Available online at www.sciencedirect.com

ScienceDirect

Materials Today: ProceedingsXX (2016) XXX–XXX

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

Efficient secure system of data in cloud using steganography based cryptosystem with FSN*

Shanthi.S , R.Jagadeesh Kannan,Santhi.S*

Assistant Professor,Valliammai Engineering College,Chennai
Professor ,VIT ,chennai. Professor,Government College of Arts and Science,Uthiramerur

Abstract

Data sharing is one of the most important functionality in cloud and one of the challenging problem is sharing data securely with others. Sharing the data with security and confidentiality on cloud with data integrity is discussed in this paper. We describe random key generation algorithm using that random sized public/master-secret key pair is created by data owner. The novelty is that data owner encrypts the data using feistal structure network along with the public key and the data index into an image and this is done by using steganography & then the data are uploaded in the Cloud Server. Aggregate Decryption Key (ADK) is mainly used to generate the Master- secret key where it is used for sharing the data to other users by transferring its ADK to those who are interested in accessing the contents through E-mail by the data owner. Original Data is downloaded only after Verification of ADK and the authentication that are done by 3D scan of finger print authentication.

Click here and insert your abstract text.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

*Keywords:*Cloud Storage;Data sharing;Fiestal Structure;Network;Key

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
*E-mail address:*author@institute.xxx

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Introduction

Data storage in cloud is popular in recent times. There is a rise in [2] demand outsourcing the data, to assist in the managing the data. [1]Data Storing is mainly considered as a main technology for many online services that are considered for social application. Nowadays almost all the files and emails can be accessed by the current wireless technology. It is possible to share the files, email, and photos with a storage capacity of 25GB and more. A [4] outdated way to ensure privacy of data is to depend on the server that imposes accessing of data. In a shared cloud computing environment, [6] Privacy and security of data become a major issue. Data are generally gathered from diverse clients that are hosted and placed on separate virtual machines (VMs) .These virtual machines are placed on a single physical machine. [7][9]VM co resident could steal the data resident by instantiating in the target VM. There are cryptographic schemes which allow third-party to access the contents that are available on the cloud. There it needs to check the availability of files without exude the data or without understanding the anonymity [5] of the owner. There is no strong belief about the confidentiality of the data in cloud. Using their private keys, the data owner encrypts the data .This encrypted data is uploaded into the server Proper security system is to be implemented in cloud server for data storage and retrieval. [10]Data upload and download is alone implemented in cloud with encryption techniques because of lack of security system in cloud.

1.1 Procedure

The functionality of the cloud computing is to share data among cloud users. In this paper, we described procedure of secure data sharing in cloud. Initially every cloud user has to own their own cloud account by registering with their details. Public Key and master secret key are randomly generated by the data owner for the data.In order to store data securely, the data owner will encrypt public key, data and data index .Then the encrypted information is hidden inside an image using the technique Steganography and the image is uploaded into cloud server.When data user wants to access the data, the search will be given for it and the request will be given to cloud server. The cloud server will send information regarding request to the data owner. If data owner is interested to share that data to the data user, then forwards the ADK along with the public key to the data user. Data user will be giving his user name, password, and Fileshis public key along with the data owner's ADK & public key to the cloud server.Cloud server will verify all those credentials and they enter into the second level of operation called authentication. This authentication is mainly done by the 3D finger print authentication which is mainly having three information that stored on the database. The three information are left, centre and right and this is more secured because if all three sides of the thumb finger match only it allows the user to enter into the server and then finally shares the encrypted data. Now user has to give the decryption key to extract the original data.

After the authentication and verification, user can download the data from the cloud server [11].

1.2 Steganography

Steganography is that [4][6] hiding of message is done in a way such that only the authenticated recipient knows that a message has been sent. Thedetection [10][5] of steganographically encoded packages is called steganalysis. Steganography hides a message and makes it invisible.

1.3 Key –Aggregate Encryption

The Key-Aggregate [2] encryption scheme contains five polynomial-time algorithm as follows.
The parameters are established by the data owner via Set**up key** by generating a master-secret key pair via key Generation. [3]Encryption is technique by which the user encrypts the plain text into cipher text thatcould be decrypted and read by the authorized user**.** By using the master secret key, the data owner for a set of cipher text classes generates an aggregate decryption key through Extraction **.**The keys that are generated are passed securely to the intended recipients. The cipher text can be decrypted with an aggregate key provided that the cipher text

- **Setup key** (1λ,n): [9][6] This is to setup account in an untrusted server by the data owner. For a Security Parameter 1 λ and n cipher text classes, the output will be param.Output param is ignored

