ISSN 2319-2720
Volume 7, No.2, April – June 2018
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn39722018.pdf
https://doi.org/10.30534/ijccn/2018/39722018

TWO CLOUD SECURE DATABASE FOR NUMERIC RANGE SQL QUERIES WITH PRIVACY PRESERVING

Sandhya S[1], Sowmya K[2], Varsha T Gowda[3], Pallavi L[4],,Mr.Hemanth Y K[5]
[1]EWIT, India, sandhyagowdas6@gmail.com
[2]EWIT, India, sowmyakdevadiga1996@gmail.com,
[3]EWIT, India, varshatg96@gmail.com
[4]EWIT, India, pallavilakshmikanth@gmail.com
[5]Mr.Hemanth Y K, Assistant Prof. Department of CSE, hemanthyk@ewit.edu

ABSTRACT

Industries and individuals outsource database to realize convenient and low-cost applications and services. In order to provide sufficient functionality for SQL queries, many secure database schemes have been proposed. However, such schemes are vulnerable to privacy leakage to cloud server. The main reason is that database is hosted and processed in cloud server, which is beyond the control of data owners. For the numerical range query (“>”, “<”, etc.), those schemes cannot provide sufficient privacy protection against practical challenges, e.g., privacy leakage of statistical properties, access pattern. Furthermore, increased number of queries will inevitably leak more information to the cloud server. In this paper, we propose two-cloud architecture for secure database, with a series of intersection protocols that provide privacy preservation to various numeric-related range queries. Security analysis shows that privacy of numerical information is strongly protected against cloud providers in our proposed scheme.

Keyword: Database, range query, privacy preserving, cloud computing.

1. INTRODUCTION

The growing industry of cloud has provide a service paradigm of storage/computation outsourcing helps to reduce users’ burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users [1], [2], [3]. However, due to the privacy concerns that the cloud service provider is assumed semi-trust (honest-but curious.), it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsourcing sensitive data - such as database system - to cloud [4], [5], [6]. The typical scenario for outsourced database is described as that in Crypt DB [7]: A cloud client, such as an IT enterprise, wants to outsource its database to the cloud, which contains valuable and sensitive information (e.g. Transaction records, account information, disease information), and then access to the database (e.g. SELECT UPDATE, etc.) [8], [9], [10], [11], [12].Due to the assumption that cloud provider is honest-but-curious [13], [14], the cloud might try his/her best To obtain private information for his/her own benefits. Even worse, the cloud could forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk. The privacy challenge of outsourced database is two-hold. 1) Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers; 2) Besides data privacy, clients’ frequent queries will inevitably and gradually reveal some private information on data statistic properties. Thus, data and queries of the outsourced database should be protected against the cloud service provider.

One straight forward approach to mitigate the security risk of privacy leakage is to encrypt the private data and hide the query/access patterns. Unfortunately, as far as we know, few academic researches satisfy both properties so far. Crypt DB [7] is the first attempt to provide a secure remote database application, which guarantees the basic confidentiality and privacy requirement, and provides diverse SQL queries over encrypted data as well. Crypt DB uses a series of cryptographic tools to achieve this security functionality. Especially, *order preserving encryption* [15] is utilized to realize numeric related range query processes. From the perspective of query functionality, Crypt DB supports most kinds of numerical SQL queries with such cryptology. However, such privacy leakage hasn’t been well addressed thoroughly, since OPE is relatively weak to provide sufficient privacy assurance. Some specific purpose cryptology like *order preserving encryption* (OPE) will expose some private information to the cloud service provider naturally: As it is designed to preserve the order on cipher texts so that it can be used to conduct range queries, the order information of the data, the statistical properties derived there from, such as the data distribution, and the access pattern will be leaked.

Can we design a new database system to provide range queries with stronger privacy guaranty**?**

From the work in [16], the privacy can be preserved Against the cloud, if the sensitive knowledge is partitioned into two parts, and distributed to two *non-colluding* clouds. In the literature [17], the authors also introduce a two-party system to design a secure ken query scheme, which enables the client to query *k* most similar records from the cloud securely. This divide-and-conquer mechanism can know any private information from one singe isolated part of the knowledge, and each of both clouds only knows its own part. In this paper

we introduce a secure two-cloud database service architecture, where the two clouds are *non-colluding* and both of them knows only part of knowledge. Based on this architecture, we further propose a series of interaction protocols for a client to conduct numeric-related query over encrypted data from remote cloud servers. The numeric-related query includes common query statements, such as *greater than*, *less than*, *between*, etc..

