Acrse-Ik- An Attribute Based Confidentialityretainingsearchable Encryption Technique using Interimkeyword for Protected Cloud Storage

Gvicto Sudha George, K.Meenakshi, Almas Begum

Abstract*: Data stored in the cloud server is in the encrypted format because the cloud server cannot be held accountable always. The cloud server makes use of the searchable encryption algorithm to fetch the required data by avoiding the decryption process. The attribute-based keyword search allows the users to access the data that they require from the cloud server any time. This method ensures that the rights of the users who access the server are not disclosed as a public data in the cloud server which is done by generating search key by the user. But still this method poses a threat to the privacy of the information.To overcome this shortfall, this paper proposes a new scheme that utilizes short lived keywords. The proposed method uses search tokens generated in a specific time span to extract ciphertext for the users and also privacy of the generated search tokens are upheld. The proposed method does not suffer from the chosen keyword attack which is verified by the random oracle model. Moreover in the proposed method it can be proved that the two parameter time complexity and the number of attributes are proportional to each other in a linear fashion. Also this scheme is well suited for real word applications.

Index Terms: Cloud Security, Searchable Encryption, Short lived Keyword Search, Secrecy, Access Policy..

I. INTRODUCTION

In recent years cloud computing is considered to be very essential in our day to day life. This is because it offers reliable, scalable and efficient recourses at an affordable price for computationalactivitiesas well as data storage. Hence many organizations are outsourcing data on public cloud. The outsourced data may contain sensitive data like financial record, personal health record. So to safeguard the privacy of the information they are kept in the encrypted format in the cloud server. This solves the security issue but it poses a problem for the data users whereby the process of searching and retrieval of data becomes increasingly difficult. This leads to the recently upcoming research domain termed searchable encryption. Searchable encryption aids the user to securely and selectively retrieve data of his interest and also which he is allowed to access from the cloud storage.The two types of searchable encryptions are symmetric searchable encryption and asymmetric searchable encryption. For searching over the encrypted data a large numbers of techniques are introduced.InSymmetric SearchableEncryption (SSE) data owner encrypt the document with the help of the secret key and shares it with the data user for decryption. Comparing the multi-users and the single user schemes of searchable symmetric encryption, literaturessay that multi-users schemes have outperformed the other[1-3]. But they are not well suited for the scenario where the number of senders and receivers are more than one. Because it will increase the communication overhead.

InAsymmetricSearchable Encryption (ASE) the data owners generate the searchable ciphertextusing data user's public key andmade it available the cloud. Later the data user decrypts the ciphertext by his corresponding private key and forwards the keyword to the cloud. On receiving this cloud server will carry out the search operation in support of the data user and find out the documents with that keyword. This asymmetric searchable encryption was first introduced in [4].Another interesting searchable cryptographic primitive is Attribute Based Encryption (ABE)that ensures secrecy of data alongwith the user specific accesspolicy of data access which is decided by the data owner. In this approach a group of attributes which are decided by the owner of the data are involved in the process of encrypting the data.This ensures that the decryption is possible only for the authorized user who is the sole owner of the attributevalues to carry out decryption. The ABE approach is well suitedfor the scenarios where more numbers of senders and receivers are involved. The searching is carried out by the cloud server for the support of the genuine user without the involvement of the owner in Ohtakeet.Al [5] which is an example for Attribute Based Keyword search. Then to search in the encrypted data using only one keyword, a Cloud computing is generally used to describe data centres available to many users over the internet. Cloud is used for storing and accessing data and programs over the internet instead of your computer's hard drive. Encryption component, that we utilize today so as to secure the information over the cloud are not sufficiently reasonable to stop the unapproved access to certifiable client information.

Therefore, we proposed a framework in which we going to utilize both client conduct profiling and fake innovation.

Revised Manuscript Received on December 22, 2018.

GVictoSudha George, Dept. of CSE,Dr.MGR Educational and Research Institute,
K.Meenakshi, Dept.of CSE, SRM Institute of Science and Technology, km121982@gmail.com
Almas Begum, Dept.of CSE, Vel Tech RangarajanDr.Sagunthala R&D Institute of Science and Technology,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Into this framework at whatever point an interloper attempts to get to the information of the authentic client, it consequently create a bait document with same name and scrambling content record in such a way it looks certifiable as the focused on record and gives the equivalent to the gatecrasher.