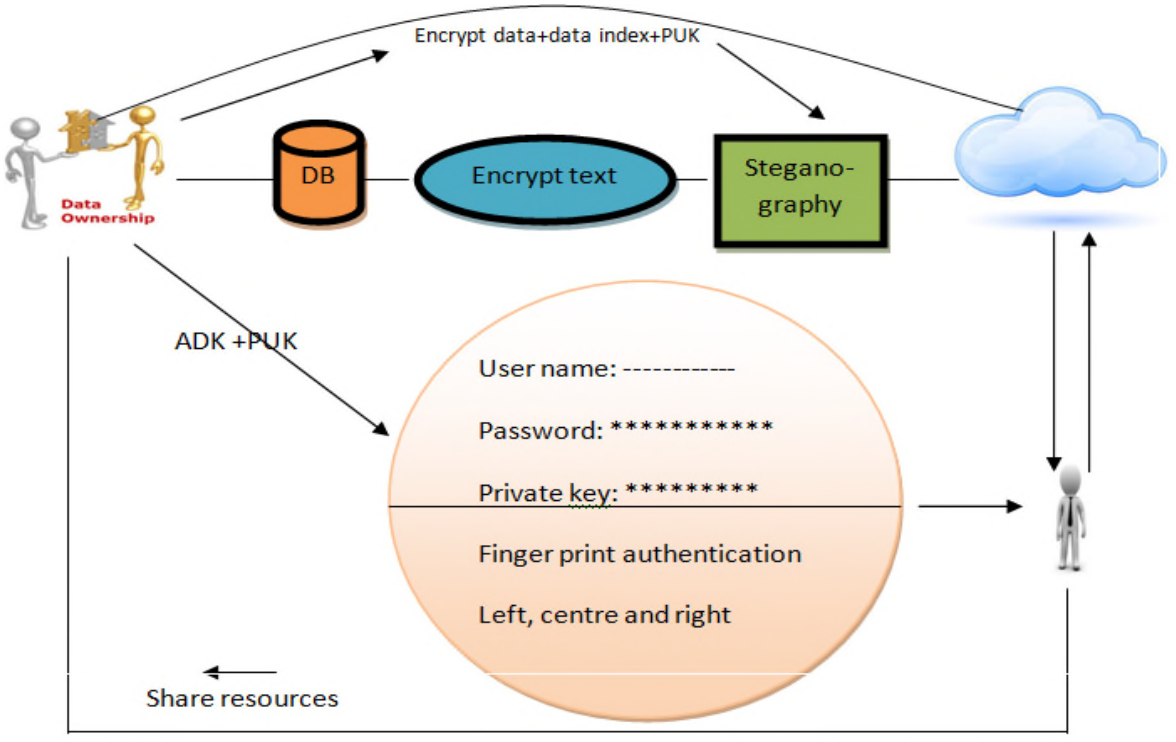

Fig .1. Steganography based encrypted data uploaded into the cloud

- **KeyGen:** [7]The random public/master-secret key pair (pk, msk) will be generated by the data owner.
- **Encryption** (pk,i,m): [11][8]performed by user who encrypts the data. For the cipher text C as an output, the authenticated user encrypts the data with the public key pk, with index I and the cipher class and the original text m.
- **Extraction** (msk,S): [3][9]Only the authorized user can decrypt the cipher text. Aggregate key denoted as K_s for set S is generated with master key msk and a indices set S
- **Decryption** (K_S,S,i,C): [5][10]Only the authorized user who receives an aggregate key K_S generated by**e**xtraction can decrypt the cipher text .Aggregate key Ks, an index I denotes the cipher class C belongs to , cipher text class C ,the delegates decrypts the cipher text resulting "m" such that the index i belongs to the set S i Є S

1.4 Feistel Structure Network (FSN):

[1] Feistal Structure is one of the Symmetric block Cipher where it encrypts and decrypts and one of the advantage is that both encryption and decryption is very similar. It is used to secure information or [4][7]data contents where it majorly done by using 3rounds or 4 rounds to generate a secure [8][5]pseudorandom function. Thus it is very safer algorithm for generating encrypt or decrypt data.

Consider F the round function and $K_0, K_1, \ldots, K_n$ the sub-keys for the rounds $0, 1, \ldots, n$ respectively. Divide the plain text into two equal parts as (L_0, R_0) For each and every

round $i = 0, 1, \ldots, n$,

Evaluate [5]

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

Then the result obtained will be the cipher text. (R_{n+1}, L_{n+1}) .[8] [7] Decryption of a cipher text (R_{n+1}, L_{n+1}) is yield by computing for each $i = n, n-1, \ldots, 0$

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i).$$

Then result obtained (L_0, R_0) is again the plaintext.

