ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 7 , July 2015

Secure Data Sharing On Cloud Using Key Aggregate Encryption and Intrusion Detection

Garima Kumari , Mr. Sunil Rathod

P.G. Student, Dr. D.Y.Patil School Of Engineering, Pune, Maharashtra, India
Professor, Dr. D.Y.Patil School Of Engineering, Pune, Maharashtra, India

ABSTRACT: Cloud storage is getting very popular these days .The two major facilities that cloud provide are data storage and data sharing. A secure data sharing in cloud is an important issue. This paper comes with an idea of making the data sharing secure and leak resilient. Data is uploaded on cloud in encrypted form. Encryption of data is done using different encryption keys, but there is only one decryption key which is securely delegated by data owner to hosts in communication. This decryption key is aggregate of all the secret keys but it is compact as a single key, which can decrypt multiple cipher text. Before sharing the aggregate key, each host in the communication will monitor the suspicious activities in their sub-network. Suspicious IP addresses are blacklisted and data sharing with blacklisted hosts are rejected. Each host in communication will work as an independent intrusion detection system thereby overcoming the challenges while data sharing.

KEYWORDS*:* cloud storage, data sharing, key aggregate encryption, intrusion detection, leak resilient system

I. INTRODUCTION

Cloud computing is growing as a huge platform for storing, maintaining and sharing data. Demand for data maintenance and storage is increasing in all fields, whether users are from corporate, military, IT organisations etc. Data privacy has become an important concern for cloud users. Users do not trust clouds in terms of confidentiality.
Clouds are intensely used for sharing data. Cloud hosts can share subset of their information with their friends and colleagues.
While sharing data, security is a major concern. Traditionally we believe third party server for providing security. Request is sent to the server for authentication, hosts accessing clouds are forced to trust the third party for their security. But there are chances of cheating, hacking and intrusion attacks [1].
Assume that in a hospital management system doctors and patients are accessing the cloud for sharing information about disease and treatments. Doctor uploads information about his patient on the cloud, but he is not comfortable with the privacy rules of cloud. So, doctor decided to encrypt all his data and then upload files on the cloud. After two days one of the patients requested the information relevant to him. As doctor has already encrypted data, the decryption key will be delegated to the patient. If traditional approach is considered for delegating decryption key, three conditions are arising:

1. All files are encrypted with similar encryption key. Here, Doctor has to send one decryption key which will disclose secrecy of all the data.
2. All files are encrypted with distinct or dissimilar key. In this case distinct decryption keys will be sent, which is practically inefficient, as data owner has to send a no. Of decryption keys.
3. While delegating the secret keys there are chances of intruder's attack. Some third party may try to get important information.

To overcome above hurdles while sharing the data, a solution is proposed in this paper. The proposed solution is to "Encrypt all data with dissimilar encryption key and send only single decryption key. This single decryption key should be able to decrypt multiple cipher text. The promising feature of decryption key is that, it is aggregate of the entire decryption key but it remains compact in size as a single key [1]. The hosts involved in communication should be able to monitor the security breaches, hence an intrusion detection system should be provided".

The decryption key is delegated securely on a secured channel. Small size of decryption key is desired, as we can use it for smart phones, wireless sensors, smart cards etc. This paper finds its application for hospital management, military services etc.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 7 , July 2015

II. PROPOSED WORK

In this paper we propose a technique to make data sharing secure and leak resilient. The purpose of this article is to provide a way for secure data sharing on cloud using key aggregate encryption and Intrusion Detection (KAEID). In KAEID Decryption key is made more and more powerful so that it can decrypt multiple cipher texts. At the same time Intrusion detection system (IDS) monitors data exchange between two hosts and ensures if these are trusted hosts [2]. Specifically, the problem statement is "To generate a constant size aggregate decryption key by data owner which can decrypt multiple cipher text. The decryption key is aggregate key which encompasses the power of all secret keys. This data sharing system also supports intrusion detection to find out the suspicious activities of hosts. If hosts involved in communication are trusted hosts data sharing will take place else rejected."

In KAEID user encrypts message under public key cryptosystem. Messages are encrypted by one who decides public key as well as cipher text category. Cipher text is categorized under different "classes". Plain messages which are subset of cipher text class possess few common features. Here all the hosts set up an account on the cloud server. Hosts can login to the cloud server; they can perform their task and logout of the server. The data owner generates public key/ master key pair. Public key is used for encryption while master key is kept secret. Master key is used for aggregating all the decryption keys. The aggregate key is extracted out of master key and corresponding cipher text class identifier.

This aggregate key is delegated to data recipient. The data recipient compares the set of cipher text classes and decrypts the message. Hence, it also prevents the downloading of unwanted data. Each host in the data sharing system works as IDS. An IDS collects IP address of all hosts in its sub network, and keep eyes on suspicious activities in the network. If any suspicious host is found it is blacklisted. Data sharing with suspicious host is rejected.

As shown in Fig-1. Two hosts data owner and data recipient are accessing the cloud network. Data owner encrypts the data and uploads data on cloud server. Aggregate key is delegated to Data recipient for decryption of requested messages. Hosts involved in communication are also working as IDS. IDS collects and lists IP addresses of corresponding sub network. Monitors the suspicious activities and reject data sharing with the hosts found blacklisted.

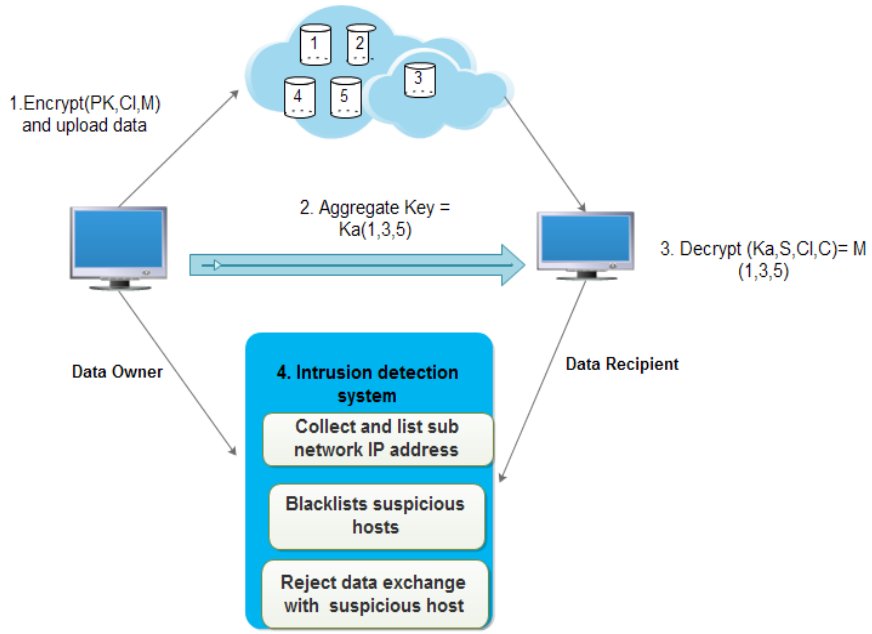

FIG-1: KEY AGGREGATE ENCRYPTION AND INTRUSION DETECTION

III.DESIGN PHASE

In this section of paper construction framework is provided. Three major phase while designing KAEID are:

a) Encryption phase.

b) Aggregate key generation phase.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 7 , July 2015

c) Intrusion Detection system.

a) Encryption phase: This is the first phase. Users open or set up their account on the cloud server. Data owner who needs to upload data will generate public/master key pair. Master key is kept secret and data is encrypted under public key and cipher text identifier. The function ENCRYPT ( ) is used here.
ENCRYPT (PK, CI, M) generates cipher text C. Where PK stands for public key, CI stands for cipher text class identifier and M stands for plane message.
b) Aggregate Key Generation Phase: In this phase aggregate decryption key is constructed. Aggregate key makes use of master key and set of CI. The function used here is AggKey( ).
AggKey(MK, S) generates Ka. Here, on giving input MK master key, and S set of CI we get output as Ka aggregate key.
c) Intrusion Detection System: Each host in communication work as IDS system referred as I. There is a set of IDS that is I={I1,I2.I3...n}. Each I monitors corresponding host in sub network. Distributed hash table scheme is used to collect IP address of neighbour host. Set of IP addresses are shared among hosts in communication network. Each host will publish the list of IP addresses for a time Δt. So if any suspicious IP address comes in picture for a time interval Δt, it can be easily caught. Suspicious host is blacklisted as bi. Data Sharing is rejected with the suspicious host, thereby overcoming the problem of single point failure[2].

1. For time interval Δt
   Collect blacklist bi
2. For each host $h_{ij} \in b_i$ do
   $h'_{ij} \leftarrow f(h_{ij})$
   Subscribe (h' , I_n)
   End for
   End for
3. while message is received
   if message = subscribe(h' , I)
   Then hash[h'] , collects $I_n \leftarrow$ hash[h'] U I_n
4. if |hash[h']| > N then
   for each $h_{ij} \in$ hash[h'] do
5. notify(I_i h', |hash[h']|)
   end for
   end if
6. else if message = = notify(I, h', n) then
   host h is confirmed as suspicious
   end if
   end while

The above three phases of tries to overcome all possible hurdles while sharing data on clouds. We are preventing the misuse of data as well as intruders are detected in effective way.

IV. RELATED WORK

Various researches are done by researchers to make data sharing secured and leak proof. Many modern cryptographic algorithms are designed to deal with the security issues. In this section comparison of proposed solution is done with other security schemes.

A) Secret Keys assignment schemes

There are a no. Of secret keys assignment schemes such as tree based assignment, identity based encryption, attribute based encryption etc. These key assignment schemes define relations among a subset of data which is to be encrypted. It makes it easier to assign secret keys over a set of data.
In tree hierarchy based scheme if a secret key is assigned to parent node, it will be automatically assigned to its child. Tree hierarchy solves the problem if one needs to share all files under a certain node in tree[4]. Another key

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 7 , July 2015

assignment scheme is Identity based scheme (IBE) for encryption. In Identity based scheme there is a third party Private key generator (PKG) which issues secret keys to all users considering their identity, PKG holds the master secret key[5],[6].

Attribute based scheme (ABE) for key assignment has also found many applications. In attribute based scheme each cipher text is associated with some attribute. If associated attribute confirms to the decryption policies, cipher text is decrypted by this key. For example, we have a secret key policy defined as (a-b-c-d), we can decrypt under the class a, b, c or d [7].

Key assignment Scheme	Key size to be delegated for decryption	Encrypted message size	Cryptographic scheme
Key assignment Using tree hierarchy	non-constant	Constant	symmetric or public-key
Identity Based Scheme	Constant	non-constant	Public Key
Attribute-Based Scheme	non-constant	Constant	Public Key
KAEID scheme	Constant	Constant	Public Key

Table- 1: KAE Scheme and other related scheme

B) Intrusion Detection System

Intrusion detection has been an important concern for cloud security. To provide security to data on cloud a number. Of algorithms are designed. In this section we study literature survey for intrusion detection system. Various intrusion detection systems have been proposed, to detect the attacks like man-in-the-middle attack, denial of service attack, traffic analysis etc, single point failure etc. Overcoming such attacks in cloud network is a challenging task. Below are the few works which are done for intrusion detection in distributed networks.

Worminator [9] proposed a peer-to-peer collaborative intrusion detection system, which uses Bloom filters that defend information privacy, and an active overlay network that is used for distributed connection. This work aims on proficient information sharing.

Netbait [10] is a service for worm detection in distributed systems. Hosts present in network parallely work as IDS. Query processing are done parallely in Netbait. Netbait is intended for worm detection, while our approach is also suits for scanning and man-in-the-middle attack. Worm attacks are prevented, suppressed and clearout using Netbait.

objects, connected component labelling is applied to the resultant image.(c) represents text detection by applying second set of criteria which eliminates all the objects whose area is less than 300 and filled area is less than 500.

V, RESULTS AND DISCUSSION

In this experiment it is assumed that we have n number of cipher text classes denoted as CI. S is a set of cipher text class identifier CI, represented as S ={CI| CI=1,2,3...n}. The encryption phase is independent of the account setup. Encryption time does not depends upon the no of message to be encrypted. Encryption is done in constant time. r is the portion of cipher text classes to which data recipient is concern. r represents the ratio of delegated cipher text classes to the total no. Of cipher text classes. Decryption is done in group; decryption key matches keys for cipher text classes, with pairing operations where S is the set of cipher text classes.

Each host in communication collects the IP addresses of neighbours in Δt time interval. IDS blacklist the suspicious IP addresses. Blacklist's size increases for fixed no. peers. As no. of peers increases detection delay increases. Here routing time is not much significant, it is less than the time taken to handle increased load.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 7 , July 2015

VI.CONCLUSION

As we all know data security is a major concern for cloud users. This paper comes with a technique, which helps to achieve a secured and leak proof system. Here modern cryptographic algorithms and intrusion detection algorithms are used in order to achieve a secured way of data sharing. In this system data owner uses distinct encryption keys and encrypts messages before uploading it on cloud and sends a single decryption key to other host. This single decryption key decrypts multiple cipher text at a time thereby saving the time as well as storage space. Unwanted data will not be downloaded at data recipient's side. Intrusion detection systems monitor the security breakdown in the network. Data sharing is stopped if any un-trusted party comes in the network. Obtaining an ideal system without data any leakage is practically is not possible, but this research work helps to solve certain problems very efficiently. It saves the storage space; it also saves time spent in key exchange. Key sizes remains constant and compact.

REFERENCES

[1] "Key-Aggregate Cryptosystem for Scalable Data sharing in Cloud Storage" Cheng-Kang Chu, Sherman S.M Chow, Wen-Guey Tzen, Jianying Zhou, Robert H. Deng IEEE, 2014

[2] "A Peer-to-Peer Collaborative Intrusion Detection System" Chenfeng Vincent Zhou, Shanika Karunasekera and Christopher Leckie National ICT Australia Department of Computer Science and Software Engineering.

[3] University of Melbourne, Australia 2005 [3] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 04). IEEE, 2004, pp. 20672071.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transac ormation and System Security (TISSEC), vol. 12, no. 3, 2009tions on Inf.

[5] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT 05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457473.

[6] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," in ACM Conference on Computer and Communications Security, 2010, pp. 152161.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 06). ACM, 2006, pp. 8998.

[8] "Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121130 [9] CERT Coordination Center, "Module 2 - Internet Security Overview", 2003.

[9] M. E. Locasto, J. J. Parekh, A. D. Keromytis, S. J. Stolfo, "Towards Collaborative Security and P2P Intrusion Detection", 2005 IEEE Workshop on IAS, June 2005.

[10] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph, "Tapestry: An infrastructure for fault-tolerant wide-area location and routing", Technical Report CSD-01-1141, University of California, Berkeley, 2000.

[11] D.Boneh, C.Gentry and B.Waters,"Collusion Resistant Broadcast Encryption with Ciphertexts and Private keys".Springer 2005.