The main contribution of this paper can be summarized as follows:

We propose a two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud, while the knowledge of query pattern is well partitioned into two parts, and knowing only one cannot reveal any private information;

We then present a series of intersection protocols to provide numeric-related SQL range query with privacy preservation, and especially, such protocols will not expose order-related information to any of the two non-colluding clouds.

2. RELATED WORKS

Fuzzy query over encrypted data is becoming a popular topic, since in practical scenarios, some query requests usually want to retrieve data with similar, rather than exactly same indexes[18], [19]. Fuzzy searchable encryption has been introduced for cloud computing in many literatures, such as [20], [21], [22], [23], [24], and [25]. These schemes deal with the issue that search keywords allows small-scaled distinction in character/numeric level. Specifically for numerical keywords, the query predicate can get numerical records within a range. Some schemes targeted at spatial query, especially ken [17], [26], [27], [28], [29], which focus on the distance between the query vector and the data. They usually inquire about certain spatial objects (or several numerical attributes) related to the others within a certain distance. Range query [30], [31], [32] has been proposed for that purpose. However, such existing range query schemes are not suitable for practical secure database due to high storage overhead to maintain the corresponding cipher text.

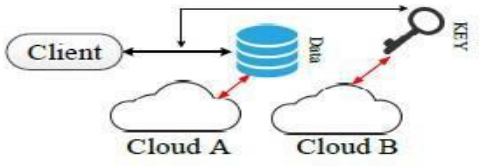
Subsequently, order preserving encryption (OPE) [15], [33], [34], [35], [36] has been introduced to provide numeric-related range query in structured database, such as Crypt [7]. OPE preserves the order of values in encryption held, while hiding the actual values. Until now, OPE has been developed to increase both efficiency and security [15], [34],
[36]. Popa et al. [15] proposed an ideal-security OPE scheme, in which, an adversary - even having the access privilege to a set of Cipher texts - still cannot learn the knowledge of data with non-negligible advantage. Although in Boldyreva et al. [34]'s definitions, such property has achieved the security boundary of OPE (IND-OCPA),that ideal-secure OPE still cannot satisfy the privacy requirement of secure database. OPE inherently exposes the order of data, that can be utilized to reveal an amount of critical knowledge, although it is always expected to be private.Bohli et al. [16] proposed a multi-cloud architecture, which can protect the private information of many outsourced services, including database. The main contribution is the introduction of four knowledge partition patterns among multiple cloud service providers:

(1) Replication of applications,
(2) Partition of application system into tiers,
(3) Partition of application logic into fragments, and
(4) Partition of application data into fragments.

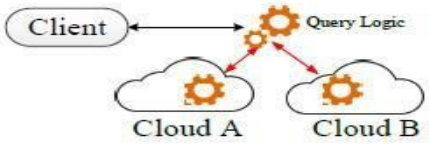
The knowledge is partitioned into two fragments, respectively stored in one cloud, who is assumed to be non-colluding to another cloud. Therefore, no cloud can get any private information in such multi-cloud architecture. However, Bohli et al. [16] have not provided a detailed scheme or realization for database. In this paper, with the multi-cloud prototype in [16], [37], [38], we introduce a two non-colluding cloud database service architecture and propose a series of practical interaction protocols to conduct database range queries. In addition to securing the data contents, our scheme also well preserves the privacy of logical relationship among data contents, such as data order, the privacy of the statistical properties and query pattern.

3. METHODOLOGY

3.1 SYSTEM ARCHITECTURE:



(a) Knowledge Partition of Stored Data



(b) Knowledge Partition of Query Logic

Our proposed secure database system includes a database administrator, and two non-colluding clouds. In this model, the database administrator can be implemented on a client's side from the perspective of cloud service. The two clouds (refer to Cloud A and Cloud B), as the server's side, provide the storage and the computation service. It briefly depicts the architecture of our outsourced secure database system in our scheme. The two clouds work together to respond each query request from the client/authorized users (availability). For privacy concerns, these two clouds
are assumed to be non-colluding with each other, and they will follow the intersection protocols to preserve privacy of data and queries (privacy). In our scheme, the knowledge of stored database and queries is partitioned into two parts, respectively stored in one cloud. The mechanism guarantees that knowing either of these two parts cannot obtain any
useful privacy information.

As shown in to conduct a secure database, data are encrypted and outsourced to be stored in one cloud (Cloud A), and the private keys are stored in the other one (Cloud B). For each query, the corresponding knowledge includes the data contents and the relative processing logic. We utilize a prototype of knowledge partition, dividing application logic into two parts, which is bristly proposed by Bohli et al. In [16]. The application logic, as a secret knowledge, is partitioned into two parts, each of which is only known to one cloud. This prototype. Intuitively, this two-cloud architecture increases some complexity to some extent, and we will analyze and point out that this overhead is acceptable in Section VII-A.

3.2 MODULES

1.Potential Threats and Privacy Requirements

This section describes the potential threats and the privacy requirements when the database is outsourced to public cloud. The stored data contents and the query processes. Although there are many data encryption schemes, some fail to provide sufficient privacy preservation after statistical analysis: Repeated and large-amount query processes not only leak the access patterns, but also disclose the stored encrypted data progressively.

2.Data contents Module:

Besides the static properties can disclose the private information of data contents, such properties themselves are already sensitive and private for the client. Order Preserving Encryption(OPE), which is widely used in constructing the secure database, with support of range queries, directly exposes the statistical information in the encryption field. Furthermore, the leakage of statistic properties is part of the nature of outsourced cloud database service: the cloud can learn the statistical properties (like order) by repeated query requests. As an example, It describes such an attack: After two simple queries over one same column, the order relationship of some data in certain column can be determined. There are also some other direct and indirect scenarios to leak statistical properties. In this way, even though the order property is not exposed to the semi-trusted cloud at the beginning, the cloud can gradually find out the order information after many query requests.

3.Query pattern Module.

The query pattern also contains privacy information, as they can reveal the client's purpose of the query. Even worse, such pattern can leak some statistical properties, as discussed above. Based on the above discussion, we assert that an outsourced secure database providing numeric-related queries should prevent the following private information from being obtained by the honest-but-curious clouds.

4.Privacy of Item Values Modules:

An ideal scheme is required to make nothing of the statistical properties be leaked to the curious clouds. However, the privacy leakage of statistical properties in a practical Outsourced database system is inevitable, as returning subset of data rather than universe requires knowledge for filtering. For instance, if the client wants to retrieve a from the outsourced database, a cloud server without any knowledge of the order can only return all items of the database to the client, which is not usable.

3.3 PROPOSED SYSTEM:

This paper presents two-cloud architecture for secure database, with a series of intersection protocols that provide privacy preservation to various numeric-related range queries. Security analysis shows that privacy of numerical information is strongly protected against cloud providers in our proposed scheme.

We propose a two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud, while the knowledge of query pattern is well partitioned into two parts, and knowing only one cannot reveal any private information;

We then present a series of intersection protocols to provide numeric-related SQL range query with privacy preservation, and especially, such protocols will not expose order-related information to any of the two non-colluding clouds.

CONCLUSION

In this paper, we presented two-cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. At the same time, with the support of range queries, it not only protects the confidentiality of static data, but also addresses potential privacy leakage in statistical properties or after large number of query processes. Security analysis shows that our scheme can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed scheme is efficient.

REFERENCES

[1] M. Armrest, A. Fox, R. Griffith, A. D. Joseph et al., "A View of cloud computing," Communications of the ACM, vol.
53, no. 4, pp. 50–58, 2010.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp.220–232, 2012.

[3] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[4]J.W.RittinghouseandJ.F.Ransome,Cloudcomputing:implementation, management, and security. CRC press, 2016.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vole 28, no. 3, pp. 583–592, 2012.

[6] H. T. Dinah, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing,vol.13,no.18,pp.1587–1611, 2013.

[7] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "Crypt: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp.85–100.

[8] C. Curino, E. P. Jones, R. A. Popa, N. Malviya et al.,
"Relational cloud: A database-as-a-service for the cloud," 2011, http://hdl.handle.net/1721. 1/62241.

[9] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in Advances in Cryptology-EUROCRYPT 2015. Springer, 2015, pp. 404–436.

[10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE Transactions on Computers, vol. 65, no. 10, pp.
3184–3195, 2016.

[11] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[12] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," in Annual Cryptology Conference. Springer, 2011, pp. 111–131.

[13] W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.

[14]K.Xue,Y.Xue,J.Hong,W.Li,H.Yue,D.S.Wei,andP.Hong," RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.

[15] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13)IEEE, 2013, pp. 463–477.

[16] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau,"Security and privacy-enhancing multicloud architectures," *IEEE Transactions on Dependable and Secure Computing*, vol.10,no.4,pp.212–224,2013.

[17] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments," in *2014 IEEE 30th International Conference on Data Engineering*.IEEE, 2014, pp. 664–675.

[18] F. Hao, J. Daugman, and P. Zielinski, "A fast search algorithm for a large fuzzy database," *IEEE Transactions on Information Forensics and Security*, vol. 3,no.2, pp.2203–212,2008.

[19] A. Castelltort and A. Laurent, "Fuzzy queries over No SQL graph databases: perspectives for extending the cipher language," in *International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems*. Springer, 2014,pp. 384–395.

[20] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM2010)*. IEEE,2010,pp.1–5.

[21] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proceedings of the 30th IEEE International Conference on Distributed Computing Systems (ICDCS2010)*. IEEE, 2010, pp.253–262.

[22] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp.
222–233, 2014.

[23] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in *Proceedings of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM2014)*. IEEE, 2014, pp.2112–2120.

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

[25] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Transactions on Information Forensics and Security*, vol. 11, no.12, pp. 2706–2716, 2016.

[26] Z. Yu, Y. Liu, X. Yu, and K. Q. Pu, "Scalable distributed processing of k nearest neighbor queries over moving objects," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 5, pp. 1383–1396, 2015.

[27] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*. ACM,
2009,pp.139–152.

[28] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical approximate k nearest neighbor queries with location and query privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 6, pp 1546–1559,2016.

[29] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vole 27, no. 2, pp.340–352, 2016.

[30] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of Cryptography*. Springer,2007,pp.535554.

[31] E. Shi, J. Bettencourt, T. H. Chan, D. Song, and A. Per rig, "Multi dimensional range query over encrypt data," in IEEE Symposium on Security and Privacy (SP'07).IEEE,2013

[32] Y. Yang, H. Li, M. Wen, H. Lou, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014

IEEE International Conference on Communications (ICC2014).IEEE,2014,pp.951–956.

[33] R. Agrawal , J. Kiernan, R. Srikant, and Y. Xu," Order preserving encryption for numeric data, in Proceedings of the 2004 ACM SIGMOD International Conference Management of Data. ACM, 2004, pp.563 574.

[34] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Advances in Cryptology–EUROCRYPT 2009.Springer, 2009, pp.224-241

[35] H. Kadhem, T. Amagasa, and H. Kitagawa, "MV-OPES: Multi valued order preserving encryption scheme: A novel scheme for encrypting integer value to many different values," IEICE Transactions on Information and Systems,vol. 93, no.9,pp.2520–2533,2010.

[36] Z. Liu, X. Chen, J. Yang, C. Jia, and I. You, "New order preserving encryption model for outsourced databases in cloud environments,"Journal of Network and Computer Applications,vol.59,pp.198–207,2016.

[37] M. A. AlZain, E. Paraded, B. So, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, 2012,pp. 5490–5499.

[38] E. Stefanov and E. Shi, "Multi-cloud oblivious storage," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013, pp.247–258.

Sandhya S: pursuing B.E in CSE, EWIT (VTU), Bengaluru, Her areas of interest are Java, Operating Systems, Database and C etc.

Sowmya K: pursuing B.E in CSE, EWIT (VTU), Bengaluru, Her areas of interest are Python, Database and Computer Graphics etc.

Varsha T Gowda: pursuing B.E in CSE, EWIT(VTU), Bengaluru, Her areas of interest are Database, Java language, Software Engineering etc.

Pallavi L: pursuing B.E in CSE, EWIT (VTU), Bengaluru, Her areas of interest are Database, Web technologies, Networking etc.

Hemanth Y K: Assistant Professor, Department of Computer Science & Engineering, East West Institute of Technology (VTU), Qualification B.E,M.Tech. His areas of interest are IoT, Artificial Intelligence, Machine learning, Data Analytics.