ISSN:0975-9646

Secured and Scalable Data Sharing by Authenticated User Using Key Aggregate Cryptosystem Technique

Shreya Kulkarni[#1], Punam Channa[#2], Chandani Madavi[#3], Prof. D. A. Kulkarni [#4]

[#]*Department of Computer Engineering, Pune*
Vidyarthi Griha's College of Engineering and Technology, Pune, India

***Abstract*— User's data is stored remotely on cloud server. Many of the online services are provided by cloud computing.This paper aims at secure data sharing in cloud storage by using key aggregate cryptosystem. It more focuses on aggregation of secret keys and making them compact as a single aggregate key. Master (user) produces constant size cipher text keys which can be stored in any kind of storage. Aggregate keys are shared via secured communication. Client uses aggregate keys given by the user and decrypts the shared data. Hence complete authenticate communication is achieved. Authentication of user is achieved using SHA algorithm.**

***Keywords*— Scalable Data, Cloud (SAAS), Aggregate Data, LFSR Algorithm, SHA-1 Algorithm**.

I. INTRODUCTION

Cloud storage is one of the major functionality now a days. It is gaining popularity because of various services[7]. Many personal applications currently use cloud computing for various online services. After authentication access control is enforced by relying on server to maintain data privacy[1].

Hence a major solution is given which is based on cryptographic system. Whenever user have trust issues on the server, a novel idea is considered where user encrypts his own data with their own keys before uploading data to the server[1]. Security of communication is achieved by using SHA algorithm where authentication of user is verified and only authenticated user can send request of data to another user[3].

Once secured communication is established sharing of particular data is achieved by key aggregate cryptosystem where keys are generated in 32 bit size and hence enhances the flexibility of particular user and data shared[2]. Variable size keys can also be produced by using LFSR algorithm so that there may not reside any constraint. It can be 8 to 16, 32 to 64 bits.

II. LITERATURE SURVEY

Literature survey comprises of two parts which describes present work as well as proposed work.

A. Present work:

Data sharing is an important functionality in cloud storage. In this existing system,[1] user provides an untrusted servers, say a proxy operated by a cloud service provided with a transformation key that allows the latter to transfer any Attribute- Based Encryption(ABE) ciphertext satisfied by that user attributes or access policies into simple ciphertext(CT).Here sharing of data takes place through encryption and decryption of data through keys. Any user can send request to supplier for required data.

B. Proposed work:

Overcoming limitations we are proposing a new system. People don't trust current systems due to privacy purpose[1]. Exchange of information is a vital functionality in cloud storage. This paper represents security, and flexibility sharing of data with others in cloud storage. Key aggregate system produces variable size keys due to which privacy can be achieved while data sharing. Basic fundamental idea is that all the secret keys are aggregated together into one aggregate key which can be sent for information sharing. So instead of sharing multiple secret key each time for different class we share 1 aggregate key which encompass power of all secret key.

So basically secret key holder will create only one aggregate key for exchange of the data for a particular set of the data and outside particular set data will remain confidential in class.

We will take an example of dropbox for illustration (refer fig 1). Suppose Alice is interested to upload all here private data on Dropbox and due to privacy issue she is interested to expose her photos only to friends and family not to everyone. Due to various data leakage possibility Alice is not comfortable on DropBox privacy mechanisms so she encrypts here own data and uploads on Dropbox

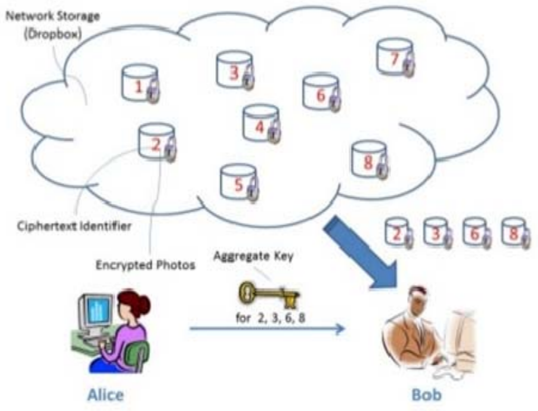

Fig 1. Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key.

