International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

An Approach: Keyword Search Method for the prevention of Keyword Guessing Attack

Shubhangini Bhorde[1], Prof.Kailash Tambe[2]
M.E(CSE) Student, Department of Computer Engineering
Zeal College of Engineering and Research, Pune
deokarshubhangi@gmail.com
kailash.tambe@zealeducation.com

May 29, 2018

Abstract

By utilizing the doorway administration approach, Data owners validate data users for the detection capacities over the outsourced encrypted data. Leaking of access structure by the various attacks fails to prevent the sensitive data from off -line keyword guessing attack and low entropy. To cope with this issue, we are proposing a special crude named ' Keyword Search Policy with Attribute- Based Ciphertext (KSABC). With this arrangement, user cannot search over encrypted data and secure any info with regard to attribute policy. Hence proposing an excellent safety analysis of the KSABC scheme which promotes a trapdoor generation for that keyword and initiates downloading of documents by the provider .Finally, the performance exploration proves that our planned theme is more efficient.

***Key Words*:** Attribute-based encryption, Cloud data, Ciphertext, Data retrieval, Keyword search, Keyword predicting attack, Search Policy.

1 INTRODUCTION

Cloud computing becoming a rising conception due to its on- demand services and access for the configurable resource pool as well as due to sensitive data outsourcing capability. As the service provider has to pay attention not only on n significant access control for gaining the privacy of data corresponding to data user, but also on data encryption expenses. As outsourcing of sensitive info to cloud increase day by day , the cloud computing attacks also there for the data theft as well as data corruption. The main attacks on cloud are

• **Denial of Service (DoS) Attacks:-**By creating resource services unapproachable to its authorized users for indefinite period, a malefactor overload the systems and bypass the authentic requests from the users.

• **Side Channel Attacks:-**An attack depend on info obtained from the computer system.

• **Authentication Attacks: -**This type of attack try to exploit the authentication process.

• **Man-in-Middle Cryptographic Attacks:-**It is an attack where attacker secretly depends and changes the communication between sender and receiver.

• **Inside-Job Attacks:-**This type of attack is due to insider intruders of the system.

2 RELATED WORK

As the data owners and cloud service provider [1] in the similar distrust sphere, user-outsourced unencrypted data may be at danger due to data leaking by unauthorized hackers. For the security of data privacy and to prevent unauthorized user access, encryption of sensitive data prior to outsourcing should be done. When Data owners requested by the data user for their outsourced data, the

most popular method is Keyword Search. To retrieve the required files by the queried user, this technique helps users specifically in terms of data integrity and data authenticity.Related work on previous papers in following fields as:

• **Attribute-Based Encryption**-Sahai was the first to propose ABE [2], for the accessible ne-grained access control systems. He emphasized on CP-ABE (Ciphertext Attribute Based Policy) as users private key attached by the access structure and ciphertext related to attribute policy of user.

• **Attribute-Based Encryption with Keyword Search (ABKS)** -As the projected by Sun [8], in order to authorization along with ne-grained with keyword search, it associates multiple data owners and data users. In this entire search process not only veriable but also data user ensured with the e returned documents authenticity. Zheng et al. [7] focused on multiple data owner with attribute based scalable data access control which moderates the key management intricacy for owners and users.

• **Verifiable Keyword Search**-In the VKS policy [3], by Zheng data owner done secure indexing with attribute- based access policies before outsourcing them cloud. The data owner (DO) denes the associate access policy for every uploaded le. If the attributes of the user on the trapdoor satisfy the access policies of the secure indexes of the uploaded files, then solely the valid search returned by the provider.

• **Keyword Guessing Attack (KGA)**-Proposed by Byun et al. [5], in the process of keyword search, the attacker challenges to keyword guessing attack due to small space chosen for keyword. Xu et al. [6] overcome this drawback as a public-key encryption with fuzzy keyword search (PEFKS) against this attack for the keyword space. Besides this possibility, by Zheng [7] and Sun [8] raised other possibility of getting the access structure by the attacker in order to get the ciphertext.

• .**Attribute-based Encryption with Hidden Policy**-Nishide et al. [9] presented dual patterns to cover the policy of CP-ABE

with partly hidden policy. In this, access structure are not approachable as the attribute credentials not matching the access structure.

2.1 PROBLEM STATEMENT-

The problem of keyword searching is finding occurrence of a sequence of contiguous characters of length l in a text of n characters. Keyword searching elaborated as: Searching presence of a keyword $K\epsilon[]linatextTx\epsilon[\sum]n, where \sum$ is the set of all characters. In the relation with proposed system, Let the documents as (Dc1,Dc2...) and keywords (w1,w2..) as follows

Dc = Dc1, Dc2,...,DcM and keywords, Ki(W) = w1,w2,...,wn.

Let I =Index Table on the on the documents for keywords and. For search process, an user with access policy request an encrypted trapdoor using the keyword query Q and submits it to the cloud server. After processing trapdoor on the index I, server returns found documents Dc from the set of keywords. Considering the two conditions in this as:

(1) The index I should not leak any information about the keywords, such as size, number, content, etc. and

(2) The keyword query retrieving efficiently handled for the larger sets of keywords.

2.2 OUR CONTRIBUTION-

In this paper, proposing an innovative cryptanalytic primitive known as 'Keyword Search Policy with Attribute-Based Ciphertext (KSABC) '.In which users will search the data whose attribute policy equalizes the ciphertext in order to authentic access for that user. The key points as follows:

•The cloud server gets valid search token for searching by the approved users, thereby reducing the process from user side. Secured a gain that, data secured from the cloud server without knowing any information about the data.

•Our theme with the access management policy, assures the security of the encrypted info through ciphertexts. Thereby creating policy which would be beneficial against keyword guessing attack.

3 PROPSED MODEL /ARCHITECTURE

3.1 ACCESS STRUCTURE-

Monotonic Access Structure: if A is a set of attributes satisfying an access structure T, then any A' such that $A \subset A'$ also satisfies T. For example, consider $T = A \cap B$, then both A=$\{A, B\}$ and $A' = \{A, B, C\}$ satisfy T.

Denition 1. Let all N attributes [4,7] be indexed as U = {attribute 1, attribute2,...,attribute N}. For each attribute ϵU, Si = {vi,1,vi,2,...,vi,ni} is a set of possible values, where ni is the number of possible values for attribute . Then let AL = {AL1,AL2,...,ALn} be an attribute list of a user, where $ALi \epsilon Si$, and P = P1,P2,...,Pn be an access structure where Pi Si. Note that, we dene $AL \mid = P$ if the attribute list AL satises the access structure P, namely, ALiϵPi for $\forall i, 1 \leq i \leq n$.

3.2 PROPSED MODEL-

The construction for modules in the proposed system as shown in figure1

• **TPA (Third Party Auditor):** is a trustful auditor that validates user attributes and create private keys andattribute keys (Public, Private, Master) for them.

• **DATAOWNER:** When a data user generates search tokens according to some keywords, and the cloud, who receives search tokens from the user, conducts the search operations over outsourced encrypted keywords.
Data Owner uploads the keywords along with the index table to the provider. He is the encrypting party who uploads file along with

his encrypted data to the cloud, generates public and master key.

•**DATA USER:** A data user sends query to the data owner for the search operations over outsourced encrypted keywords.

• **CLOUD SERVER:** One who provides storage and outsourced computation services for the clients on payper service base.

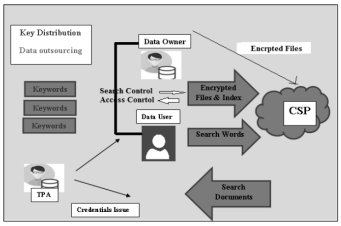

Fig.1. Proposed Architecture

3.3 ALGORITHMS INVOLVED INVARIOUS PHASES:

Input: Security Parameter( );
Output: Message
Step 1: Encrypting party who uploads file and get encrypted data to the cloud and generates Public and Master Key.
Step 2: Authority Attribute key generator (i.e. Public, Private, Master)
Setup ( ): The input value of this algorithm mainly a security parameter. It returns the output value as a public parameter PK and a master key MK.
GroupSetup((PK)GMK , GPK , Dic)) : This polynomial algorithm is performed by Group Manager by Inputting public parameter PK , returns the group master key GMK (0)- , the group public key GPK (0) and Dic (0) where (0) directs initial edition. At the time of user leaving the group, the group key as well as the dictionary will be incremented .Here the current version is ver.