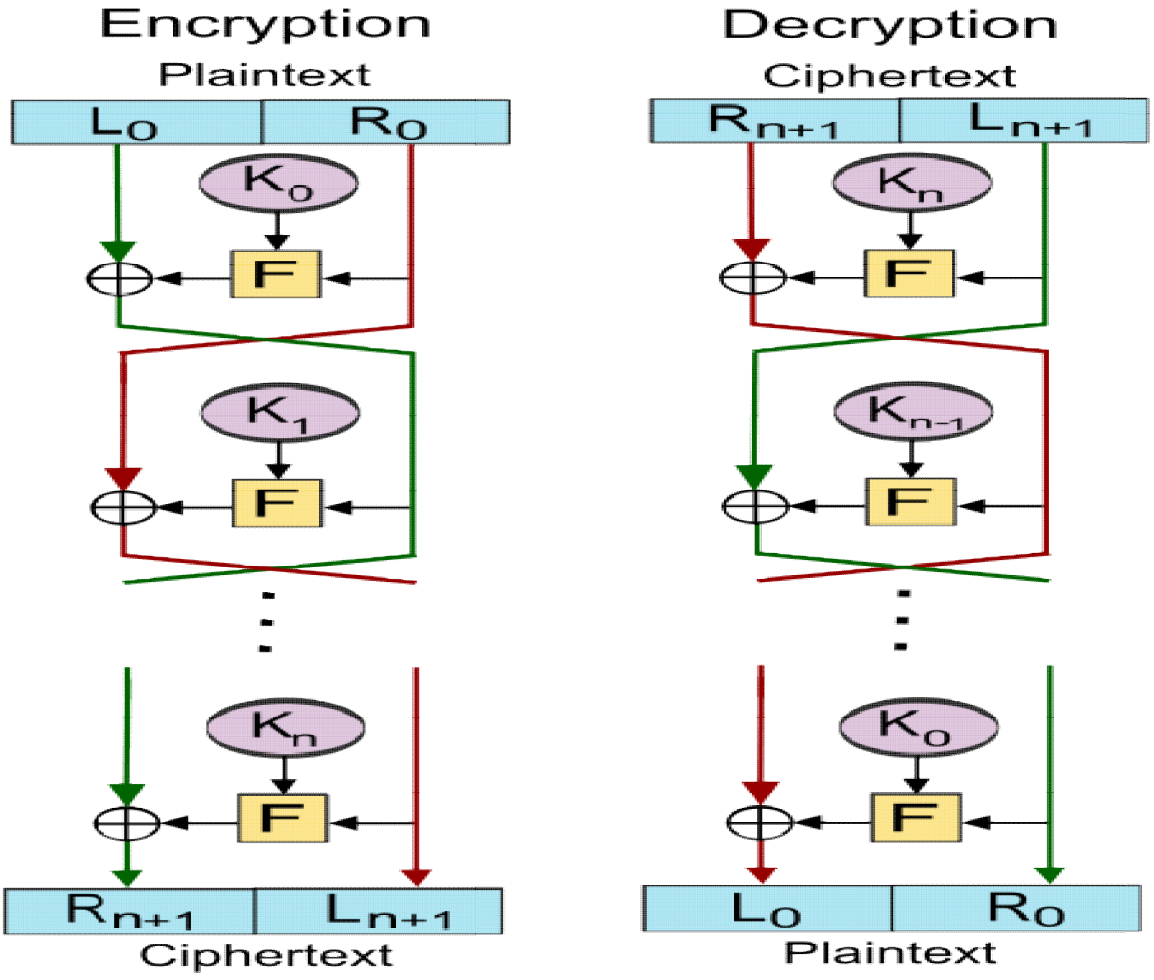

Fig.2 Fiestal Structure

1.5 *Existing System*

[9]The challenging problem in the existing is that how to share data securely. The problem can be overcome by encrypting the data, virtualization, using firewalls and packet filters. Without encrypting the user uploads the data into the cloud. The drawback of encrypting the data is that the encryption is done at course grained level by giving your private key for decryption. In attribute based encryption, the drawback is that attribute is not used as keyword for searching [10]. In Cryptographic solution to aproblem of access control in hierarchy by akl and Taylor has a problem of key management in which a central authority (CA) maintains the key and the related information. In aggregateandVerifiablyEncryptedSignatures from Bilinear Maps by DanBoneh the construction of signature requires the extra structure provided bythe bilinear map.

