ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Survey on Key Aggregate Crypto System Methods for Data Sharing In Cloud

Gore Samruddhi[1], Kakde Sonali[2], Nibe Amita[3], Sarode Meghana[4], Prof. Rakshe D. S.[5]

B.E Student, Department of Computer Engineering, PREC, Loni, Ahmednagar, Maharashtra, India[1,2,3,4]

Asst. Professor, Department of Computer Engineering, PREC, Loni, Ahmednagar, Maharashtra, India[5]

ABSTRACT: Cloud computing is a popular area of research for inventors. And it is very important in data sharing applications. On cloud the data being shared must be secure. The flexibility and the efficiency of the data is depend upon the security parameter. To achieve purpose we define new algorithms which is depend on public key cryptography and define constant size cipher text. by using these key we can decrypt cipher text.The other encrypted files except these cipher remain private. We can able to save this aggregate key or can send it to others for further data sharing The survey depicts some encryption schemes introduced inthis data privacy for securely and efficient sharing of confidential data over a secure channel. Recently research focus on aggregation of keys of the keys in signal aggregation key which is help on load of network Data sharing being important functionality in cloud storage implement show to securely, efficiently, and flexibly share data with others.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

I. INTRODUCTION

Now a day's internet is most widely used in many applications. In that cloud computing has wide scope of area, so that the data can be upload or download from cloud and can accessed easily. Large numbers of users can use data and share on cloud but present on single physical machine. But this data is not secure as user not able to control all over distributed data. The need is to share data securely among users. The assistance provider uses various authentication method to avoid the loss and leakage of data on cloud. Affection preserving in cloud is done to make sure that user's identity is not revealed to everyone. Anyone can access large amount of data on cloud as much they want i.e. only selected content can be shared. As using Cryptography user can able to share data securely on cloud. In that user can share data on cloud in encrypted format. Disparate encryption keys as well as decryption keys are develop for each bunch data. The encryption and decryption keys may be disparate for disparate set of data. Which data will be decrypted that data only share in decryption keys. In our studies we proposed public key cryptosystem which is developed cipher text. These cloud storage providers maintains all the data related operations and these are responsible for keeping the data available, protected and running. Other people uses storage capacity from the providers to store end user, they pay for that. With the help of a web service application programming interface (API) Cloud storage services may be accessed such as cloud desktop storage, a cloud storage gateway or Web content management systems.

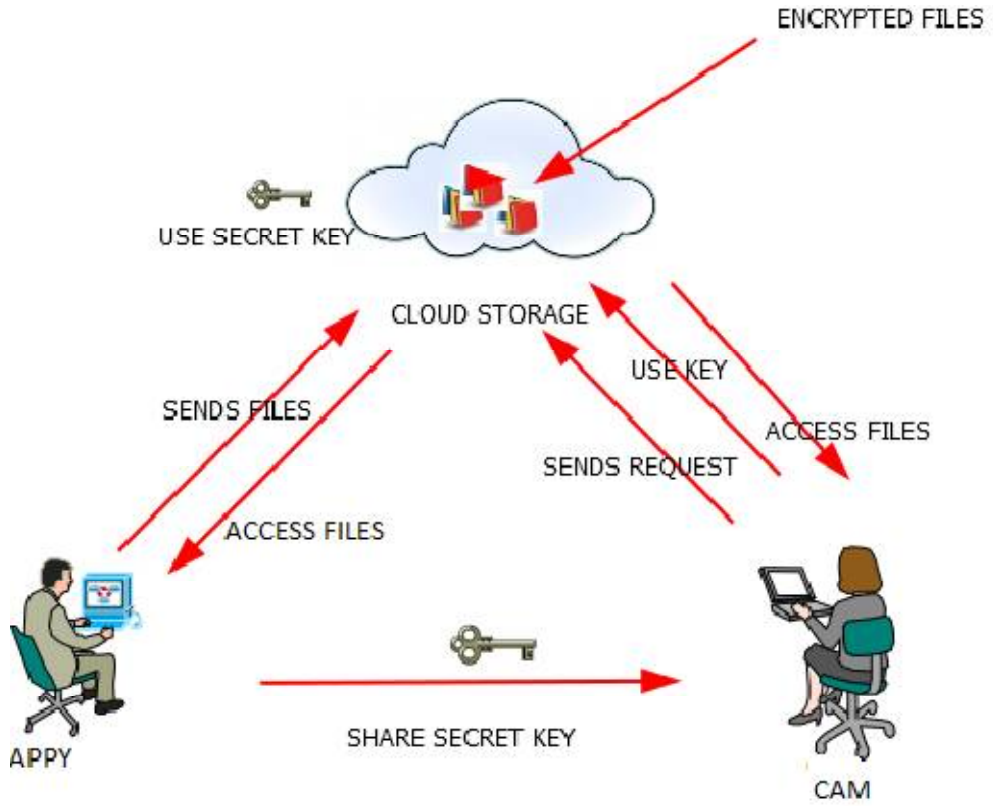
Cryptography is the way of storing and sharing the data in the form of that only those authenticated for it can access. It is the knowledge of securing the message by encoding it into an unreadable format. The main goal of cryptography is transforming data securely and user can share data safely on cloud without any attacker. This data is stored on cloud through the internet. The cloud storage is a cloud computing model in which the data is stored and remote servers are accessed from the internet.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016