III. FRAMEWORK

A. Authentication:

Cryptography is one of the major paradigms for privacy as well as security purpose. This paper represents **SHA-1** algorithm which based on the hash function. Design of SHA-1 was completed by the United States National Security Agency. Algorithm of SHA are classified into 3 types and are known as *SHA-0*, *SHA-1*, and *SHA-2*. SHA-1 are somewhat similar to SHA-0, only corrects some errors in the original SHA hash specification that led to significant weaknesses. Out of all SHA algorithms, the most widely used of the existing SHA hash functions is SHA-1, and is employed in several widely used applications and protocols[4].

SHA-1 uses hash function where *L* is the number of bits in the message digest. Here L finds a message that is equivalent to a given message digest and it can be done by using Brute-force search in 2L evalutaions. This procedure is called a pre-image attack and for practical applications it depends on *L* and the particular computing environment. There is a second factor where two different messages are found which produces the same message which is known as a *collision.* Hash function strength is compared to a half the message digest length which is symmetric cipher. Thus SHA-1 was originally thought to have 80-bit strength[8].

Structure of algorithm possesses blocks and iterative structure and additional final steps are absent. Partial-message collision attacks takes SHA-1 hash function. These attacks allow an attacker to fake a message, signed only by a keyed hash - SHA (message||key) or SHA (key|| message) - where message is extended and also hash value can be recalculated without knowing the key.

B. Security:

Secrecy of the data is maintained by a encryption technology as data is transferred over a long distance. Overall 80-85% of data security is achieved as data is decoded which involves inverting of the feedback function or generation of binary sequence which is helpful in retrieving the data after some recombination operation.

Data is converted to its ASCII value where one character at a time is converted. Conversion is done by using a 2^8 x 8 priority encoder (1 byte per character). Here 8-bit sequence is stored in a 8-bit right shift register. Then a shift control input is introduced with the clock pulse in which an octal word-time signal is used so that number pulse is equal to the number of bits in the shift register. The shift register has got a 0-bit feedback. When the input bits are shifted towards right, from the leftmost register, the 0-bit enters so that at the end of the 8th clock pulse the content of 8-bit register is refreshed back to 0.

After the first clock pulse, the linear feedback shift register (LFSR) set-up causes the extreme right bit of the register is made to undergo some transformation. A 3-bit register have to use an initial content set to 000.Let the 3-bit register (SERIALLY IN SERIALLY OUT)A, B and C from left to right are used. The 8-bit right shift register and the 3-bit LFSR are working under the same clock pulse or timing sequence. XOR-ed with the first bit shifted out of the 8-bit shift registers is the initial output given by C. The input to A has been supplied by the feedback function which gives f =((AB XNOR C) XOR A).(ABC)'. This is continued for 8-clock pulses where we obtain the output from C as given below:-

C0	C1	C2	C3	C4	C5	C6	C7
0	0	0	1	0	1	1	1

Simultaneously output from the 8-bit shift register is then XOR-ed with the output given by C.

For example, suppose you want to transfer the character ‘b’ having 98 as its ASCII value. When ‘b’ is decoded gives the bit sequence 01100010. Then 01100010 is transferred to the 8-bit right shift register. Then these bits are transferred serially one by one.

After providing the system specific password which sensitive to user PC and user’s device configuration/id, decoding of the shared data is possible. The unique bit pattern from Y0-Y7 is read from ROM area on provided password (password is device sensitive, applicable only for user PC). Later, the shift registers are loaded with these bit patterns (Y0-Y7, different for all the 100 devices) and for decoding of the 8-bit character, the 8 X 256 bit decoder is enabled. After it is XOR-ed with the bit pattern and decoded then the receiver is able to read the original mail.

The data transmission done with the following process does not provide 100% security because of 8-bit data size, but when number of bits being transferred increases to 16, 32 or 64, then it becomes very hefty for data attacker to performing decoding operation with the transmitted data by using the process of deriving the bit sequence, As it is a very tough process to match combination of bits will work out.

To generate plain text from cipher text, even if the bit sequence is intercepted while transferring of data, the correct combinations of 8-bit sequence which is stored in ROM and to be XOR-ed with incoming bit sequence then has to be discovered. It consists of a mixture of various combinational operations instead of a conventional polynomial feedback function.

