International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving

Kanad Kartey[1], Harshil Somia[2], Vivek Madawat[3], Pallavi Mathur[4]

[1,2,3] B.E Student, Dept. of Computer Engineering, D.Y.Patil Institute of Engineering & Technology, Ambi, Pune University ,Maharashtra, India
[4]Assistant Professor, Dept. of Computer Engineering, D.Y.Patil Institute of Engineering & Technology, Ambi, Pune University, Maharashtra, India

---

Abstract - In the present scenario businesses and people are outsourcing database to accomplish helpful administrations and minimal effort applications. These are buried in the cloud server, which is outside the ability to control of the data proprietor. The SQL Queries require a few secure database scheme for its undeniable working, yet this at long last prompts privacy spillage to the cloud server. For numerical range inquiry (>, <, and so forth.) these neglect to give adequate security insurance. A portion of the difficulties faced are privacy leakage of statistical attributes, access patterns and so on. Likewise increased number of queries will release more information to the cloud server. Thus regarding these issues numerous work have been done by various researchers. We have studied some of these research works and analyzed the best possible ways to come to the desired level of privacy preservation in the case of cloud computing. Some of the works studied are the fuzzy logic, range queries, CryptDB order preserving encryption and multi-cloud architecture.

Keyword — cloud computing, database, privacy preserving, range query.

1.INTRODUCTION

In the present circumstances as it can be seen cloud has taken the control over the IT business with its innumerable advantages. It holds the possibility to change an extensive segment of the IT business, making software considerably more appealing as an service. Cloud computing [1] is alluded to as SaaS (Software as a Service) since it renders the applications as administrations over the Web and the hardware and systems software in the data centres that offer those administrations. The hardware of data centre and software is called a cloud. Today the clouds can be open/public and in addition private. Private clouds are associated to the inner datacenters of a business or other association, not made accessible to the overall public. Cloud computing in this manner can be compressed as a blend of saas and utility computing, booting out the data centre (little + medium estimated). Security is the chief concern of the cloud computing. Cloud clients confront security dangers both from outside and inside the cloud. Shielding the information from the server itself is the pro of the main issues related with it. The server will by definition control the "bottom layer" of the product stack, which adequately goes around most known security methods. As said the cloud server is accepted as semi-trusted (honest-but-curious).

CryptDB [5], a framework that gives confidentiality to applications that utilize database administration frameworks (DBMSes). CryptDB permits to perform queries over encrypted data, likewise the SQL's very much characterized set of operators, and queries over encrypted data. CryptDB tends to the hazard of an inquisitive database administrator (DBA) who endeavors to learn private information (e.g., health books, financial articulations, individual data) by keeping an eye on the DBMS server by keeping the DBA from learning private information. It uses a few instruments to accomplish this security functionality.

One of the devices being the Order preserving encryption (OPE)[11][12] is generally utilized as a part of databases to process SQL Questions over encrypted information. It permits to perform order operations on ciphertext like the plaintext for e.g. data server can fabricate index perform range queries[10] and sort the encrypted information like the plaintext. Regardless of going to the security reason well, despite everything it uncovers the order of the ciphertext.

Therefore the objective of security protection of the outsourced information to a cloud server is refined by partitioning the sensitive knowledge into two parts and store them in two non-colluding clouds.

Moreover a secure database service architecture is acknowledged by utilizing two non-colluding clouds in which the information learning and query rationale is divided into two clouds. Henceforth, perceiving just a single cloud can't help uncover private data. Other than a progression of intersection protocols to give numeric-related SQL range queries [1] with privacy preservation is additionally executed and it won't uncover order related data to any of the two non-colluding clouds.

1.1: MOTIVATION

Privacy is most vital factor in cloud and modern day data storage services. Many creators took a shot at security protection, yet private data can't be fully protected by some technique. Everybody has some private and confidential data that they don't share to any one similarly all enterprises and organizations has numerous private information, they don't impart the information about this to anybody. If any of the information is leaked the organization's misfortune is sure shot. With the goal that we are turning on protection of the sensitive information. Present day innovation additionally takes a shot at privacy preservation [7] in the cloud servers.

2. RELATED WORK

John Daugman, and Piotr Zielinski have proposed a fast search algorithm for a large fuzzy database[9] that stores iris codes or data with a comparative binary structure. The hazy nature of iris codes and their high dimensionality is handled by the novel procedure, Beacon Guided Search (BGS), which does so by dispersing a large number of "beacons" in the search blank. BGS is considerably quicker than the present ES with an immaterial loss of precision. It takes substantially less memory and it doesn't rely upon caching data in storage, in this way murdering the requirement for complex storage administration. The preprocessing is basic and brisk. It holds up to 30% bit errors in the query and also up to seven cyclic rotations. The abundance memory put is little and promptly affordable– it bolsters dynamic upkeep, empowering simple ordering of new books.

Yin Yang, Hongwei Li, Mi Wen, Hongwei Luo, and Rongxing LuSS, proposed a ranked range query (RRQ) scheme [10], which can bolster both range query and ranked search. Established on the homomorphic Paillier cryptosystem, we utilize two super-increasing sequences to total multidimensional keywords. The first one is used to total one purchaser's or vender's multidimensional keywords to a collected number. The second one is connected to make a synopsis number by amassing the accumulated quantities of all sellers. Security investigation exhibits that RRQ can accomplish confidentiality of keywords, confirmation, information trustworthiness and query privacy. In any case, in the meantime more intricate pre-filtering rules, for example, "and", "or", "not" isn't finished by RRQ strategy.

R.A.Popa, C. Redfield, N.Zeldovich and H.Balakrishnan proposed CryptDB, a framework to defend the private information in databases from firstly the inquisitive cloud server itself and secondly the application server's bargains. CryptDB fundamentally includes utilizing the range queries productively finished the encrypted information utilizing a novel SQL-aware encryption system. It limits the data uncovered to the untrusted database server. Regardless of satisfying the assignment of protection safeguarding, still a few information is uncovered in the process.

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu proposed Order Preserving Encryption for Numeric Data[11] that enables any comparison operation to be straightforwardly connected on encrypted information. Query results produced are sound (no false hits) and complete (no false drops). OPES (Order Preserving Encryption Scheme) enables comparison operations to be specifically connected on encrypted information, without decrypting the operands. Accordingly, balance and range inquiries and also the MAX, MIN, and COUNT , GROUP BY and ORDER BY queries can be specifically prepared over encrypted data. OPES results are correct and don't contain false positives , a value in a column can be modified or a new value can be inserted in a column without requiring changes in the encryption of other values and it can be effortlessly incorporated with existing database frameworks. Encryption of non-numeric information, for example, factor length strings aren't finished by OPES. Also while applying SUM or AVG to a group the values should be decrypted.

Raluca Ada Popa, Frank H. Li, Nickolai Zeldovich, proposed "An Ideal-Security Protocol for Order-Preserving Encoding", which accomplishes perfect security. The fundamental method utilized is variable/mutable ciphertexts,which implies, the ciphertexts for few plaintext values change and its demonstrated that impermanent ciphertexts are required for perfect security. mOPE is superior to anything OPE scheme by 1-2 requests of extent. The same-time OPE security (sTOPE)[7] executes such that only the order of items present in the database is known. mOPE and stOPE utilize Merkle hashing to secure clients against a malevolent server. Although leak the order information of the data in plaintext. Furthermore the prototype issues only single query at a time where more finegrain ordering is possible.

J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, proposed the Security and privacy-enhancing multicloud architectures[8], This paper works as an overview paper where creators talked about the security in open cloud and multiple cloud. Also the high potential for security prospects in cloud computing have been discussed. Homomorphic encryption and secure multiparty calculation protocols to be exceptionally encouraging regarding both technical security and regulatory compliance. However there is no single ideal way to deal with cultivate both security and legal compliance in an omniapplicable way. The confinements of these methodologies just originate from their restricted applicability and high multifaceted nature being used.

M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, proposed the Cloud computing security from single to multi-clouds, It indicates security in single cloud and multiple clouds[13].

Additionally demonstrates some limitation and points of interest in security in cloud computing. Single clouds work on three phases SaaS,PaaS,IaaS. Clients and bussiness organizations don't lose their private data because of vindictive attaker in the cloud. It has a high capacity to diminish security chances that influence the cloud computing client. Find conceivable to conceivable confinement. However the service availability is still a disappointment and also there is a loss of administration accessibility.

2.1 LITERATURE SURVEY

Sr. No.	AUTHOR	APPROACHES	ADVANTAGES	DISADVANTAGES
1.	John Daugman, Piotr Zielinski	Fast search algorithm for a large fuzzy database	takes less memory, Doesn't require complex storage administration.	interpret any fuzzy query statement into a crisp query and evaluate
2.	Yin Yang, Hongwei Li, Mi Wen, Hongwei Luo, and Rongxing LuSS,	ranked range query (RRQ) scheme	Keyword confidentiality, information trustworthiness ,query privacy.	
3.	R.A.Popa, C. Redfield, N.Zeldovich and H.Balakrishnan	CryptDB,	limits the uncovered data to the untrusted database server.	a few information is uncovered in the process.
4.	Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu	Order Preserving Encryption for Numeric Data	Query results are sound (no false hits) and complete (no false drops). MIN,MAX,SUM/AVG can be prepared	Encryption of non-numeric information aren't finished by OPES. Data for SUM or AVG to a group should decrypted.
5.	Raluca Ada Popa, Frank H. Li, Nickolai Zeldovich,	"An Ideal-Security Protocol for Order-Preserving Encoding ",	mOPE is superior to any OPE scheme by 1-2 requests of extent. Only the order of items present in the database is known.	issues only single query at a time where more finegrain ordering is possible.
6.	J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau,	Security and privacy enhancing multicloud architectures	Provides technical security and regulatory compliance.	both security and legal compliance cant be implemented together.
7.	M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom,	The Cloud computing security from single to multi-clouds,	Find conceivable to conceivable confinement.	The service availability is a disappointment loss of administration accessibility.

3.CONCLUSIONS

In this paper, we have studied the various techniques and protocols associated with the privacy preservation of the outsourced data to the external cloud server. In order of the advance in this field some of the works include the fuzzy logic, range queries, order preserving encryption and multi-cloud architecture. The fuzzy logic implemented the, Beacon Guided Search (BGS), which requires substantially less memory and no complex storage mechanism. The Range Queries operate by implementing the RRQ can accomplish confidentiality of keywords, confirmation, data integrity and query privacy. Then came the CryptDB which fundamentally includes utilizing the range queries productively finished the encrypted information utilizing a novel SQL-aware encryption system. However some data is still exposed to the cloud server. The order preserving encryption is one of the tools used by the CryptDB which enables comparison operations to be specifically connected on encrypted information, without decrypting the operands. But encryption of non-numeric information isn't possible with this tool. Later the multi-cloud architecture was introduced which introduced the idea of partitioning the sensitive information and query logic into two different non-colluding clouds which don't have the knowledge about each other. However this architecture doesn't hold true for queries such as SUM/AVG.

ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We thank the college authority for providing the required infrastructure and technical support. Finally, we extend our heartfelt gratitude to friends and family members.

REFERENCES

[1] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security ,2017

[2] M. Armbrust, 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.

[3] 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.

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

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

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

[7] 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, pp. 463–477, 2013.

[8] J.-M. Bofhli, 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.

[9] 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. 203–212, 2008.

[10] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014 IEEE International Conference on Communications (ICC2014). IEEE, Vol.2, No.4,April 2014

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

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

[13] M. A. AlZain, E. Pardede, B. Soh, 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, pp. 5490–5499, 2012.