IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-8 E-ISSN: 2347-2693

Key Aggregate Cryptography in Cloud for Scalable Data Sharing

Sonali A. Karale[1*], Sachin D. Choudhari[2]

[1*]Department of Computer Science & Engineering, University of Bhopal, India
[2] Department of Computer Science & Engineering, University of Bhopal, India

Available online at: www.ijcseonline.org

Received: 29/Jun/2016 Revised: 14/Jul/2016 Accepted: 16/Aug/2016 Published: 31/Aug/2016

***Abstract*— Cloud computing provide facilitates computing assets on demand by the use of service provider. In IT communications cloud computing is out sourcing by the use of the Internet and maintaining own hardware and software environment. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use. Security is a prim concern in the use of cloud computing. In this paper, we have presented encryption based security algorithms for cloud computing. Data Sharing is an important functionality in cloud storage. We show how to securely share data. We describe new public key cryptosystems which produce constant size cipher text but the other encrypted files outside the set remain confidential.**

***Keywords*— Computing, Advance Encryption Standard, Dara Encryption Stancared, Key aggregate cryptography.**

I. INTRODUCTION

Today's Cloud is very popular for media of storage. We manage data using planning and strategic. High levels of data repositioning have off-putting implications for data security and data shield as well as data availability. Although, consumers know the dimensions and location of web data high in no data mobility, you can find questions associated with its security and confidentiality of the USB ports. Secure data sharing is most important today. Cloud Computing area happens to be larger to its broad network access and edibility. Secure data sharing is most important today. Cryptography technique can be applied in a two major ways- one is symmetric key encryption and other is asymmetric key encryption. In symmetric key encryption, same keys are used for encryption and decryption. By contrast, in asymmetric key encryption different keys are used, public key for encryption and private key for decryption. Using asymmetric key encryption is more flexible for our approach. There are various policies issues and threats in cloud computing technology which include privacy, segregation, storage, reliability, security, capacity and more Generally cloud computing has several customers such as ordinary users, academia and enterprises who have different motivations to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises most important problem is also security but with different Vision. Scalability is one of the major advantages of the cloud paradigm. More specifically, it is the advantage that distinguishes clouds from advanced outsourcing solutions. However, some important pending issues must be addressed before the dream of automated scaling of applications can be realized.

*Corresponding Author: Mr. Sachin Choudhari
e-mail: sachin.choudhari1986@gmail.com ,
Tel.: 9881330641

II. RELATED WORK

We take the tree structure as an example. Jon and Smith can first classify the cipher text classes according to their subjects like Figure. Each node in the tree represents a secret key, while the leaf nodes represent the keys for individual cipher text classes. Filled circles represent the keys for the classes to be delegated and circles converted by dotted lines represent the keys to be granted. Note that every key of the non-leaf node can derive the keys of its descendant nodes.

In Figure1 We represents the cloud storage network box all data storage in that area. The cipher text key 1, 2, 3 and 4, 5, 6 is the encrypted key from that storage media all the collected and aggregate. It is scalable data. There are two persons and its computer one is Jon and another is smith. Smith accepts aggregate key 2, 3, 6 from Jon.

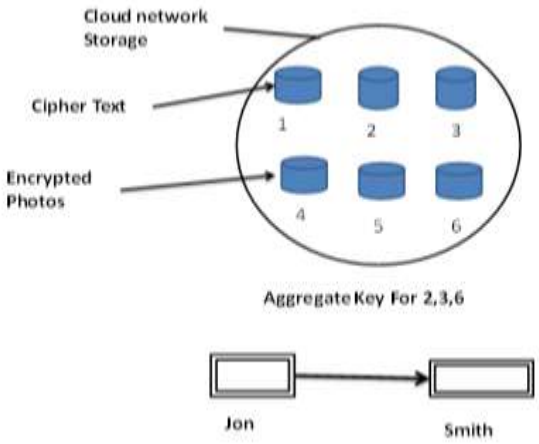

Figure1.Example of key aggregate Cryptography

III. LITERATURE SURVEY

A. **Asymmetric key encryption with Compact Key**

The construction is simple and briefly review of its key derivations process for a concrete of desire properties Encryption scheme is originally proposed for succinctly transmitting large number of keys in broadcast situation. The derivation of the key for set of classes which is a subset of all possible cipher text classes. Each classes associated with distinct prime A composite modulus is chosen where p and q are two large random primes. A master secret key is chosen at random. All these prime numbers can be put in the public system parameter. A constant-size key for set can be generated. However, it is designed for the symmetric-key setting instead. Finally, there are schemes which try to reduce the key size for achieving authentication in symmetric-key encryption.

