ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

Research Paper

IMPROVED AGGREGATED KEY CRYPTOSYSTEM FOR SCALABLE DATA SHARING IN CLOUD STORAGE

SHIVANGI MISHRA[1], SAHANA T EDWIN[2]

1. **M. TECH. SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, BTIRT, SAGAR, (M.P.) INDIA**
2. **PROF. & HOD, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, BTIRT, SAGAR, (M.P.) INDIA**

ABSTRACT

Data sharing is a essential functionality in cloud storage .With the Internet technology and the usage of it in different smart devices, the sharing of data has become very easy. Data sharing has become an important feature to be considered in cloud Computing. The users who use cloud want their files, folders, pictures and other confidential things to be available for their utilization in cloud storage. It is essential to safely, productively, and adaptable impart important information to others in distributed storage. A special type of public-key encryption which is called Improved Key-Aggregation Cryptosystem is designed to outline an effective scheme that helps in flexible delegation by a constant-size decryption key. The uniqueness of this approach is that one can aggregate any set of secret keys and make assemble as compact as a single key, but passing the decryption power of all the keys that is being aggregate. In cryptography, a fundamental problem is influence the secrecy of a small piece of knowledge into the capability to perform cryptographic functions multiple times. Here the efforts are taken for developing the powerful decryption key, which permits decryption of different cipher texts without expanding the size of aggregate. This scheme performs well in the standard model and can be applicable in cloud storage anytime.

KEYWORDS

Cloud storage, data sharing, cipher texts, powerful aggregate key.

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

I. INTRODUCTION

Cloud computing is the new storage trending model used for computing. Internet is used in cloud computing for communicating and storing the data. Some of the most vital functionalities of cloud computing is data security, data sharing and securely storing the important data dumped into cloud. When cloud computing comes to data sharing and data storing , the users of the cloud become a bit uncertain to put the data onto the cloud. They were scaring about the security and confidentiality of the data. Due to these aspects to ensure the security and confidentiality of the data, the concept of encryption came into existence. For this, the users are able to encrypt their data using various encryption algorithms before going to put them into the cloud. If user have problem for encryption they can also take the help of the third party key generators for encryption and decryption of data or can encrypt by themselves using various algorithms.

Cloud storage is being popular day-by-day. It is being utilized as hub equipment through various online services. In today's world some service provider offer to users for free accounts for data sharing, emails, and storing confidential information with storage size up to 25 GB. The wireless technology enables some key points to us to access almost all the files, emails and data for the users through their smart devices from any remote site of the world. In cloud storage Data sharing is a prime functionality. Today some blog writers also allow their followers to access some of the confidential materials.

Among the various materials dumped into the cloud, organization may allow their employees to access a small amount of their confidential data. So it is the challenging job to sharing the encrypted data with only the authentic users, who are given the rights to access it. Although users have the option of downloading the encrypted data from the cloud, decipher the data, and later send ti to their friends for further sharing it, but this will simply reduce the impact of cloud storage environment.

Instead the authentic users must be given the rights for accessing data and sharing with others in such a way for accessing those data directly from the server. Cloud Storage is a prime service where data is maintained, managed, and backed up through remotely. This service is available to cloud users over the network, which is usually the internet. It allows the user to store files online so that the user can access them later from any location via the internet [4]. The cloud concept that has recently become the technological hot topic is actually very old. It has roots dating back to the 1950's and 1960's. Computer scientist John McCarthy has been credited as one of the founding fathers of the cloud computing concept. Cloud storage is a subcategory of the complex cloud computing environment. It is a service model in which data is:

Maintained, managed and backed up remotely and made available to users through a network (Internet).

The FilesAnywhere.com was one of the first companies to offer the cloud storage services. Their cloud storage service enables users to store data on their servers from anywhere throughout the world at any time, while being able to retrieve their data from anywhere at any time. FilesAnywhere.com would become a pioneer in the area of cloud storage business and many companies follow it [6].

In cloud storage data sharing functionality is important. Consider Alice has some data, she want to store in the cloud and does not want expose it to in front of anybody. She first encrypts the data and then uploads it into the cloud server in such order to avoid data leakage [10] [16]. If Bob needs some data of the Alice then he give requests to her, to share the data. Now the main job is sharing of the encrypted data. There are ways to do this. 1) Alice can encrypt the data using single key and share the same key with Bob. 2) Alice can encrypt the data with different keys and then send key to Bob using secure medium.

In the first approach, the data that is not required to be exposed may also get exposed to the bob while the second approach the numbers of keys required increases as the number of files and the number of users want to share the data. The storage space required to store the key and secure channel to share it also becomes expensive. Encrypting the data using the different keys by the Alice and sending the single key for the decryption of the constant size to the Bob is the best solution. The decryption key has to be sent through the secure channel and the size of the secret key is smaller and enviable. The public key encryption scheme is supportable and is flexible such that any encrypted data is decrypt able by constant sized decryption key. Here we face some problem that how the data is efficiently stored in cloud computing. The user directly upload the data into cloud using the drop box without encryption, so the attacker can easily attack and it leads to missing data integrity and provides less security[2].

In the proposed method the data owner generates the public key after the account is created. He encrypts both the data and the public key upload in the cloud. The data owner also generates the aggregation detection key (ADK) using the public key. Data owner generates Aggregate Decryption Key (ADK) using its Public key [9] [13]. Data owner can share the data to other users by sending its ADK to those via Secured E-mail. After the verification of ADK, the other person can download the original data [15] [7] [8]. Data owner shares both the selected file and the ADK in order to download original data [4] [7]. Authentication of the file with ADK in the remote

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

cloud ensures security. It provides confidentiality and data integrity [9] [11] [12]
[14].

The encryption of the data came into picture to secure the confidential data of the user. This encryption involves generating and sharing of the secret keys. These secret keys' size varies for the different encryption schemes based on the length of files. There is a need for keeping the key size constant. The use of single aggregate key for decrypting data will avoid the burden of sharing many single secret keys. The aggregate key size should remain constant so that the network overhead can be reduced. This will also reduce the fuss of sharing many keys for deciphering the encrypted files.

As more and more enterprises and people are moving to cloud it is becoming crucial for people to get the security for the privacy of their data. Since data is a very essential thing to be secured and taken care, the data needs to be encrypted prior to putting onto the cloud. The aggregate key can be generated for any number of files that are dumped into the cloud. This aggregate key size remains constant using which the decryption of those files is possible for which the rights to access are given.

With the property of lower maintenance cost, cloud computing also makes it possible to share the files, data and other crucial information among cloud users. Unfortunately, preserving the privacy of the data from an un-trusted cloud is still a challenging issue. This project proposes a secure data privacy scheme, for user data in the cloud. The proper verification and validation of the user is done before uploading or downloading of the files into or from the cloud. The sharing of secret keys is done in a secured way by sending them in encrypted format through the e-mails.

Comparing our basic KAC technique with different techniques of sharing data in cloud storage like Cryptographic Keys for a Predefined Hierarchy, Compact Key in Symmetric-Key Encryption, Compact Key in Identity-Based Encryption (IBE) ,Attribute-based encryption (ABE) , the results are listed in following table-

TABLE I
COMPARISON BETWEEN KAC AND OTHER SCHEMES

	Decryption Key size	Ciphertext size	Encryption Type
Key Assignment Schemes for predefined Hierarchy	Non constant	constant	Symmetric key or Public key
Symmetric key Encryption with compact key	constant	constant	Symmetric key
IBE with compact key	constant	Non constant	Public key
Attribute based Encryption	Non constant	constant	Public key
IKAC	KAC	constant	Public key

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

II. OUR CONTRIBUTION

Cryptography is an amazing technique by using this; various users can access data from other users. The Improved Key- Aggregate Cryptosystem (KAC) [1] generates great results, it reducing the computational complexity of the overall algorithms. The IKAC aggregates various cipher texts into cipher text classes and each and every class holds a secret key from which the aggregate key could be generated. This aggregate key holds the decryption power of any subset of cipher text classes.

We use blowfish algorithm to propose IKAC to perform the encryption and decryption process. Since Blowfish has a 64-bit block size and a variable size key length from 32 bits to 448 bits and keeping it ideal for securing the data. It is a variable-length size key block cipher. It is suitable for those applications where the key usually not change often, like a communications channel or an automatic file encryption. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for IDEA or DES. It has been analyzed as considerable, and it is slowly gaining acceptance as a strong encryption algorithm it is much faster when it is compared to other symmetric algorithms.

III. EXISTING SYSTEM

The Improved key-aggregate encryption process comprises with five polynomial-time algorithms as follows.[1]-

The data owner develops the public system parameter with the 'setup' algorithm and generates a public/master-secret3 key pair through the KeyGen. The process of Encrypting the messages and stored it on to the cloud can be done with the help of Encryption algorithm. Thus the generated master-secret key can be used to form the aggregate key in the Extraction process. The generated aggregate key can be sent to delegate securely through an email or through portable devices. Any client with an aggregate key can decrypt the data associated with this key receive though the process called Decryption.

1. Setup: This algorithm is a randomized in nature that takes no input accept implicit security parameter.
2. KeyGen: randomly generate a pair of public/master secret key (pk,msk).
3. Encrypt (pk,i,m): Use public key and the index i of the cipher to Encrypts the data m using the class and produce outputs C.
4. Extract (msk,S): when we input the set of indices of the cipher class along with the master secret key produce results of an aggregate key
5. Decrypt: decryption of the message is done by the one who have the aggregate key obtaining the message m iff i ε S.

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

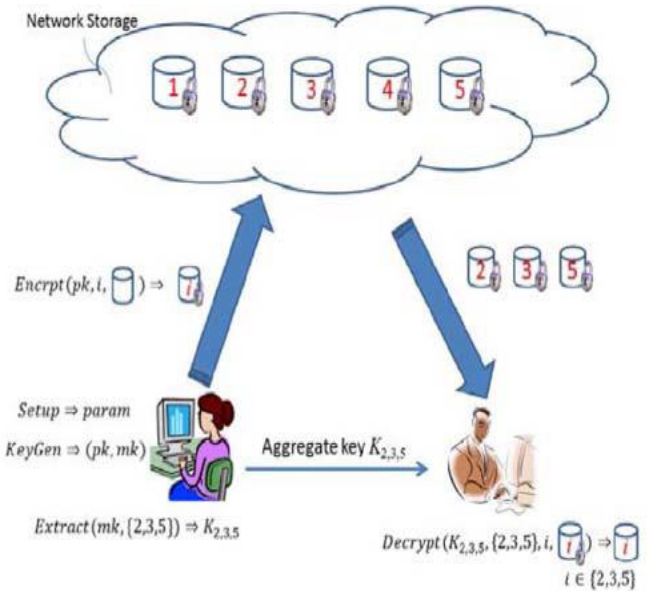

Fig. 1 Data sharing using IKAC

IV. PROPOSED SYSTEM

The proposed system is based on the Blowfish algorithm which was designed in 1993 by a great scientist Bruce Scheier as a swift, substitute to accessible encryption algorithms like DES, 3DES and AES etc. Blowfish algorithm is a symmetric block encryption scheme which provide,

Fast: Data encryption takes place on 32-bit microprocessor at a rate of 26 clock cycles per byte.

Compact: To execute efficiently, 5K of memory is more and enough.

Simple: It keeps use of XOR, addition, lookup table with 32-bit operands.

Secure: The key length is variable, it can be in the range of 32 to 448 bits: default length 128 bits key.

It is appropriate for applications like communication link or an automatic file encryptor, where the key does not alter often.

It does not have a patent and also it is royalty-free.

Description of Algorithm:

Improved Key Aggregate Cryptosystem is a symmetric block cipher algorithm which encrypts block data of 64-bits at a time. This algorithm is mainly divided into two parts.

1. Key-expansion
2. Data Encryption

1. Key Expansion: the key expansion process converts a key of 448 bits into numerous subkey arrays making it to a

size of 4168 bytes. IKAC makes use of a large number of sub-keys. These keys will be generated earlier to any data encryption or decryption.

The p-array consists of 18, 32-bit sub-keys:

P1,P2,P3……,P18

Four 32-bit S-Boxes consist of 256 entries each:

S1,0, S1,1,S1,2……..S1,255

S2,0, S2,1, S1,2……..S2,255

S3,0, S3,1,S1,2……..S3,255

S4,0, S4,1, S1,2.....S4,255

2. Data Encryption: Data encryption is having a function to iterate the function 16 times of network. Each separate round consists of a key-dependent transformation and a key and data-dependent changeover. All operations performed are XORs and the additions on the 32-bit words.

The only supplementary operations to the above functions are four indexed array data lookup tables for each round.

Divide x into two 32-bit halves: xL, xR

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

For i = 1to 16:

xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

Implementations of Blowfish require the fastest speed should unroll the loop and ensure that all sub-keys are stored in cache.

V. RESULT ANALYSIS

Compared to all other algorithms the IKAC algorithm has made its mark in the cryptographic field. The strength of the encryption algorithm is mainly depended upon the key length. Bruce, originator of the encryption algorithm, has calculated that according to quantum mechanics what we know today , that the entire energy output of the sun is insufficient to break a 197-bit key. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode used.

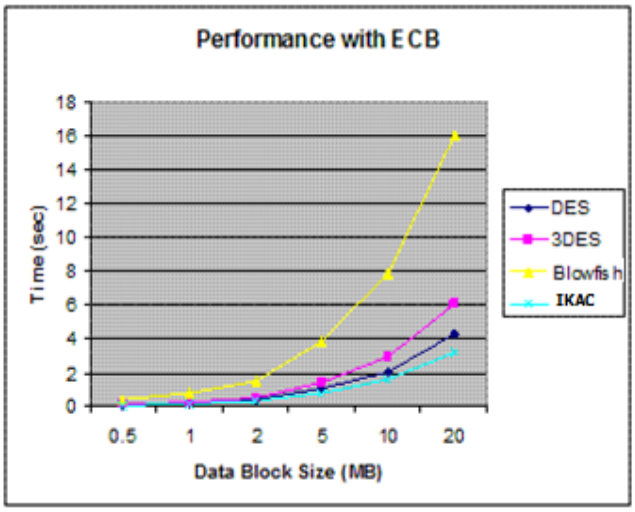

Fig 2 Encryption performance comparison with ECB

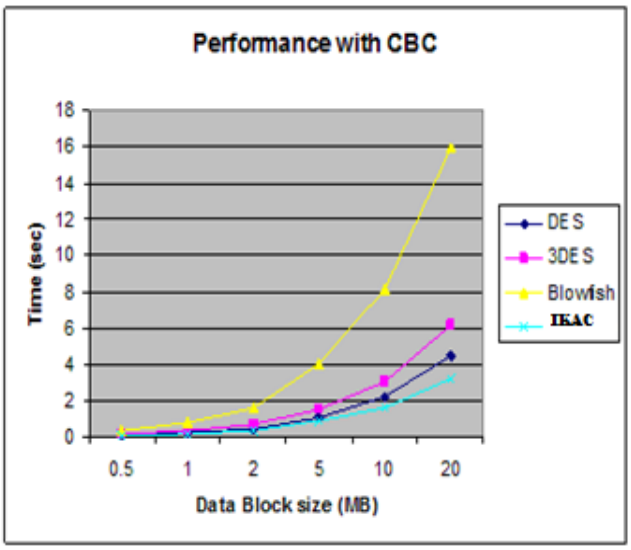

Fig 3 Encryption performance comparison with CBC

VI.CONCLUSION

Thus the IKAC algorithm is implemented in given system. The results shows that IKAC is much more advantages when compared to the performance of many other algorithms. Since IKAC has not any known weak points related to security so far, this makes it an excellent algorithm to be considered as a standard encryption algorithm.

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 3 , MARCH -2017

REFERENCES

[1] Cheng Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage , IEEE Transaction on Parellel and Distributed System, vol. 25, no. 2, February 2014.

[2] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, " Privacy- Preserving Public Auditing for Secure Cloud Storage ," IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[4] Milind Mathur, Ayush Kesarwani, " comparison between DES , 3DES , RC2 , RC6 , Blowfish and AES, " Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[5] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009

[6] M. Evans, T. Huynh, K. Le and M. Singh," Cloud Storage", 2011.

[7] S. S. M. Chow, Y. Dodis, Y. Rouselakis and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010.

[8] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.

[9] B. Alomair and R. Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication," J. Universal Computer Science, volume 15, Issue 15, pp. 2937-2956, 2009.

[10] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," Proc. IEEE INFOCOM '04, 2004.

[11] S.S.M. Chow, J. Weng, Y. Yang and R.H. Deng, "Efficient Unidirectional Proxy Re-Encryption," Proc. Progress in Cryptology, Volume 6055, pp. 316-332, 2010.

[12] D. Boneh, C. Gentry and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," Advances in Cryptology Conference, Volume 3621, pp. 258-275, 2005.

[13] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology, volume 2139, pp. 213-229, 2001.

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, Volume 9, Issue 1, pp. 1-30, 2006

[15] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Theory and Applications of Cryptographic Techniques, Volume 3494, pp. 457-473, 2005.