The cloud storage provider is maintaining, operating and managing the cloud storage on a server. Cryptographic mechanism is used to hide the data from unauthorized users. The most encryption algorithms can be broken and the data is stolen by the attacker. So a more realistic goal of cryptography is to make gaining the data too severe to be value it to the attacker.

Fig 2.The encryption process converts plaintext into cipher text

Fig 3 the decryption process convert cipher text to plain text

Encryption is a technique of converting original message called clear text or plaintext, into unreadable format that can't understood by the attacker, called ciphertext. The user not able to access data till data cant decrypted and not convert in plain text.User not able to upload data on cloud illegally and cannot have authority to broadcast private data on insecure channels. When data is stored on a computer, logical and physical access controls are confined it. When this same susceptible data is sent over internet.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

II. LITERATURE SURVEY AND RELATED WORK

A. PREDEFINED HIERARCHICAL SCHEME

In [1], author can Predefined Hierarchical Schemes the author aims to reduce cost in storing and managing secret keys for general cryptographic use. Develop tree structure in which produce secret key for given roots and which will be used for leaf node. In [2] author proposed a technique hierarchy of symmetric keys by using reiterated evaluations of pseudo random functions block cipher on stable secret. This notion can be verbalized from a tree to a graph. In these scheme Symantec cryptosystem construct keys, required modular arithmetic for the key deviation as used in public key cryptosystems, which are more expensive than" symmetric key operation" such as pseudorandom function[3].

B. ATTRIBUTE BASED ENCRYPTION

In attribute based encryption, the data owner with master secret key can obtain a secret key for the policy of attributes so that a ciphertext can be decrypted by this key if its associated attributes conforms to policy. Each attribute is associated with data this leads to increase in size of keys. For example the secret key for the data (2V3V6V8V).we can decrypt data as using cipher text 2, 3, 6and 8.

C. SYMMETRIC-KEY ENCRYPTION USING COMPACT KEY

In [8], author presented an encryption scheme which is used for constantly transforming data and generate large number of keys in broadcasting scenarios. For encrypted data need to be secret key for each content providers and which is not able to using another application. This method used for generate one signal secret key not pair of secret keys, it is unclear how to apply this idea for public-key encryption scheme.

D. IBE USING COMPACT KEY

Identity-based encryption (IBE), [10] is a public-key encryption in which the public-key of a data user can be set as an identity-string of the user (e.g., an email address, mobile number). In that type there is private key generator(PKG) which is generate master secret key for each user with the specific user identity. The content provider can take public parameter and user identity for encrypt data.

III. PROPOSED ALGORITHM

In propose structure we are using two keys to encryption and decryption data which are secret key and its aggregate key. This structure is basically design on the basis of key aggregation encryption. The data holder creates a secrete key and public structure which is public key pair. User is responsible for data encryption and he may decides cipher text block associated with the plaintext file which want to be encrypted. The data holder have rights to use the secret key from which he can generate an aggregate key which is use for decryption of a set of cipher text blocks. The both keys can be sent to end user in very secure manner. The authenticated user having an aggregate key can decrypt any block of cipher text.