In AES Algorithm data will be first encrypted and then sent to provider.

B. Identity Based Encryption with Compact Key

Identity-based encryption is identity-string of the user which provides public-key encryption.IBE which hold master-secret key. Provide secret key to all users from its own identification (PKG) is a private key generator. Content provider can take the public parameter and a user identity to encrypt a message. The recipient can decrypt this cipher text by his secret key in their schemes, key aggregation is constrained in the sense that all keys to be aggregated must come from different identification.

IBE is used to key aggregation. Secret keys are exponential number of only a polynomial number of them can be aggregated. Thud it increase storing cost and transmitting cipher texts text which is impractical in many situations such as shared cloud storage for example of hash function. Our schemes feature constant cipher text size, and their security holds in the standard model. In fuzzy system IBE one single compact secret key can decrypt cipher texts encrypted under many identities for an arbitrary set of identities and do not match with our idea of key aggregation.

IV.SYSTEM ANALYSIS AND DESIGN

A. Motivations

Key aggregation cloud computing is the recent workflow model in IT industry and it gives security, flexibility in data operation. To manage the security of data deployed over the cloud. We propose the technique of encryption of data, the searching in the encrypted content is quite critical. It gives the overhead of managing keys for multiple keys. We developed key aggregation system with searchable encryption.

"To design an efficient public-key encryption scheme which It supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decrypt able by a constant-size decryption key (generated by the owner of the master secrete key).

B. Problem statement

Cloud computing has given the users the accessibility to deploy number of files to the centralized cloud and share those with number of users. System needs secure storage of keys that increase the number of key management the flexibility of cloud computing always comes with the hurdles of security concerns. The data owner always needs to encrypt the files before uploading and it must decrypt before end users.

C. Public-Key Extension

User needs to classify his cipher texts into more Than n classes, he can register for additional key pairs Number of classes is increased by n for each added key. Since the new public-key can be essentially treated as a new user, one may have the concern that key aggregation across two independent users is not possible. It seems that we face the problem of hierarchical solution as reviewed.

D.DFD

Upload and Download key aggregate data

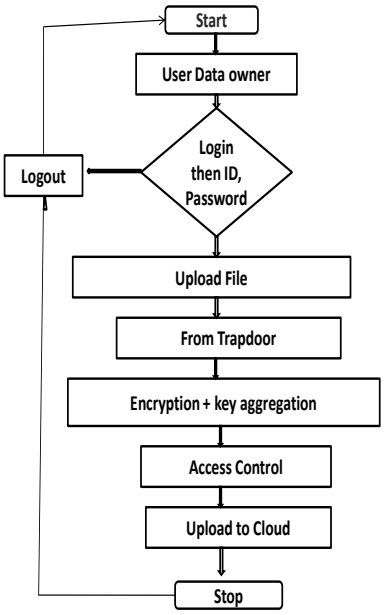

Figure2. Example of Data Upload

DFD is used for system module design structure. In figure no.2 indicate the use data or files upload from trapdoor. At the time of uploading use the encryption and key aggregation and give access to user. In figure no 3

encryption data and download data. It gives the access control for data download and upload**.** A data flow diagram (DFD) is a flowchart of the "flow" of data throughout an information system, modeling its process aspects. A DFD show the kinds of information that will give the input to the system and take output from system often they are a primary step used to create an overview of the system which can be in future it will expand and where the data we needs to stored. It does not show information about the timing of processes.