Client Profiling method connected to screen ordinary conduct of the client. Portrayed conduct based security generally utilized by cops in misrepresentation recognition. Bait innovation is Serving imitation document to the un-recognized client confound into trusting that they separated genuine data, when they are definitely not. Document Generation is utilized for programmed record age once the conduct of the client is being distinguished as unknown utilizing client conduct profiling innovation. quite number of attribute-based encryption methods are proposed[6-10].

It is noted that in all the above mentioned ABE schemes the access control policy is in the plain form. This may disclose the data users attributes to the adversary. But it is necessary to maintain data confidentiality and also secrecy of data access.Thesolutionis to encrypt the access policy which might ensure the confidentiality of the purpose and the person who uses the encrypted data.In[11,12], the authors have proposed searching schemes where encryptedaccess policy was used .There exist two Attribute bases encryption method. They are Key Policy ABE and Ciphertext Policy ABE. They differ from one another on the basis of what is being associated with the access policy. First one used a secret key while the other used cipher text.

II. RELATED WORK

If we look into the above listed in all schemes on receiving the search token associated with a keyword, the cloud can search for the availability of the keyword in the old and any new cipher text that might be generated later also. This might disclose the information pertaining to the subsequent documents stored in the cloud. Hence it is advisable to limit the validity of the search token for a stipulated time period. Here in this paper we propose An Attribute Based Confidentiality Retaining Searchable Encryption Technique using Interim Keyword(ACRSE-IK).The proposed approach is well suited for multi data owners and usersscenario.

The proposed ACRSE-IKmethod assign a set of attribute values for each data user. The data user intern submits these attribute values to a trusted third party and obtain the search token. One of the salient features of the proposed approach is that on receiving the search token the data user can herself generate the query to the cloud server as a trapdoor to find out the availability of the documents without the intervention of the data user. The significance of the trapdoor is that it never discloses the user's attributes or the search keyword.Additionally the proposed method provides the flexibilityfor the data receivers to decide their intended access policy.

The proposed cryptographic primitive works as follows:

1. The data sender along with a trusted third part first generates the ciphertext of the index. The main secret key appended tothe index by the third party makes the index moresecure.
2. The data owner also generates the time stamp of encryption relevanttoan access control policy wished for.
3. The encrypted document along with the encrypted index and the timeofencryptionis uploaded on the cloud server.
4. Subsequently the legitimate user chooses a random time period and communicatesthe trapdoor. On receiving that checking for the relevant documents will be carried out in the cloud server by using trapdoor and ciphertextof index.
5. Step 4 is repeated unit all documents checked out for the encrypted index
6. The seeking process is successful only when

The data receiver's attributesgo with the policy of access control. The trapdoor time span enclose the time stampof encryption. The keyword available in the trapdoor is available in the index. It is demonstrated that the new method pit forward here is not affected by chosen keyword attack.Also the performance of the proposed work is evaluated in terms of the execution time. A commercial data set[13] is used to validate the proposed scheme.

III. THE ATTRIBUTE BASED CONFIDENTIALITY RETAINING SEARCHABLE ENCRYPTION TECHNIQUE USING INTERIM KEYWORD – ACRSE-IK

The proposed ACRSE-IKallow the data owner to impose the access controls policy which is hidden into the ciphertext. The scheme supports multi-owner and multi-user scenario. The scheme comprises of the below mentioned parties. They are

A. *Data Owner*: Data owner encrypts the document using an access control policy and uploadit on to the cloud server. The three components of the encrypted data are encrypted keyword's index, the time of encryption in producing the ciphertexts and the document in the ciphertext format.

B. *DataUser:*The entity whichinitiatesthe seeking operationto filter out the relevant documents that have an anticipated keyword, and are encrypted in a particular time span. The data user randomly chooses the time interval.

C. *Cloud Service Provider(CSP):*This entity offers the computation and storage services for the data owners and the users. The CSP stores a huge amount of data in the encrypted form. Later on behalf of the data users it searches the encrypted documents for agiven search token.If the corresponding documents are available the CSP send them to the data users.

D. *Trusted Third Party:* The TTP has two components. They are the Attribute Centre (AC) and the Token Generator (TG). The duty of AC is to produce the security keysand to forward them to data

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

users. The TG helps the data owners for producing the encrypted index. The prime role of TG is enclosing the main secret key parameter into the ciphertextpart of the index that is being encrypted. This makes the scheme adaptively secure with respect to chosen-keyword attack.

It is also noted that though the TG isresponsible for producing the hidden form of index,the information available in side it that are related to other parties are is not disclosed to it. This ensures that there is no information leakage.

