ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Certain Investigations on Effective Query Service Mechanism in Clouds

S.Dhaarani[1], K.Anitha[2], Prof.M.Sarmila[3] and Prof.S.Balamurugan[4]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3,4]

ABSTRACT: This paper details about various methods prevailing in literature for effective query service mechanisms in cloud. A privacy indexing for range query is discussed in detail. Methods for deriving privacy information from randomized data are portrayed. Geometric data perturbation for privacy preserving outsourced data mining and attack-resilient geometric data perturbation private information retrieval and Dynamic authenticated index structures for outsourced databases are examined. Various attacks view of distance preserving maps for privacy preserving data mining and privacy preserving index for range queries are semantically evaluated. Various methods to derive private information from randomized data are studied in detail. This paper would promote a lot of research in the area of query service mechanism in clouds.

KEYWORDS: Privacy Index, Data Perturbation, Dynamic Authentication, Privacy Preserving Data Mining(PPDP), Randomized Data.

I. INTRODUCTION

Researching on Cloud Security issues, makes to know about the use both in academic and as well as in industrial works. The Cloud can be used only through the Internet and the data stored in Cloud is very Secure and privacy so that the Authentication in Cloud by User can retrieve a Secure Transaction , in other hand the user must ensure that data received doesn't had an any error. Wang et al who addressed cloud is a Secured and Dependable storage area. Cloud servers can have a Byzantine failure which mean any unknown error can occur in Cloud and even an Colluding attack , to prevent the error data must be encrypted while Designing the Secure storage techniques. The Searching of encrypted data is an important concern in the Cloud in which queries are used to Obtain the data. Cloud should not know the Query but it must be able to return the records by specifying the keyword through the Query,thus the records are obtained only with the exact keyword. Many researcher had addressed about the security and privacy that protects in clouds, Wang et al had introduced Reed-Solomon erasure coding which is used to check the Multiple random symbol error. The Authentication by the users are been using the public Cryptographic Technique. Many Homomorphism Encryption have been suggested that cloud couldn't able to read the data while the cloud Computation , Using the homomorphism Encryption the cloud gets the Encrypted data by the User which mean a Cipher Text and this text is decoded and sent to the receiver and checks the cipher text received, but the Cloud cannot know what the data is been operated.

II. A PRIVACY PRESERVING INDEX FOR RANGE QUERIES

In this paper author introduced a privacy preserving techniques is data partitioning(bucketization). In this technique, authors built privacy preserving indices on sensitive attributes of a relational table. The author proposed two useful techniques for privacy measures. First, optimal algorithm for data partitioning which is used for maximizes the accuracy of query processing. Second, controlled diffusion algorithm is used for achieve the data privacy for data owners. In this both algorithm is used for efficient Query processing and accuracy measures. Then to achieve a data privacy from the outsides.

III. DERIVING PRIVATE INFORMATION FROM RANDOMIZED DATA

Data marking in privacy-preserving data mining is achieved by randomization is that the data have high risk of disclosing their. Private contents even though they are randomized. The author proposed two data construction

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

methods. Based on data correlation. One method, principle component analysis (p(a),and other method uses the Bayes estimate (BE). Authors analysed the relationship between data correlation and amount of private information. If data correlation is high the original data must be build up (or) reorganised more accurately. The author describes more private information can be revealed. Using this method, the data privacy is decreased data correlation affects the privacy of data. To improve data privacy, we can recognize the data.

IV. GEOMETRIC DATA PERTURBATION FOR PRIVACY PRESERVING OUTSOURCED DATA MINING

In this paper author describe the geometric data perturbation for privacy preserving outsourced data mining. These data perturbation act as major role in privacy preserving data mining because this does not guarantee to better privacy and usage. One of the earlier data mining model is multidimensional geometric information. Authors propose geometric data perturbation method, first is describes the several types of data mining model. Second it is compared with other perturbation that is random projection perturbation, rotation perturbation, translation perturbation and distance perturbation. Third perturbation against to three types of attacks naive-inference attacks, distance inference attacks. Geometric perturbation not only provide security also provide the accuracy compare to previous multidimensional perturbation techniques.

V. TOWARDS ATTACK-RESILIENT GEOMETRIC DATA PERTURBATION

In this paper describes the potential attacks to random geometric perturbation. Major challenges in this paper is privacy protection and data quality. In earlier many perturbation techniques such as random translation perturbation, random data perturbation are aim to provide the privacy and quality. This data perturbation is use for data owners to publish data while privacy data while privacy, we propose the framework of attacks and threats. This helps to analyze more attacks and geometric perturbation as well. They are four kinds of attack that is based upon the different level of knowledge.

VI. PRIVATE INFORMATION RETRIEVAL

In this paper author describes the private information retrieval data base are necessary resource for retrieving data. But these provided the privacy risk to user. In this paper author gave solution to the avoid replicating database and privacy retrieval problem . They can solve the retrieval problem can obtain the following

i. A two database project with communication complexity of 0(n 1/3)
ii. A project for a constant number, M of database with communication complexity 0(n 1/m)
iii. A project for 1/3 log2 n+1 database with total communication complexity 1/3(1+0(1)).log2 n.