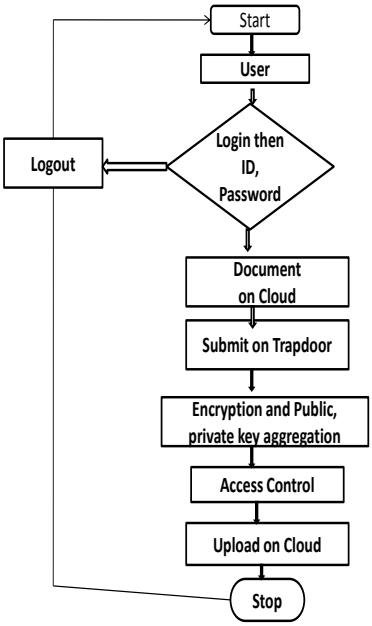

Figure 3.Example of Data Download

DFD is used for system module design structure. In figure no.2 indicate the use data or files upload from trapdoor. At the time of uploading use the encryption and key aggregation and give access to user. In figure no 3 encryption data and download data. It gives the access control for data download and upload.

V. FRAMEWORK

The data owner can use the master the master-secret key for set of cipher text classes through establishes the public system parameter is associated with the plain text encrypted message Setup and generates a public/master-secret key pair through Key Gen. Data can be encrypted by anyone who also decides what key for a set of cipher text classes through Extract Any user using aggregate key to decrypt the document. The generated keys can be passed to delegates securely through secure e-mails or secure devices Finally Key aggregate encryption schemes consist of five polynomial time algorithms as follows:

1. Setup (1 λ , n) : On the input of security levels parameter 1 λ and n is number of cipher text classes. The data owner establishes public system parameter using Setup. It provide (PARAM) as out of system parameter.
2. Key Gen: It is use to generate key private and public (P k, msk). It executed this key by data owner randomly.msk is master secret key.
3. Encrypt (pk, i, m) : Encrypt is used for encrypt data function. It is executed by data owner and for message m and index i, it computes the cipher text as C. Pk is public key.
4. Extract (msk, S): The set of S denoted by Ks. It is output of aggregate key. It is executed by data owner for delegating the decrypting power for a certain set of cipher text classes.
5. Decrypt (Ks, S, I, C): It is Decryption function for use decrypt information and it executed by a delegate who received, an aggregate key Ks generated by Extract. On input Ks, set S, an index i denoting the cipher text class cipher text C belongs to and output is decrypted result m.

System Description:-

A. System Description Let {r1, r2, -----,r_n} denote the set of resources in the system. In the group communication scenario, each resource corresponds to a data stream that is transmitted in one multicast session. Each multicast session is associated with a multicast address and a multicast routing tree [1]. The routing trees for different multicast sessions can be jointly constructed [30]. From the data transmission points of views, the users belonging to the same multicast session form a Data Group (DG). That is, one DG contains the users that can access to a particular resource. It is clear that the DGs can have overlapped membership because users may subscribe multiple resources. The users are also divided into non-overlapping Service Groups (SG) according to access privilege. One SG contains the users that are authorized to access the exactly same set of resources.

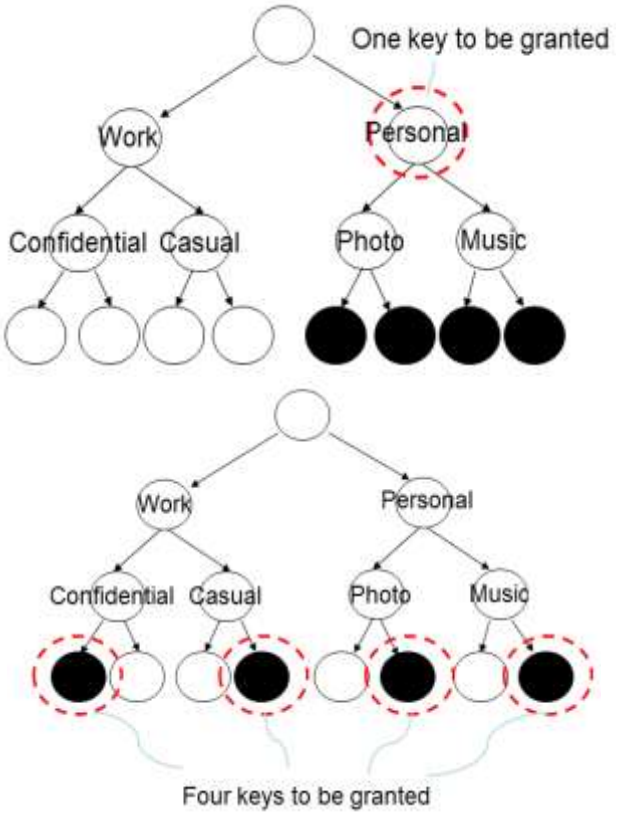

Figure 4. Example of Compact is not possibal for fix hierarchy every time

VI.ACKNOWLDGEMENT

In this paper, encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons between AES, DES and RSA algorithms. The best one security algorithm, which has to be used in cloud computing for making cloud data more secure and not any one hack by attacker. Encryption algorithms is use to comparison of different parameters used in algorithms, it has been found that AES,DES,RSA algorithm uses least time to execute cloud data, Consumes least encrypt-time, consume longest memory size and time. Two algorithms tools use by IDE and JDK for implementation. The desired output for the data on cloud computing has been achieved. In texts today's demand of cloud is increasing so the security of the cloud and user is on top concern. In future scope related several comparisons with different approaches and results to show effectiveness data privacy is question of centralized storage framework can be provided. Compress public key and secret key for create different cipher text classes in cloud.

VII. REFERANCES.

[1] Ronald L. Krutz, Russell Dean vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing" Indianapolis, Ind. Wiley Publication, First Edition - 2010,ISBN: 978-470-58987-8.

[2] Nicholas J. Daras, Michael Th. Rassias, "Computation Cryptography and network security, Springer Publication, First Edition – 2015,ISBN:978-3319182742

[3] Oded Goldreich, "Modern Cryptography Probabilistic Proofs and Pseudo-randomness" Springer Publication, 1999 Editio-1998, ISBN: 978-3540647669

[4] Peter Gutmann," Cryptographic Security Architecture", Springer-verlag Publication, First Edition-2003, ISBN:978-0387953878.

[5] Maram Mohammed Falatah, Omar Abdullah Batarfi, "Cloud Scalability Considerations", International Journal of Computer Science & Engineering Survey,Volume-05, Issue-04,Page No(1-19) August 2014.

[6] Zuzana Priscakova and Ivana Rabova, "Model of solution for data security in cloud computing", International Journal of Computer Science, Engineering and Information Technology, Volume-03,Issue-03,Page no(1-18),June 2013.

[7] Anisaara Nadaph And Vikas Maral "Cloud Computing – Partitioning Algorithm and Load Balancing Algorithm" International Journal of Computer Science, Engineering and Information Technology,Volume-04, Issue-05,Page no(1-4) October 2014.

[8] Satish s Hottin and Mr. S. Pradeep," "Efficient Secure Date Sharing In Cloud Storage Using Key-Aggregate Cryptosystems", International Journal of Engineering Development and Research, Volume-03, Issue-02, Page no (38-44), May 2015.

[9] Mithun V Mhatre1, Dr. M. Z. Shaikh, " Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage-A Review", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 7,Page no(1-4)July 2015.

[10] G.Tzeng, "A Time:-Bound Cryptography key assignment scheme for access control in a hierarchy", IEEE Trans. Knowledge and data engineering,Volume-14,Issue-01,Page no(182-188)Feb-2002.

[11] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptography for scalable data sharing in cloud storage", IEEE Transactions on parallel and distributed system,Volume-25,Issue-02,Page no(468-477),Feb-2014.

[12]Overview of Cryptography, www.garykessler.net/library/crypto.html,Aug 7, 2016.

[13] Encryption Algorithm www.storagecraft.com/blog/5-common-encryption-algorithms,31 July 2014

[14] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications, "org by-at The convention and exhibition center ,Hong Kong in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM'04). March 7-11, 2004.

[15] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions",Proceedings of the 13th AC conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[16] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th AC conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

Authors Profile

Ms Sonali .A. Karale pursed her Master Degree in Computer Science & Engineering from Shri Balaji Institute of Technology & Management, Betul, University of Bhopal, Madhya Pradesh, India in year 2014. She was working as Assistant Professor in Department of Computer Science & Engineering, IBSS College of Engineering, and University of Amravati. India. Her main research work focuses o Cryptography, Cloud computing, Network Security she has published 3 research papers in reputed international journals. She is 2 year of teaching experience.

Mr Sachin D.Choudhari completed his Ph. D. He is Associate professor And Principal in Computer Science and Engineering of Shri Balaji Institute of Technology & Management, Betul, and University of Bhopal, India. since 2014. His main research work focuses on Cryptography, Data Mining, Network Security. He is M-Tech Project Guide of Ms. Sonali Anil Karale and helping her research.