A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data holder provides the public structure parameter via Setup and generates a public/master-secret3 key pair via KeyGen. Encrypt is use for message encryption by anyonewho also decides what cipher text class is associated with the plaintext message to be encrypted. This project consist of five algorithms which are used to perform the above operations. These algorithms are as follow:

[1] Setup: The data holder executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter. The account is created on the untrusted server for sharing of data. This account is generated by data holder.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

[2] KeyGen: In these phase data holder can executes key as well as user will generate master key pair and private key. These technique used for generate public key and this key used for upload data securelyon cloudas encrypted form .User can use an aggregate key for access the block of ciphers of limited size.

[3] Encrypt: In this phase data can be encrypted by any user who want to send encrypt data. In these algorithms required input Massage, Public Key and cipher text class. This algorithms used for encrypt massage and convert that in cipher text only user can able to provide set of characteristic which is able to decrypt the message. This algorithm encrypts the data organize by the data holder by using the secrete key. This encrypted data is then share among the cloud.

- Input= public key pk, an index i, and message m
- Output = cipher text C.

[4] Extract: The aggregate key is use for extracting the particular block of the ciphers from the cipher file. But other encrypted data remains secure.

- Input = master-secret key mk and a set S of indices corresponding to disparate classes
- Outputs = aggregate

[5] Decrypt:The execution performing when user have decryption authority. The encrypted data is then decrypted by using the same secrete key which is use for decryption also user have authority to give Permissions like

- Input = kS and the set S, where index i = cipher text class
- Outputs = m if i element of S

read, write etc. to data for security and proceeds to encryption function. It encrypt data using aggregate key that key size is fixed for every user but it can be generated dynamically. Split function uploads the data but before uploading it splits the encrypted data into different parts and stored that part on different clouds. Here, Merge is the function of receiver side, it fetch the data from different clouds like C1,C2,C3…Cn. Decrypt function decrypt the date using the private key and aggregate key and proceed for the further processing.

Extractor checks wheatear that file is accessible to that user or not. In case it accessible then it decrypt from that whole bunch. Fig. 4 shows how the key's assigned to the separate users. Each user has separate key as per the aggregation cryptosystem. Basically initially grated key is recycled to generate separate user key as per their bits status.In aggregate cryptosystem authentication is imperative for each user in which user login if user login successfully then proceed for further process. User may be sender or receiver

IV. CONCLUSION AND FUTURE WORK

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among disparate users. The outsourcing of cloud data to server may causes leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for disparate cipher text classes in cloud storage. Scalable sharing of data is the main issue in cloud computing.Data owner prefer cloud to upload their data with differentusers. Uploading of data to server may lead to leakage ofprivate data of data owner to everyone. Encryption is the bestsolution, which is provided to share selected data withdesired users. Sharing of decryption keys in secure wayplays important role.Public-key cryptosystems provide delegation of secret keys for different cipher text classes in cloud storage. The delegate gets securely a constant size of an aggregate key in order to maintain limited number of cipher text classes.

REFERENCES

1. S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no.3, pp. 239–248, 1983.
2. G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology – CRYPTO'89, ser. LNCS, vol. 435.Springer, 1989, pp. 316–322.
3. G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp.243–270, 2012.
4. R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95–98, 1988
5. C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional Proxy Broadcast Re-Encryption," in Australasian Conference on Information Security and Privacy (ACISP '09), ser.LNCS, vol. 5594. Springer,2009, pp. 327–342..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

6. S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient Unidirectional Proxy Re-Encryption," in Progress in Cryptology - AFRICACRYPT 2010, ser.LNCS, vol. 6055.Springer, 2010, pp.316–332.
7. 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 DistributedSystems. Volume: 25, Issue: 2. Year :2014.
8. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ in Proceedings of ACMWorkshop on Cloud Computing Security (CCSW '09).ACM, 2009, pp. 103–114.
9. J. Benaloh, ―Key Compression and Its Application to Digital Fingerprinting,‖ Microsoft Research, Tech. Rep.,2009.
10. D. Boneh and M. K. Franklin, ―Identity-Based Encryption from the Weil Pairing,‖ in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS,vol. 2139. Springer, 2001, pp. 213–229.

BIOGRAPHY

Mr. Amol Chincholkar is M. Tech., Student at Computer Department.,Patel College of Science and Technology, Indore, India

Prof. Makrand Samvatsar is Assistant Professor at, Patel College of Science and Technology, Indore, India

Prof. Abhilasha vyas is Assistant Professor at, Patel College of Science and Technology, Indore, India

.