1.6Proposed System

Encryption of the data with master–secret key is done by the data owner. Secret key /public key is generated by the data owner randomly after creating an account in the server. Encrypted data, public key and data index are uploaded into the server. Data owner generates Aggregate Decryption key (ADK) using his secret key. User's authentication is verified by the data owner by the ADK. Original data can be accessed or downloaded only the first stage process of verification and second stage process of authentication is done by the data User. Index and the public can be downloaded only after the verification of ADK by the data ownerand the finger print that are already scanned and stored in the database are need to be authenticated. In Stenography based system ,encrypted data, public key, and the index is concealed into an image called as steganography by the data owner is uploaded into the cloud User searches the data by specifying the keyword. The request is forwarded by the cloud to the data owner if the keyword matches with that of the index. If the owner is interested to share the Data to the user, and then forwards the ADK along with the Public Key to the User. The authenticate User will give his user name, [11]ADK, Public key to the cloud server.After verification, the Cloud Server ask for the second stage process called authentication where it consider all the three sides of finger print authentication and thus all those Credentials are checked, it allows the user finally to Shares the Encrypted Data. The data User decrypts the data by the decryption key to extract the original data.

1.7Modules

- **Data User / Owner Registration**

  The user should create an account for accessing the cloud network. [1][5]Encrypted data is uploaded by the data owner into the cloud and the user downloads as needed. Interaction between the Cloud and the user is done by the Cloud service provider. The CSP will process the job requested by the user and gives response. The Cloud Service Provider stores the user detail in the Database. Communication between the user interface frame and the cloud server is through the network coding using the programming language.

- **Uploading Data with Index**

  Data Encryption is done by the Data owner using [1][7]Feistal structure network .Index value is provided with the file so as to make searching a file by the user easier by comparing the keyword with the index. This public key , index value, and data are encrypted by the Feistel Structured Network and stored in the cloud server. For every uploaded file a link will be sent to the owner of the cloud through the electronic mail.

- **Steganography**

  [1][11] The practice of concealing a stealthy messages, pictures, or file within another message, image, or file. The concealed image view as something else such as other image articles. In this paper, the text, index and the keys are encrypted. The encrypted data is stored in the cloud server after it is concealed in the image by the stenographic technique.

- **ADK Generation**

  Every registered user has a master key on cloud. ADK is generated for every uploads of the user, after validating the data owner. In this way [6][8]ADK aggregatedecryption key is generated .

- **User Authentication & Data Sharing**

  Data is [10][3]shared securely into the cloud by the by encrypting the data into an image by stenographic technique thereby the data security is preserved. The user searches the file but cannot perceive the file as the user should obtain the permission from the cloud owner as the cloud has the user name, password, public key and thus authentication is maintained. Decryption is done by the cloud user only after getting the ADK key and public key from the data owner. The data owner sends the ADK key and public key through the email. After authentication process data sharing with the user can be done.

1.8 Conclusion

Data privacy for secured data sharing in cloud seems to lack security. This technique of securely sharing the data using encryption and steganography is discussed here. We are using the technique steganography in which encrypted Outlet of original Data is done through the Feistal cipher algorithm and Public Key and Index is made steganography into an Image. The authenticated user obtains the ADK and he is need to carry out two stages to decrypt the data. Cloud would authenticate the Image along with the ADK and all those credentials are verified with the cloud data server then he allows to download Data which ensures security.

References

[1] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, “SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.
[2] Modification In Spatial, Extraction of Transform: A new approach for steganography M.Darvish Morshedi Hosseini, M.Mahdavi Information and Cryptology, 2015.
[3] Visual Cryptographic Steganography in Images P.Marwaha, Computing Communication and Networking Technologies,2010
[4]Security Improvisation in image steganography in DES Manojj Kumar Ramaiya, N.Hemaranjani, A.K.Saxena Advanced Computing Conference, 2013
[5] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, “Dynamic Secure Cloud Storage with Provenance,” Cryptography and Security, pp. 442-464, Springer, 2012.
[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’03), pp. 416-432, 2003.
[7]A Proposed Preventive Information Security System M.M.Anwar, M.F.Zafar,2007
[8] A new hybrid Security Allocation Steganography Algorithm M.B.Tayel, A.E.D.Sayed Hafz, H.S.Zied

Computer Engineering & System,2013
[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, “Multi-Identity Single-Key Decryption without Random Oracles,” Proc. Information Security and Cryptology (Inscrypt ’07), vol. 4990, pp. 384-398, 2007.
[10] Security Considerations in ITRI cloud OS Tzi-cke chiueh,E.J.Chang, R.Huang, Hogan Lee, V.Sung,M.H.Chiang, Security Technology, 2015
[11].S. Akl and P. Taylor. Cryptographic solution to aproblem of access control in a hierarchy.ACMTransactions on Computer Systems, 1(3):239–248,September 1983