Here in the proposed ACRSE-IK schemeowner of the dataproduces a ciphertextfor a keyword in accordance with the policy that controls the access right of a user which is searchable along with the time of encrypting. Tolook for a keyword available in a document, the data user produces a token for searchingwhose validity is specific for a time spanandsendsitto the cloud service provider without the intervention of owner of the data. If the encrypted document relevant to the search token is found with the specified time interval and the intended access control policy, it will be send to the data user.

E. ***Access Control Policy:***Thepolicy which controlsthe access rights of a ciphertext is defined as an access structure. It is decided by the data owner. Only when the attributes available in the secret key of the data user matches with the ciphertext'saccess structure, user is allowed to convert theciphertext to plain text.The policy used to construct the structure for accessing is "Single ANDoperation on multi-valued Attributes". It is described as below.

Consider there exist n attributes and are represented as $\{Att_1,Att_2,\ldots,Att_n\}$.Each attribute $Att_i(1 \le i \le n)$can have a set of permissible values. This is represented by $Val_i=\{Val_{i,1}, Val_{i,2}, Val_{i,3}, \ldots..,Val_{i,m}\}$. Herem is the upper limit of Val_i.Thepolicy of the ciphertextP is given as $P=\{P_1, P_{2,}\ldots..P_n\}$.$P_i(P_i \subseteq Val_i)$denotesallof the possible values that an attribute i can havefor decrypting the ciphertext. The attribute value list of each user $VL=[VL_1,VL_{2,}\ldots..,VL_n]$ such that $VL_i(VL_i \in Val_i)$.The access structure P and the attribute list VL matches with one another only if $VL_i \in P_i$forall of the attributes n . HenceB(VL,P) , a function that compares VP and Pand returns 1 if VL and access structure P matches with one another. Otherwise the value will be 0.

IV. FORMAL DEFINITION OF THE PROPOSED ACRSE-IK

The objective of the proposed method is as follows. To perform the privacy preserving search over the encrypted documents available in the cloud server , as a first step an index corresponding to the encrypted keywords which is relevant to each of the documents is generated. Then the search operation is carried out on to the encrypted index itself.Thefive basic operations that are formulated to do the above mentioned task are SETUP,KeyGener,Enc-Index, Trapdoor, FIND.
The functions are explained as follows:

A. Setup(1^{Ω}):The Attribute Center is responsible executing this function. A security parameter **Ω**being the input passed to the function. The outputs are a Master Secret Key M_{sk}, the secret key Ticket GeneratorTG$_{sk}$andP_k which is a public key.

B. ***KeyGener(M_{sk},VL):*** This function is also executed by AC. The secret key $SK_{ur}$for the data user is produced by taking the main secret key M_{sk}andthe attributes VL of the data user.The trapdoor which will perform the search operation on behalf of the user is generated with the help of his private key.

C. ***Enc_Index(P_k ,kw,TG_{sk}, t_i,P):***This function isthe communication among the data ownerand the TG. The inputs used are the keywordsetKW related to a document D, the time instance of encryption, the permitted attribute set by the data owner for each user .Thethe data ownerinitiate the computation of encryptingeach keyword kw available in the keyword set. Using its secret key TG_{sk} ,the TG compute the encrypted token for each keyword and send it to the data owner. Now the data owner outputs the attribute based searchable cipher text for all the keywords $KW_{encrypt}$called the encrypted index of the document and outsource it to the cloud server.

D. ***Trapdoor(P_k,SK_{ur}, kw,[t_s,t_e]):***To look for whether the needed document is available in the CSP trapdoor is used. The computation of the trapdoor is done by the data user using this function. The data user havingrights for accessing and also the secret key SK_{ur}canonlygeneratethe trapdoor $TD_{kw}$for the keyword kw which is encrypted in a particular time interval $T_{encrypt}=[t_s,t_e]$.

E. ***FIND(TD_{kw}, $KW_{encrypt}$):***This function is run by the cloud service provider. The inputs are the Trapdoor for the keyword and the encrypted index of the document $KW_{encrypt}$..

The result will be1 only when all the conditions mentioned below are satisfied.

- B(VL,P) = 1 [ie. attribute list VL match with an access structure P]
- $KW^{*}_{encrypt} \leftarrow$ Enc_Index(P_k , kw,TG_{sk}, t_i,P)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- ← TD_{kw} Trapdoor(P_k,SK_{ur}, kw,[t_s,t_e])
- $t_i \in [t_s,t_e]$else the result will be 0

V. SECURITY ANALYSIS OF ACRSE-IK

The features pertaining to the security of the proposed method are discussed here. It is assumed that the two parties, data owners and the authorized data users are trustable. On the other hand the cloud service provider is considered asanhonest server but some extend curious. This is due to the fact that in spite of honestly executing the protocols and algorithms the CSPattempts to get some fewprivate information.

Generally the objectives of the adversary A are 1:try to get information about the access policy used. 2: try to gather information about the words that are being searched. Hence to insist security against the adversary, the proposed system is designed to satisfy both the below mentioned requirements.

a. **Security against Chosen Keyword Attacks:**Thedemandthissecurity featureisthat for the adversary A in the selective security model, it is impossible to get any informationof the keyword for its corresponding ciphertext unless otherwise any matching search trapdoor is being given.

b. **Secrecy of the Keyword:** This requirement saysthat for the adversary it is impossible to find out the keyword from the ciphertext and the search token apart from making any random keyword guess.

The proposed scheme is highly secure in such a way that by having a look into the trapdoor, it is impossible for the adversary to gain information pertaining to the keyword and the user's access policy which is kept hidden in the trapdoors. And also even if the opponent has access to the trapdoors and the ciphertext of the index, the proposed approach is highly secure for chosen keyword attack. Hence the ability of an opponent in understanding the keyword or the data users attributes from the trapdoor pattern negligible. This infers that apart from the search outcome it is quite impossible for the opponent to understand anything else from the search.

VI. EXPERIMENTAL RESULTS AND PERFORMANCEANALYSIS

The promising aspect about theproposedAPSE-SKSmethod is that after obtaining the private key from the trustable third party, the data user can create the search token on its own without making any communication furthertothe trustable third party. This will drastically reduce the communication overhead.

Table 1 Execution Time of the algorithms used in the proposed ACRSE-IKscheme. The intended Time units is fixed as Ω =12

ame of the	No. of Attribute Values used (n*m)

Algorithms						
		0	0	0	0	0
nc-Index(ms)	.19	.82	.29	.83	.29	.25
rapdoor(ms)	.85	.63	.82	.81	.82	1.83
eyGener(ms)	.24	.43	.03	.12	2.07	5.8
IND(ms)	0	0	0	30	80	30

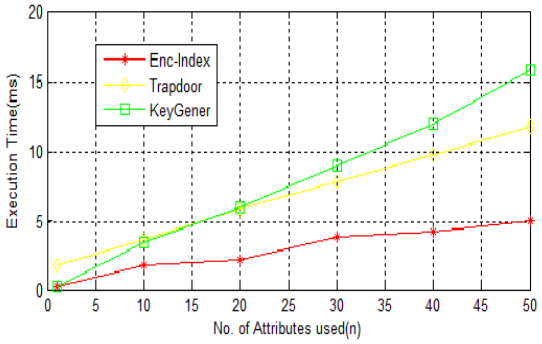

Fig1. The time taken for of the Enc-Index, Trapdoor and Key Generation algorithms

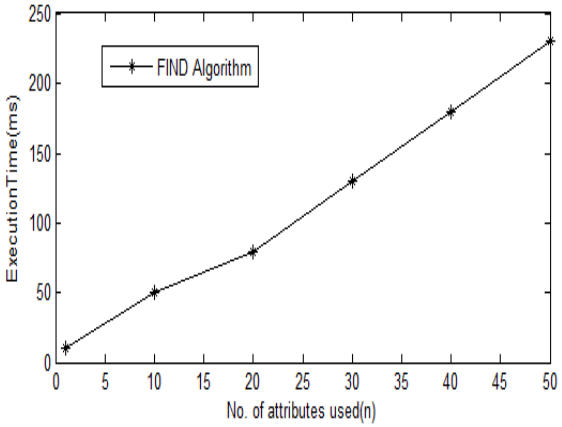

Fig2. The time taken by the FIND algorithm

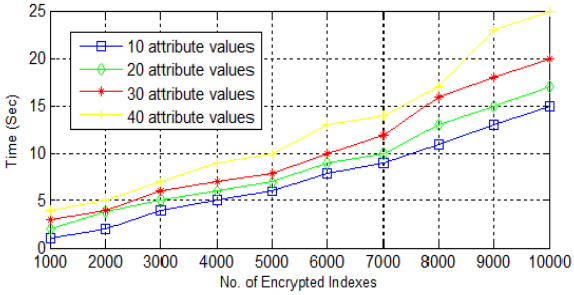

Fig3. FIND algorithm time against varying no. of encrypted index for varying total attribute values(n*m)

To make the simulation resemble the real situation the SETUP, KeyGeneration, EncIndex, Trapdoor protocols are implemented on Intel core-i5 processor with 2.20Ghz and 8 GB RAM. The computational time of the essential operations are calculated with the help of Multiprecision Integer and Rational ArithmeticCryptographricLibrary[14]. The evaluation of the proposed scheme is carried out for variable number of attributes n={1,10,20,30,40,50} and for each value of n a range of m is used. The execution times of the algorithms are given in Table 1 and figure 1 and 2.

The results depicted in the graph are got from the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

experiments for a fixed value for m as 5andΩ=12.The dataset used for conducting the experiment is available at [13] which is a speech data. It is clear from the results depicted in figure (1) and (2),the total number of attribute values and time complexity of the proposed scheme's operations are linearly proportional to one another. The figure (3) illustrates the time taken to look for the required document from 500 to 10000 encrypted indexes that has 5 keywords. The timetaken to perform the search taskisO(n* m) where n*m is the total number of attribute values in the system. That is the reason the results are shown for different values of n*m.

VII. CONCLUSION

In cloud computing provision of security to the stored documents in the cloud server is an important issue. In this paper an Attribute Based Privacy Preserving Searchable Encryption using short lived Keywordis proposed. Thescheme permit the legitimate data users to access the encrypted documents stored in the cloud server based on the keyword chosen, rights of the user for accessing the documents and also the time validity of the generated trapdoor. It is noticed that the privacy of access rights and also the confidentiality of the data are preserved by the propose scheme. It is shown that the proposed scheme is provably secure in random oracle model.

REFERENCES

1. Kaoru Kurosawa ,Yasuhiro Ohtaki, UC-Secure Searchable SymmetricEncryption,In Proceedings of SpringerInternational Conference on Financial Cryptography and Data Security,pp 285-298, 2012 .
2. Ji-Jian Chin , Wei-ChuenYau , Kim-Kwang Raymond Choo , MoesfaSoeheilaMohamadGeongSenPohSearchable Symmetric Encryption: Designs and Challenges, ACM Computing Surveys (CSUR), Volume 50 Issue 3, October 2017
3. H. Sun and S. A. Jafar, The Capacity of Private Information Retrieval, arXivpreprint arXiv:1602.09134, 2016
4. D. Boneh, G. D. Crescenzo, and R. O. et al., "Public key encyrption with keyword search," in Advances in Cryptology-EUROCRYPT 2004, ser. 12 LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer-Verlag, 2004, pp. 506–522
5. Go Ohtake ,ReihanehSafavi-Naini, and Liang Feng Zhang, Outsourcing of Verifiable Attribute-Based Keyword Search , Nordic Conference on Secure IT SystemsNordSec 2017 Springer International Publishing , pp 18-35
6. Wang S, Yao L, Zhang Y ,Attribute-based encryption scheme with multi-keyword search and supporting attribute revocation in cloud storage, PLoS ONE, 2018,Vol. 13,No.10
7. Feng Tao ,YinXiaoyu , Liu Chunyan An Efficient and Anonymous KP-ABE Scheme with Keyword ,Search Information Science and Applications 2018, pp.251-258
8. K. Liang and W. Susilo. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. In IEEE Transactions on Information Forensics and Security 10(9):1981–1992,2015
9. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B., Attribute-based encryption for fine-grained access control of encryption data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98
10. Hui Yin, Jixin Zhang, Lu Ou, Shaolin Liao, Zheng Qin, A Key-Policy Searchable Attribute-Based Encryption Scheme for Efficient Keyword Search and Fine-Grained Access Control over Encrypted Data, Electronics 2019, Vol.8, No. 3
11. Hui Cui ,Zhiguo Wan ,Robert H. Deng ; Guilin Wang ; Yingjiu L, Efficient and Expressive Keyword Search Over Encrypted Data in Cloud, IEEE Transactions on Dependable and Secure Computing ,2018,Vol.15,Issue.3,pp.409-422
12. H. Wang, X. Dong, and Z. Cao. Multi-value-Independent Ciphertext-Policy Attribute Based Encryption with http://www.fon.hum.uva.nl/david/massp/2007/timit/train/dr5/fsdc0/.
13. http://www.fon.hum.uva.nl/david/massp/2007/timit/train/dr5/fsdc0/.
14. Shamus,"Multiprecision integer and rational arithmeticLibrary(Miracle)
15. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
16. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
17. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
18. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.
19. Rajesh, M. "A signature based information security system for vitality proficient information accumulation in wireless sensor systems." International Journal of Pure and Applied Mathematics 118.9 (2018): 367-387.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication