ISSN 2349-0292
Impact Factor 2.675

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

A PROPOSED APPROACH ON PRIVACY CONTINGENCY HIERARCHY MULTI-KEYWORD SEARCH IN CLOUD COMPUTING

Vedavyas J*
[*] Asst. HOD. Department of MCA, BITM, Ballari, VTU

ABSTRACT

The cloud computing is the most awaited technology for the data owners so that they can securely outsource their data on the cloud. This allows them to retrieve the information from any part of the globe.

Today's cloud support multi owners to share their data among users securely. In our paper we have proposed a protocol called Privacy Contingency Hierarchy Multi-keyword Search (PCHMS) which is used in multi-owner cloud model. Dynamic key generation prevents the attackers from hacking the secret key.

KEYWORDS: Cloud Server, Protocol, Dynamic Key Generation, Multi-owners.

INTRODUCTION

"The practice of using a network of remote servers hosted on the Internet is to store, manage, and process data, rather than a local server or a personal computer" is known as Cloud Computing.

Cloud computing provides the rich benefits like easy access, reduced costs, fast distribution and flexible resource management etc.

Enterprise of all sizes can act effectively on the cloud to increase conception and collaboration. Regardless of voluminous benefit of cloud computing all types of enterprises disinclined to outsource the sensible data such as e-mails, personal records and confidential files to the cloud. As soon as the sensible data in contract to work out on the remote cloud, the owners loose the direct control of data.

Virtualization and firewalls are the mechanisms used to provide security provided by the cloud service providers. The data is not hidden from the service providers, because they have full control on the infrastructure of the owner data, hardware and software.

The key problem is the searching of plain text keywords, as it relies on the traditional encryption techniques. A protocol called *"Privacy Contingency Hierarchy Multi-keyword Search"* (PCHMS) is used in multi-owner cloud model. Normally, for the secure search both keywords and trapdoors are used systematically as a novel secure protocol with different encrypted files and keywords. To prevent the owner data from hackers we are using Dynamic Privacy Key Generation Protocol.

PROBLEM STATEMENT

In this paper, we describe the conventional problem, and the threat model. Here we predefine the system model with respect to threat model. Then goals of our design will make clear about the problem.

System Model

The four entities of the multi-user and multi-owner of the cloud computing model are:

1. Data Owners
2. Cloud Server
3. Administration Server
4. Data Users

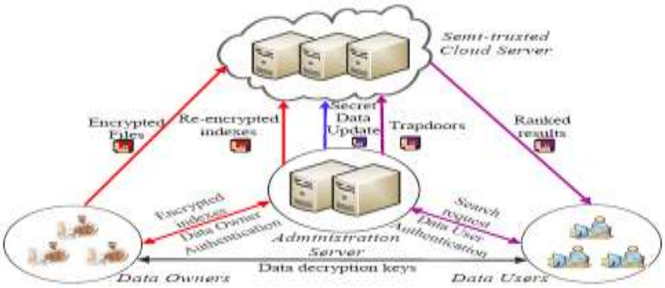

Fig. 1: Architecture of Privacy Contingency Hierarchy Multi-keyword Search in Cloud Computing

Let F be the group of files.
I- searching Index.
W- Keyword..
C - Encrypted files.
K –Parameter to be passed to the server.

By sending the parameter K and top-k relevant files from the cloud server by decrypting we can improve the file access and reduce the communication cost.

Threat Model
Here cloud server is not trusted, Administration Server is trusted. Once the data owners and users pass the authentication from the Administrative server, it can be treated as trusted. Here the efficiency of the server is not concentrated, the contents of files, keywords are to be considered.

DATA AUTHENTICATION

In traditional authentication method, the process of authentication is shown in three steps:

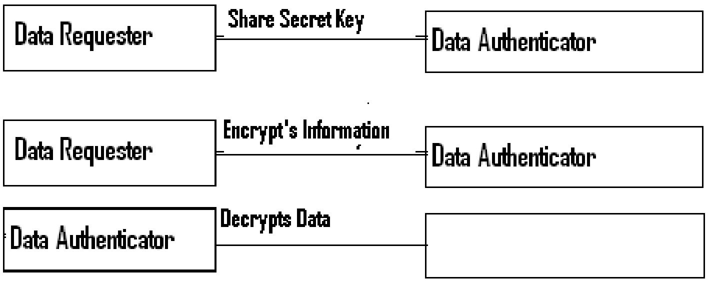

Fig 2: Traditional Method for generating Secret Key.

The major setback for the above method is that the secret key is unchanged which is shared between Requester and Authenticator. The identification of the legal requester is difficult when the hackers hack the secret key.

Solution to the above said problem is by introducing the Dynamic Key Generation and Authentication Protocol. To understand this approach let us consider the above scenario with an example.

Ram wants to be authenticated by Administration Server, the server authenticates Ram by giving the initial key as in traditional approach. In our proposed approach, Ram has to provide the historical data of their conversations, based on the historic data of Ram, the protocol goes on updating the secret key contents which attacker cannot start a legal conversation with administration Server.

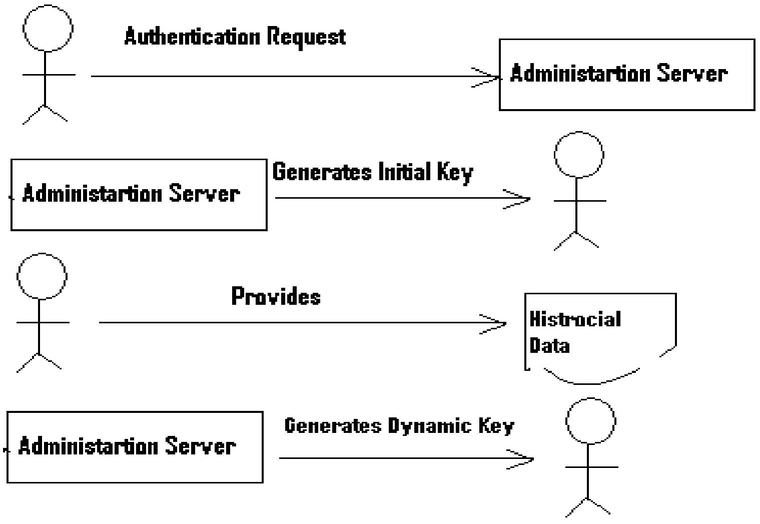

Fig. 3. Dynamic Key Generation

User Authentication

Counter	Last Access	Historical Data	Random Number	CRC

Fig.4: Format of Authentication Data

The counter fields keep tracks of number of users submitted the request. The last Access filed holds the last accessed time to the network by the user. Personnel data of the user is stored in the Historical Data filed. Random Number and the CRC is used to check any tamper had been attempted by the attackers.

FUTURE WORK

Encryption technique is used to prevent the cloud server from knowing exact search words from the data file. In our research we are going to propose Complementally Order and Privacy Uphold Functions (COPUF) protocol which we are implementing on commercial clouds. The data owners can easily choose any family members of COPUF for their encryption.

CONCLUSION

To authenticate data users and to find attackers from stealing the secret key, a new kind of Dynamic Secret Key generation Protocol for the authentication purpose has been proposed in this paper. The search is based on Hierarchy of search results to preserve the scores and the keywords of the files.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] C.Wang,S.S. Chow,Q.Wang,K. Ren, andW. Lou, “Privacypreserving public auditing for secure cloud storage,” *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, “Practical techniques for searches on encrypted data,” in *Proc. IEEE International Symposium on Security and Privacy (S&P’00)*, Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003) secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in *Proc. ACM CCS’06*, VA, USA, Oct. 2006, pp. 79–88.

[6] D. B. et al., “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

[7] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” in *Proc. Applied Cryptography and Network Security (ACNS’04)*,Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8] L. Ballard, S. Kamara, and F. Monrose, “Achieving efficient conjunctive keyword searches over encrypted data,” in *Proc. Information and Communications Security (ICICS’05)*, Beijing, China, Dec. 2005, pp. 414–426.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in *Proc. IEEE Distributed Computing Systems (ICDCS’10)*, Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacypreserving multi-keywordranked search over encrypted cloud data,” in *Proc. IEEE INFOCOM’11*, Shanghai, China, Apr. 2011, pp. 829–837.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacypreserving multi-keywordranked search over encrypted cloud data,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 222–233, 2014.

[12] W. Sun, B.Wang, N. Cao, M. Li,W. Lou,Y.T. Hou, and H. Li, “Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 11, pp. 3025–3035, 2014.

[13] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, “Efficient multi-keyword ranked query on encrypted data in the cloud,” in *Proc. IEEE Parallel and Distributed Systems (ICPADS’12)*, Singapore, Dec. 2012, pp. 244–251.

[14] J.Li,Q.Wang,C.Wang,N.Cao,K.Ren,andW.Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in *Proc. IEEE INFOCOM’10*, San Diego, CA, Mar. 2010, pp. 1–5.

[15] M. Chuah andW. Hu, “Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data,” in *Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS’11)*, Minneapolis, MN, Jun. 2011, pp. 383–392.

[16] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-key encryption with fuzzy keyword search:A provably secure scheme under keyword guessing attack,” *Computers, IEEE Transactions on*, vol. 62, no. 11, pp. 2266–2277, 2013.

[17] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in *IEEE INFOCOM*, Toronto, Canada, May 2014, pp. 2112–2120.

[18] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 8, pp. 1467–1479, 2012.

[19] C.Wang, K. Ren, S.Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity search over outsourced cloud data,” in *Proc. IEEE INFOCOM’12*, Orlando, FL, Mar. 2012, pp. 451–459.

[20] W.Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, “Secure distributed keyword search in multiple clouds,” in *Proc. IEEE/ACM IWQOS’14*, Hongkong, May 2014, pp. 370–379.

[21] W.Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” in *Proc. IEEE INFOCOM’14*, Toronto, Canada, May 2014, pp. 226–234.

[22] Q. Zheng, S. Xu, and G. Ateniese, “Vabks:Verifiable attribute-based keyword search over outsourced encrypted data,” in *Proc. IEEE INFOCOM’14*,Toronto, Canada, May 2014, pp. 522– 530.

[23] T. Jung, X. Y. Li, Z. Wan, and M. Wan, “Privacy preserving cloud data access with multi-authorities,” in *Proc. IEEE INFOCOM’13*,Turin, Italy, Apr. 2013, pp. 2625–2633.

[24] Q. Liu, C. C.Tan, J.Wu, and G.Wang, “Efficient information retrieval for ranked queries in cost-effective cloud environments,” in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 2581–2585.

[25] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” *Journal of the ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[26] I. H. Witten, A. Moffat, and T. C. Bell, *Managing gigabytes: Compressing and indexing documents and images*. San Francisco, USA: Morgan Kaufmann, 1999.

[27] W.Zhang,S.Xiao,Y.Lin,T.Zhou,andS.Zhou, “Secure ranked multi-keyword search for multiple data owners in cloud computing,” in *Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014)*. Atlanta, USA: IEEE, jun 2014, pp. 276–286.

[28] IETF, “Request for comments database.” [Online]. Available: http://www.ietf.org/rfc.html

[29] H. Systems, “Hermetic word frequency counter.” [Online]. Available: http://www.hermetic.ch/wfc/wfc.htm

[30] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[31] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” in *Proc. IEEE ASIACCS’13*, Hangzhou, China, May 2013, pp. 71–81.

[32] J. Hur, “Improving security and efficiency in attribute-based data sharing,” *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*, vol. 25, no. 10, pp. 2271–2282, 2013.

[33] R. Agrawal, J. Kiernan, R. Srikant, andY. Xu, “Order preserving encryption for numeric data,” in *Proc. ACM SIGMOD’04*, Paris, France, Jun. 2004, pp. 563–574.

[34] A. Boldyreva,N. Chenette, Y. Lee, and A. O, “Orderpreserving encryption revisited: Improved security analysis and alternative solutions,” in *Proc. Advances in Cryptology (CRYPTO’11)*, California USA, Aug. 2011, pp. 578–595.

[35] Y.Yi, R. Li, F. Chen, A. X. Liu, and Y. Lin, “A digital watermarking approach to secure and precise range query processing in sensor networks,” in *Proc. IEEE INFOCOM’13*, Turin, Italy, Apr. 2013, pp. 1950–1958.

[36] R.A.Popa,F.H.Li,andN. Zeldovich,“An ideal-securityprotocol for order-preserving encoding,” in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 463–477.

[37] F. Kerschbaum and A. Schroepfer, “Optimal average-complexity ideal-security order-preserving encryption,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 275–286.