The following process does not come with 100% secured data transmission, but as number of bits being transferred increases from 8 to 16,32or 64, process of deriving the bit sequence for performing the decoding operation with the transmitted data becomes difficult for data attacker ,as it is a tedious process to match which combination of bits will work out. Even if the bit sequence is intercepted while transferring of data , discovering the correct combinations of 8-bit sequence (stored in ROM and to be XOR-ed with incoming bit sequence) for generating plain text from the cipher text is not at all feasible. Further it does not have a conventional polynomial feedback function but a mixture of various combinational operations.

IV. ARCHITECTURE

A. BASIC ARCHITECTURE:

Basic architecture of the system which is depicted in the fig 2. Here flow of the system is given which comprises basic elements such receiver, supplier, cloud storage. This paper represents exchange of the information between client and supplier through secured communication. Here supplier and receiver are the members of the system so first verification method is performed through registration and login (OTP).

Note that supplier stores his data in encrypted format in the cloud storage using his private key. Now receiver will send request for a particular data to the supplier. System will again check for authentication of the receiver at cloud by identity-based encryption. For authentication purpose it may have to satisfy conditions which are based on identify-based encryption.

Further request is forwarded to the supplier. If supplier is interested, then he sends his private key to the receiver through secured communication channel. Then receiver receives private key from supplier and decrypts required data.

Hence successfully clients can communicate with each other in a secured manner.

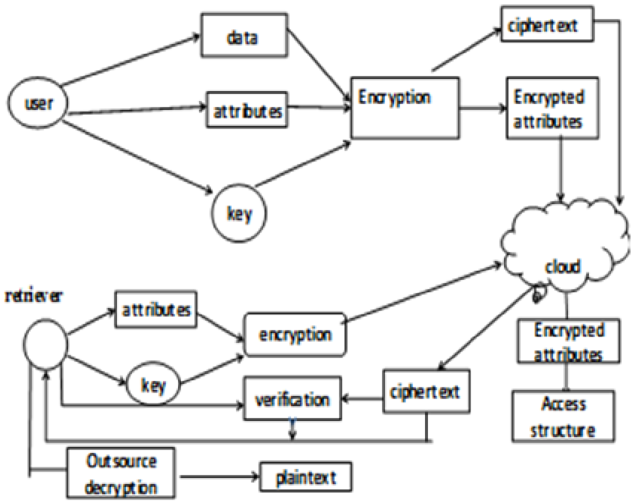

Fig 2.Basic Architecture

V. CONCLUSIONS

This paper concludes that authentication is achieved by applying authentication on every user and it can be done by using SHA-1 algorithm. We propose KAC and support delegation of secret keys for different cipher text classes in cloud storage and provide entire security by LFSR

REFERENCES

[1] Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou and Robert H.Deng, Senior Member, IEEE, IEEE trans. On parallel and distributed system, VOL. 25, NO. 2, FEBRUARY 2014.

[2] https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiwiqj2n6TLAhUQbY4KHTXdC4UQFggcMAA&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FLinear_feedback_shift_register&usg=AFQjCNGDhEDBNoXIvHf4inIbVBYE4HtaA

[3] Development of improved Aggregated Key Cryptosystem for scalable data sharing Rashmi Khawale, Roshani Ade D.Y. Patil School of Engineering and Technology, Lohgaon, SPPU, Pune, India

[4] https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjZpouhoKTLAhUDkI4KHfHSBekQFggcMAA&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FSHA-1&usg=AFQjCNGaCqTalQgajXwOjiJ0_HKdBG-6AQ

[5] Data Authentication and Integrity Verification Techniques for Trusted/Untrusted Cloud Servers, Satheesh K S V A Kavuri, Dr.Gangadhara RaoKancherla, Dr. Basaveswara Rao Bobba. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) IEEE Dec 2014.

[6] Google Trends,Cloudcomputing,http://www.google.com/trends/explore#q=cloud%20computing, 2012.

[7] 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.

[8] Subhra Mazumdar , Tannishtha Som “ Data Encryption with Linear Feedback Shift Register”, International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012.