Step 3: Encrypt (PK, M, A) : In this step, it captures the PK , a message M and an access policy A in the attribute space. it gives out a ciphertext CT which are constrained to attribute set

confined to access policy only.
Step 4:Keyword Search Function (KSFOABE) : Data user scans the whole document to build the index table on local storage which is used in searching query along with the document Id.
KeyGen (MK, S) : This process receives the master key MK and an attribute set S. It sends a private key SK to the respective user with respect to the attribute set S.
Step 5: Decrypt(PK, CT, SK) : This is the reverse process of encryption .By using PK , CT and a private key SK ,it decodes the message M.

4 PERFORMANCE EVALUATION

For the efficient working of proposed system, we evaluated its performance by conducing the experiments using JAVA by running a server with Windows 10 as OS, 3.2 GHz, Intel Core CPU -i5, and 8 GB RAM. In this operation, by using different attributes in the access structure. Each reading is repeated more times in order to gain the accuracy .The experimental analysis is shown in figure 2.

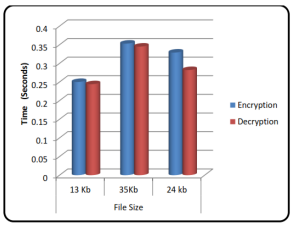

Fig.2. Encryption & Decryption Process with File Size

We practiced on the database of IEEE Digital Library consisting of 2020 unique keywords extracted from 500 documents as used like [3] to validate performance our scheme .As analyzing the existing system comprising of CP-ABE with our proposed system, experimental results shows proposed system is more efficient and reliable in terms of confirmable fine-grained access control.

5 CONCLUSION

To oppose collusion attack, making difference in search scheme, our scheme proves to be more reliable in authorized keyword search. The proposed scheme is more useful for the betterment of the service provided and relishes efficient file download with authenticated access policy bind by user attribute, on such documents for searching keyword by keeping index for the same file .Future scope of this research not only on the indicating policies but also authenticity controlled user attributes of CP-ABE .

ACKNOWLEDGMENT

I would like to thank my guide, Prof.Kailash Tambe Sir for his guidance and support. I will forever remain grateful for the constant support and guidance extended by my guide.

References

[1] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han, Member, IEEE KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage , IEEE Transactions On Services Computing, VOL. 10, NO. 5, 2017

[2] A. Sahai and B. Lewko A, Okamoto T, Sahai, Fuzzy identity-based encryption, in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techni., 2005, pp. 457473.

[3] Q. J. Zheng, S. H. Xu, and G. Ateniese, VABKS: Verifiable attribute-based keyword search over outsourced encrypted data, in Proc. IEEE INFOCOM, 2014, pp. 522530, doi: 10.1109/INFOCOM. 2014.6847976.

[4] J. Z. Lai, R. H. Deng, and C. Guan, Attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 13431354, Aug. 2013, doi: 10.1109/ TIFS.2013.2271848.

[5] Byun J W, Rhee H S, Park H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted

data. In: Proceedings of the 3rd VLDB International Conference on Secure Data Management. Berlin: Springer, 2006. 7583

[6] P. Xu, H. Jin, Q. H. Wu, and W. Wang, Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack, IEEE Trans. Comput., vol. 62, no. 11, pp. 22662277, Nov. 2013.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131143, Jan. 2012, doi: 10.1109/TPDS.2012.97. [8]Sun W, Yu S, Lou W, et al. Protecting your right: attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In: Proceedings of IEEE Conference on Computer Communications, INFOCOM, Toronto, 2014. 226234

[8] F. Zhao, T. Nishide, and K. Sakurai, Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems, in Proc. 7th Int. Conf. Inform. Security Practice Experience, 2011, pp. 8397.