VII. DYNAMIC AUTHENTICATED INDEX STRUCTURES FOR OUTSOURCED DATABASES

In this paper author describes the solution for ODB dynamic authenticated index structures. Outsourced database (ODB) is used for the database owner publishes its data through a remote servers. Query authentication is important part of ODB system. Existing solution for query authentication is a static scenarios based on the cryptographic primitives. In this work, we look at the solutions that, dynamic scenarios, in which the owners regularly update the data on serves. Finally, authors defined the query freshness, that data authentication has not been investigated before. In this paper, to improve the performance for data authentication both static and dynamic environments.

VIII. ATTACKER'S VIEW OF DISTANCE PRESERVING MAPS FOR PRIVACY PRESERVING DATA MINING

In this paper, author examines the preserving maps for privacy preserving data mining. This techniques is useful for data mining algorithm and used to transformed data. We examine how the attacker got the original information from the transformed data. The first is linear algebra and the second is principal component analysis. This techniques is used for computation efficient and good performance. It also used produce an error free result o the disrupted data. Searchable symmetric encryption(SSE) is used to store the data from one party to another party in a private manner. In this paper, author describes the solutions for SSE. SSE schemes is more efficient & secure. SSE Scheme introduces they67 two solutions. The first solution describes the design construction which avoid the pitfalls. The second solution,

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

the queries to the server can be chosen when we call adaptive SSE security. The both solutions are very efficient and stronger security over the encrypted data. The author additionally add multi user SSE in which the data owner is rights of submitting search queries. The SSE scheme present an efficient construction & achieves better performance using access control mechanisms.

IX. A PRIVACY PRESERVING INDEX FOR RANGE QUERIES

Transform the it operation of corporation is an emerging data management techniques. There were a privacy issues in database outsourcing. The data owners must trust the service providers is limited. In this paper author introduced a privacy preserving techniques is data partitioning(bucketization). In this techniques, authors built privacy preserving indices on sensitive attributes of a relational table. The author proposed two useful techniques for privacy measures. First, optimal algorithm for data partitioning which is used for maximizes the accuracy of query processing. Second, controlled diffusion algorithm is used for achieve the data privacy for data owners. In this both algorithm is used for efficient Query processing and Accuracy measures. .

X. DERIVING PRIVATE INFORMATION FROM RANDOMIZED DATA

Data marking in privacy-preserving data mining is achieved by randomization is that the data have high risk of disclosing their Private contents even though they are randomized. The author proposed two data construction methods. Based on data correlation. One method, principle component analysis (p(a)),and other method uses the Bayes estimate (BE). Authors analysed the relationship between data correlation and amount of private information. If data correlation is high the original data must be build up (or) reorganised more accurately. The author describes more private information can be revealed. Using this method, the data privacy is decreased data correlation affects the privacy of data. To improve data privacy, we can recognize the data.

XI. CONCLUSION AND FUTURE WORK

This paper detailed about various methods prevailing in literature for effective query service mechanisms in cloud. A privacy indexing for range query is discussed in detail. Methods for deriving privacy information from randomized data are portrayed. Geometric data perturbation for privacy preserving outsourced data mining and attack-resilient geometric data perturbation private information retrieval and Dynamic authenticated index structures for outsourced databases are examined. Various attacks view of distance preserving maps for privacy preserving data mining and privacy preserving index for range queries are semantically evaluated. Various methods to derive private information from randomized data are studied in detail. This paper would promote a lot of research in the area of query service mechanism in clouds.

REFERENCES

1. Huiqi Xu, Shumin Guo, and Keke Chen, "Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014
2. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order Preserving Encryption for Numeric Data," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2004.
3. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.K. Andy Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," technical report, Univ. of Berkerley, 2009.
4. J. Bau and J.C. Mitchell, "Security Modeling and Analysis," IEEE Security and Privacy, vol. 9, no. 3, pp. 18-25, May/June 2011.
5. S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge Univ. Press, 2004.
6. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOMM, 2011.
7. K. Chen, R. Kavuluru, and S. Guo, "RASP: Efficient Multidimensional Range Query on Attack-Resilient Encrypted Databases,"Proc. ACM Conf. Data and Application Security and Privacy, pp. 249-260, 2011.
8. K. Chen and L. Liu, "Geometric Data Perturbation for Outsourced Data Mining," Knowledge and Information Systems, vol. 29, pp. 657- 695, 2011.
9. K. Chen, L. Liu, and G. Sun, "Towards Attack-Resilient Geometric Data Perturbation," Proc. SIAM Int'l Conf. Data Mining, 2007.
10. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private Information Retrieval," ACM Computer Survey, vol. 45, no. 6, pp. 965-981, 1998.
11. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions, Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

12. N.R. Draper and H. Smith, Applied Regression Analysis. Wiley, 1998.
13. H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model,"Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2002.
14. T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning. Springer-Verlag, 2001.
15. B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. Very Large Databases Conf. (VLDB), 2004.
16. Z. Huang, W. Du, and B. Chen, "Deriving Private Information from Randomized Data," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2005.
17. A. Hyvarinen, J. Karhunen, and E. Oja, Independent Component Analysis. Wiley, 2001.
18. I.T. Jolliffe, Principal Component Analysis. Springer, 1986.
19. F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic Authenticated Index Structures for Outsourced Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2006.
20. K. Liu, C. Giannella, and H. Kargupta, "An Attacker's View of Distance Preserving Maps for Privacy Preserving Data Mining," Proc. 10th European Conf. Principle and Practice of Knowledge Discovery in Databases (PKDD), 2006.
21. M.L. Liu, G. Ghinita, C.S. Jensen, and P. Kalnis, "Enabling Search Services on Outsourced Private Spatial Data," The Int'l J. Very Large Data Base, vol. 19, no. 3, pp. 363-384, 2010.
22. Y. Manolopoulos, A. Nanopoulos, A. Papadopoulos, and Y. Theodoridis, R-Trees: Theory and Applications. Springer-Verlag, 2005.
23. R. Marimont and M. Shapiro, "Nearest Neighbour Searches and the Curse of Dimensionality," J. Inst. of Math. and Its Applications, vol. 24, pp. 59-70, 1979.
24. M.F. Mokbel, C. yin Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. 32nd Int'l Conf. Very Large Databases Conf. (VLDB), pp. 763-774, 2006.
25. P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 223-238, 1999.
26. S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. Very Large Databases Conf. (VLDB), 2010.
27. F.P. Preparata and M.I. I, Computational Geometry: An Introduction. Springer-Verlag, 1985.
28. M. Rudelson and R. Vershynin, "Smallest Singular Value of a Random Rectangular Matrix," Comm. Pure and Applied Math., vol. 62, pp. 1707-1739, 2009.
29. E. Shi, J. Bethencourt, T.-H.H. Chan, D. Song, and A. Perrig, "Multi-Dimensional Range Query over Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2007.
30. R. Sion, "Query Execution Assurance for Outsourced Databases," Proc. Very Large Databases Conf. (VLDB), 2005.
31. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2010.
32. P. Williams, R. Sion, and B. Carbunar, "Building Castles Out of Mud: Practical Access Pattern Privacy and Correctness on Untrusted Storage," Proc. ACM Conf. Computer and Comm. Security,2008.
33. W.K. K, D.W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure KNN Computation on Encrypted Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), pp. 139-152, 2009.
34. M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. Very Large Databases Conf. (VLDB), pp. 782-793, 2007.
35. H. Xu, S. Guo, and K. Chen, "Building Confidential and Efficient Query Services in the Cloud with Rasp Data Perturbation," Wright State Technical Report, http://arxiv.org/abs/1212.0610, 2012.
36. M.L. L, C.S. S, X. Huang, and H. Lu, "SpaceTwist: Managing the Trade-Offs among Location Privacy, Query Performance, and Query Accuracy in Mobile Services," Proc. IEEE Int'l Conf. Data Eng. (ICDE), pp. 366-375, 2008.
37. B.Powmeya , Nikita Mary Ablett ,V.Mohanapriya,S.Balamurugan,"An Object Oriented approach to Model the secure Health care Database systems,"In proceedings of International conference on computer , communication & signal processing(IC^3SP)in association with IETE students forum and the society of digital information and wireless communication,SDIWC,2011,pp.2-3
38. Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013
39. Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.
40. S.Balamurugan, P.Visalakshi, V.M.Prabhakaran, S.Chranyaa, S.Sankaranarayanan, "Strategies for Solving the NP-Hard Workflow Scheduling Problems in Cloud Computing Environments", Australian Journal of Basic and Applied Sciences, 8(15) October 2014.
41. Charanyaa, S., et. al., , A Survey on Attack Prevention and Handling Strategies in Graph Based Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 2(10): 5722-5728, 2013.
42. Charanyaa, S., et. al., Certain Investigations on Approaches forProtecting Graph Privacy in Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 1(8): 5722-5728, 2013.
43. Charanyaa, S., et. al., Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization. International Journal of Innovative Research in Computer and Communication Engineering, 2(3): 3554-3561, 2014.
44. Charanyaa, S., et. al., , Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 3(2): 5722-5728, 2014.
45. Charanyaa, S., et. al., Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
46. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
47. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
48. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

49. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
50. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
51. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
52. S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014.
53. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "Investigations on Methods Evolved for Protecting Sensitive Data", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
54. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "A Survey on Approaches Developed for Data Anonymization", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
55. S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014
56. S.Balamurugan,M.Sowmiya and S.Charanyaa, "Principles of Scheduling in Cloud Computing" Scholars' Press, Germany,, ISBN: 978-3-639-66950-3, 2014
57. S.Balamurugan, S.Charanyaa, "Principles of Database Security" Scholars' Press, Germany, ISBN: 978-3-639-76030-9, 2014