www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9637-9642

A Literature Survey on performance evaluation of query processing on encrypted database

Rajendra H. Rathod [1], Dr.C.A.Dhote [2]

[1] Prof.Ram Meghe Institute of Technology & Research,
Badnera-Amravati: 444701
rh_rathod@yahoo.com

[2] Prof.Ram Meghe Institute of Technology & Research,
Badnera-Amravati: 444701
vikasdhote@rediffmail.com

ABSTRACT: ***All database systems must be able to respond to requests for information from the user that is process queries. Secure and efficient algorithms are needed that provide the ability to query over encrypted database and allow optimized encryption and decryption of data. Data encryption is a strong option for security of data in database and especially in those organizations where security risks are high. Firms outsourcing their databases to untrusted parties started to look for new ways to securely store data and efficiently query them. When we apply encryption on database then we should compromise between the security and efficient query processing, because the operations of encryption and decryption greatly degrade query performance.***

This paper presents a survey on various encryption algorithms and identifies many of the common issues, themes, and approaches that cover query processing. Also in this paper a survey is made based on performance of query processing as well as pros and cons of existing algorithms.

Keywords: Data Security, Query Processing, Encryption, RC6, REA.

1. Introduction

A database query is the vehicle for instructing a DBMS to update or retrieve specific data to/from the physically stored medium. Obtaining the desired information from a database system in a predictable and reliable fashion is the scientific art of Query Processing. Database system must be able to respond to requests for information from the user i.e. process queries [32]. Database security is always provided to provide the information to the user securely when user queries. Database security has been provided by physical security and operating system security. Neither of these methods sufficiently provides a secure support on storing and processing the sensitive data. Cryptographic support is important dimension of database security [1]. Many organizations cannot work properly if their database is down, so they need its protection. Also the information should not fall into the hands of those who would misuse it. [9]. Protecting the confidential data stored in a repository is the database security. So encryption in database system is an important issue, as protected and efficient algorithms are essential that provides the ability to query over encrypted database and allow encryption and decryption of data. This paper ensures maximum protection and limits the time cost (delay time) for encryption and decryption so as to not decrease the performance of a database system [2]. However, designing a database that will achieve security requirement is very difficult, since a database system processes large amount of data in complex ways [3]. This usually implies that the system has to sacrifice the performance to obtain the security. When data is stored in the form of cipher, we have to decrypt all data before querying them [1]. The performance measure of query processing will be conducted in terms of query execution time that is delay time. A comparison has been presented for other encryption algorithms for encryption and decryption times [9]. The remainder of this paper is organized as follows. Section 2 discusses the survey of the papers on query processing on encrypted databases performance. Section 3 describes the comparative table of various papers on query process performance on encrypted database. Finally section 4 presents approach to solve the problem faced in various papers related to encryption of database and section 5 presents conclusion.

2. Literature Survey

Literature review is the process of presenting the summary of the journal articles, conference papers and study resources. So in this section we have studied the related topics and summarized it below.

Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie, Osama Faragallah in [1] is conducted on encryption of data of various sizes and video files. Several performance matrices are

collected like encryption time, CPU process time, and CPU clock cycle and battery power. Encryption time is used to calculate the throughput of an encryption scheme. In this paper authors propose a new encryption algorithm, Reverse Encryption Algorithm (REA). This paper observes a method for evaluating query processing performance over encrypted database with the proposed encryption algorithm REA and with the most common encryption algorithm AES. The performance measure of query processing conducted in terms of query execution time. REA represents a significant improvement over the encrypted databases. The results of a set of experiments show that REA can reduce the cost time of the encryption/decryption operations and improve the performance. But the encryption of database is not so truthful and it needs some extra security by encrypting the data with another algorithm so that the security may be tighten without degrading the performance.

Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud [2] has conducted a comparison between the result of the selected different encryption and decryption scheme in terms of the encryption time. Experimental results are for the selected six encryption algorithms at different encoding method. A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm. The selected algorithms were AES, DES, and 3DES, RC6, Blowfish and RC2.

The following tasks performed to check the performance

- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different en-coding bases namely; hexadecimal base encoding and in base 64 encoding.
- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.
- A study is performed on the effect of changing data types - such as text or document, audio file, and video file - for each cryptography selected algorithm on power consumption.
- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

It concludes that there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. In the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Also 3DES still has low performance compared to algorithm DES. In the case of audio and video files we found the result as the same as in text and document. And in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption.

Authors Ayman Mousa, Osama Faragallah, Elsayed Nigm, and Elsayed Rabaie [3] introduced an encryption algorithm called REA, restating its benefits and functions over other similar encryption algorithms. It examines a method for evaluating the performance of REA and compares it with most common encryption algorithms like DES, 3DES, RC2, AES and BLOWFISH. A comparison has been conducted for those encryption algorithms at encryption and decryption time. The result shows the advantages of REA over other algorithms in terms of the encryption and decryption time. Also results shows that Blowfish requires less encryption and decryption time than all algorithms except REA. 3DES has low performance in terms of encryption and decryption time when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. RC2 has low performance in terms of encryption and decryption time when compared with other five algorithms.

Manish Sharma, Atul Chaudhary, Santosh Kumar [4] had proposed two tables for a single main table for introducing the security in database. The first table contains the actual data and the second one contains only that data on which the search query runs. The first encrypted data table have sensitive data column and encrypted using strong encryption algorithm. In the second, Query Table, the data column is copied from the first Encrypted Data Table is kept in the unencrypted form and the key column in the encrypted form. And also the rows of the Query Table will be reorder randomly. In this paper author proposed that the actual security is introduced by hiding the relationship between the encrypted data table and query table.

Naoual MOUHNI, Abderrafiaa EL KALAY [5], studied the existing projects that treat the query processing problem across heterogeneous data sources are considered. Example of some existing query processing architecture are discussed in this paper: XQuery Based processing system, OBSERVER to support Query processing. In this paper new track of research have been discovered to optimize and improve existing systems and algorithm for data cleaning and query processing to meet the new data environment requirements such as handling big amount of data in an efficient way, integrate data from different data domains and eliminating duplicate data in case of big data sets with the minimum loss of information by improving the learning machine algorithms and minimizing the human intervention.

Arvind Arasu, Ken Eguro, Raghav Kaushik, Ravi Ramamurthy[6], authors introduces a system with data encryption, where sensitive columns are encrypted before they are stored to address data security. In this paper, author proposed a system for cloud DBMS, database-as-a-service. The author organizes the tutorial around three broad approaches to query processing over encrypted data:

1. Homomorphic Encryption: Homomorphic encryption is a specially designed encryption scheme that allows computation directly over encrypted data.
2. Client-Server based Approaches: Here, query processing over part of data in plaintext or encrypted using (partially) homomorphic encryption is performed at the server and the remainder, at the client, which is assumed to be trusted.
3. Trusted Hardware based Approaches: These approaches use a secure, tamper-proof hardware at the server to securely decrypt data and perform computations.

This paper is focused less on issues such as checking the correctness of query answers, but survey techniques and results in Homomorphic encryption.

Nian Liu, Yajian ZhOU, Xinxin Niu, Yixian Yang [7] had proposed a querying encrypted character data in DAS model, a cryptographic scheme of character data in relational database. A cryptographic scheme of character data in relational database is proposed in this paper. The core idea was to store the

positions of all the character strings in database. For character data type, double filtration method and positions encryption method are proposed.

Ayman Mousa, Osama S. Faragallah and S. EL-Rabaie, E. M. Nigm [9] have proposed a novel encryption algorithm "Reverse Encryption Algorithm (REA)". The proposed algorithm REA is simple and yet leads to a cipher. The proposed algorithm REA is a symmetric stream cipher that can be effectively used for encryption and safeguarding of data. The various factors are used as the secure and efficient criteria such as the key space, the key sensitivity, the security of data against attacks, the computational speed, the information entropy, and the correlation coefficient. REA is compared with the most common encryption algorithms namely: DES, 3DES, RC2, AES and Blowfish. The comparisons have been conducted for those encryption algorithms at computational speed (encryption and decryption time) and secure analysis such as information entropy and correlation coefficient. Also it analyzes the security of the proposed encryption algorithm REA and compares it with the most common encryption algorithms namely: DES, 3DES, RC2, AES and Blowfish. A comparison has been presented for the security.

Purushothama B R, B B Amberker [12] have presents the performance of the query processing without compromising the privacy of the data and the queries. The number of operations (decryption) performed to process a matching queries is in the order of the size of the result set as compared to the basic scheme in which is sequential for any matching query. Author has provided an idea to reduce the number of cryptographic operations required in processing a matching query.

Mohammed Alhanjouri, Ayman M. