International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Encrypted Mobile Cloud Data Implement Using Multi-Keyword Ranked Search

G.Revathi
MCA Sri Padmavathi College of Computer Sciences And Technology Tiruchanoor, Tirupati, Andhra Pradesh, India

ABSTRACT

In mobile cloud computing, a basic application is to source the mobile information to external cloud servers for scalable information storage. In existing, It adopts CP-ABE, an access control technology utilized in traditional cloud atmosphere, however changes the structure of access control tree to create it appropriate for mobile cloud environments. LDSS moves an outsized portion of the process intensive access management tree transformation in CP-ABE from mobile devices to external proxy servers. moreover, to reduce the user revocation price, it introduces attribute description fields to implement lazy-revocation, that could be a thorny issue in program based mostly CP-ABE systems.during this paper, we develop the searchable encryption for multi-keyword ranked search over the storage information. Specifically, by considering the large range of outsourced documents (data) within the cloud, we utilize the connectedness score associate degreed k-nearest neighbor techniques to develop an efficient multi-keyword search theme which will come the ranked search results supported the accuracy. at intervals this framework, we leverage an economical index to additional improve the search potency, and adopt the blind storage system to hide access pattern of the search user. Security analysis demonstrates that our theme can do confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user.

Keywords: Mobile Cloud Computing, Encryption, K-Nearest Neighbor Techniques

I. INTRODUCTION

Mobile cloud computing gets obviate the hardware limitation of mobile devices by exploring the ascendable and virtualized cloud storage and computing resources, and consequently is ready to supply far more powerful and ascendable mobile services to users. In mobile cloud computing, mobile users usually source their information to external cloud servers, e.g., iCloud, to fancy a stable, low-priced and ascendable approach for information storage and access. However, as outsourced information usually contain sensitive privacy data, like personal photos, emails, etc., which might cause severe confidentiality and privacy violations, if while not economical protections. it's thus necessary to cipher the sensitive information before outsourcing them to the cloud. the information coding, however, would lead to salient difficulties once different users have to be compelled to access interested information with search, because of the difficulties of search over encrypted information. This elementary issue in mobile cloud computing consequently motivates an intensive body of analysis within the recent years on the investigation of searchable encryption technique to realize economical looking over outsourced encrypted information. a group of analysis works have recently been developed on the subject of multi-keyword search over encrypted information. Cash et al. propose a cruciate searchable

coding theme that achieves high potency for giant Mobile cloud computing gets obviate the hardware limitation of mobile devices by exploring the ascendable and virtualized cloud storage and computing resources, and consequently is ready to supply far more powerful and ascendable mobile services to users. In mobile cloud computing, mobile users usually source their information to external cloud servers, e.g., iCloud, to fancy a stable, low-priced and ascendable approach for information storage and access. However, as outsourced information usually contain sensitive privacy data, like personal photos, emails, etc., which might cause severe confidentiality and privacy violations, if while not economical protections. it's thus necessary to cipher the sensitive information before outsourcing them to the cloud. the information coding, however, would lead to salient difficulties once different users have to be compelled to access interested information with search, because of the difficulties of search over encrypted information. This elementary issue in mobile cloud computing consequently motivates an intensive body of analysis within the recent years on the investigation of searchable coding technique to realize economical looking over outsourced encrypted information. a group of analysis works have recently been developed on the subject of multi-keyword search over encrypted information. Cash et al. propose a cruciate searchable coding theme that achieves high potency for giant.

In distinction to the theoretical edges, most of the prevailing proposals, however, fail to supply ample insights towards the development of full functioned searchable coding as represented higher than. As a shot towards the problem, during this paper, we propose AN economical multi-keyword ranked search (EMRS) theme over encrypted mobile cloud knowledge through blind storage. Our main contributions will be summarized as follows:

We introduce a connection score in searchable coding to realize multi-keyword hierarchic search over the encrypted mobile cloud knowledge. additionally to it, we construct an economical index to boost the search potency. By modifying the blind storage system within the EMRS, we have a tendency to solve the trapdoor unlinkabilitydownside and conceal access pattern of the search user from the cloud server. we provide thorough security analysis to demonstrate that the EMRS will reach a high security level together with confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user. Moreover, we implement in depth experiments, that show that the EMRS can do increased potency within the terms of practicality and search potency compared with existing proposals.

II. ALGORITHM

ENCRYPTED DATABASE SETUP

The data owner builds the encrypted database as follows:

Step 1: The data owner computes the d-dimension relevance vector p = (p1, p2, · · · pd) for each document using the TF-IDF weighting technique, where pj for j ∈ (1, 2 · · · d) represents the weighting of keyword ωj in document di . Then, the data owner extends the p to a (d+2)-dimension vector p ∗ . The (d+1)-th entry of p ∗ is set to a random number ε and the (d+2)-th entry is set to 1. We would let ε follow a normal distribution N(μ, σ2).For each document di , to compute the encrypted relevance vector, the data owner encrypts the associated extended relevance vector p ∗ using the secret key M1, M2 and S. First, the data owner chooses a random number r and splits the extended relevance vector p ∗ into two (d+2)-dimension vectors p 0 and p 00 using the vector S. For the j-th item in p ∗ , set

$$\begin{cases} p'_j = p''_j = p^*_j, & \text{if } S_j = 1 \\ p'_j = \frac{1}{2}p^*_j + r, & p''_j = \frac{1}{2}p^*_j - r, \end{cases}$$

whereSj represents the j-th item of S. Then compute the P = {MT 1 · p 0 , MT 2 · p 00} as the encrypted relevance vector.

Step 2: For each document di in D, set the document into blocks of mb bits each. For each block, there is a

header H(idi) indicating that this block belongs to document di . And the sizei of the document is contained in the header of the first block of di . Then, for each document di , the data owner chooses a 192-bit key Ki for the algorithm Enc(). More precisely, for each block B[j] of the document di , where j represents the index number of this block, compute the Ki ⊕ 8(j) as the key for the encryption of this block. Since each block has a unique index number, the blocks of the same document are encrypted with different keys. The document di contains sizei encrypted blocks and the first block of the document di with index number j is as

$$Enc_{(K_i \oplus \Phi(j))}(H(id_i)||size_i||data)$$

And the rest of the blocks of di is as

$$Enc_{(Ki \oplus 8(j))}(H(idi)||data)$$

Finally, the data owner encrypts all the documents and writes them to the blind storage system using the B.Build function.

Step 3: To enable efficient search over the encrypted documents, the data owner builds the index z. First, the data owner defines the access policy υi for each document di . We denote the result of attribute-based encryption using access policy υi as ABEυi (). The data owner initializes z to an empty array indexed by all keywords. Then, the index z can be constructed as shown in Algorithm 1.

Algorithm 1 Initialize F

1: **for** each keyword $\omega \in W$ **do**
2: Set t an empty list
3: **for** each document d_i containing the keyword ω **do**
4: Get the associated vector P of d_i
5: Choose a random number x
6: $Dsc \leftarrow ABE_{\upsilon_i}(id_i||K_i||x)$
7: Append the tuple (Dsc, P) to t
8: **end for**
9: $F[\omega] = t$
10: **end for**
11: **return** F

As we can see, the index z maps the keyword to the encrypted relevance vectors (P) and the descriptors (Dsc) of the documents that contain the keyword. And each list z[ω] can be transformed to be stored in the blind storage system with ω as the document id. Specifically, for each z[ω], the data owner computes σω = 9K9 (ω) as the seed for the function 0 to generate the set Sf . Here, for each block of z[ω] indexed by the integer j, the data owner adds an encrypted header as Enc(KT ⊕8(j))(H(ω)||sizeω), where sizeω represents the number of blocks that belong to z[ω]. Finally, the data owner writes the index z to the blind storage system using the Build function, it is crucial to determine the way we compute the seed for generating the set Sf . We use the document id idi to compute the seed for the documents stored in the blind storage system, and the keyword ω to compute the seed for each z[ω]. Moreover, each header of the blocks of the documents contains the encrypted H(idi) and the first block indicates the sizei . And the blocks of index z are different from those of the documents. Each header of the blocks of index z is denoted as Enc(KT ⊕8(j))(H(ω)||sizeω). This little change is for the security concerns and does not affect the implementation of the blind storage. In addition, since each block is encrypted using the key generated by the index number, the headers would be different even if the two blocks belong to the same document or the same list z[ω].

III. CONCLUSION

In this paper, we've got proposed a multi-keyword rankedsearch theme to modify correct, economical and secure searchover encrypted mobile cloud data. Security analysis havedemonstrated that proposed theme will effectively reachconfidentiality of documents and index, trapdoor privacy,trapdoor unlinkability, and concealing access pattern ofthe search user. intensive performance evaluations haveshown that the proposed theme are able to do

higher efficiency in terms of the functionality and computation overheadcompared with existing ones.

IV. REFERENCES

[1]. H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An SMDP-based service model for interdomain resource allocation in mobile cloud networks," IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2222-2232, Jun. 2012.

[2]. M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

[3]. Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, "Exploiting geodistributed clouds for a e-health monitoring system with minimum service delay and privacy preservation," IEEE J. Biomed. Health Inform., vol. 18, no. 2, pp. 430-439, Mar. 2014.

[4]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587-1611, Dec. 2013.

[5]. H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in Cloud Computing. Berlin, Germany: Springer-Verlag, 2009, pp. 157-166.

[6]. W. Sun, et al., "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur., 2013, pp. 71-82.

[7]. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2112-2120.

[8]. E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic searchable encryption with small leakage," in Proc. NDSS, Feb. 2014.

[9]. Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proc. GLOBECOM, Anaheim, CA, USA, 2014.

[10]. D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean queries," in Proc. CRYPTO, 2013, pp. 353-373.

[11]. Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12]. Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13]. Stehle D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14]. Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15]. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute- based encryption. in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc.

EUROCRYPT. Berlin, Germany: Springer-Verlag, 2011, pp. 568-588.

[17]. NSF Research Awards Abstracts 1990-2003. Online]. Available: http://kdd.ics.uci.edu/databases/nsfabs/nsfawards.html, accessed 2004.

[18]. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, 2004, pp. 506-522.

[19]. D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. TCC, 2007, pp. 535-554.

[20]. B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 262-267, Jan. 2011.

Author's Profile:

Ms. Gadduru Revathi has received her graduation degree in BSc. Bachelor of Science from Sri Gnanambica Degree College, Madanapalli, Chittoor Affiliated to SV University in the year of 2012-2015 . At Present She is Pursuing Post graduate degree MCA, Master of Computer Applications from Sri Padmavathi College of Computer Sciences and Technology Affiliated to Sri Venkateswara University , Tirupati, AP, India.