue 6, pp 665-669, 2008

[4] Dan Boneh and Craig Gentry, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," Volume 3621 of the series Lecture Notes in Computer Science pp 258-275, 2005

[5] Leonardo B. Oliveira, Diego Aranha, Eduardo Morais, Felipe Daguano, Julio Lopez, and Ricardo Dahab, "TinyTate: Identity-Based

Encryption for Sensor Networks," http://eprint.iacr.org/2007/020, 2007

[6] Sherman S. M. Chow, Jian Weng, Yanjiang Yang and Robert H. Deng, "Efficient Unidirectional Proxy Re-Encryption," Volume 6055 of the series Lecture Notes in Computer Science pp 316-332, 2010

[7] Matthew Green and Giuseppe Ateniese, "Identity-Based Proxy Re-Encryption," https://eprint.iacr.org/2006/473, 2006

[8] Kaoru Kurosawa and Le Trieu Phong, "Leakage Resilient IBE and IPE schemes," https://eprint.iacr.org/2011/628, 2011

[9] Ran Canetti and Susan Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryptionhttps://eprint.iacr.org/2007/171, 2007

[10] Cheng-Kang Chu, Jian Weng, Sherman S. M. Chow, Jianying Zhou and Robert H. Deng, "Conditional Proxy Broadcast Re-Encryption," Volume 5594 of the series Lecture Notes in Computer Science pp 327-342, 2009.

[11] C.Kayalvizhi, S.Arun Prasath, S.ArunKumar, C.Broons Gandhi, "Secure Multi-owner Data Sharing For Dynamic Group In Cloud," March 2016, Volume:16 Issue:3, pp 119-124, 2016.

[12] Geeks for Geeks. "Greedy Algorithms | Set 3 (Huffman Coding)". http://www.geeksforgeeks.org/greedy-algorithms-set-3-huffman-coding/.

[13] Amanpreet Kaur,Renu Dhir,Geeta Sikka,"A New Image stegnography Based On First Component Alteration Technique", Volume:6 Issue:3, pp 53-56, 2009.

Marshall Desouza A,Student M.E CSE Department 2nd year in Saveetha University, Chennai.

Arul k,Associate Professor CSE Department, Saveetha University, Chennai.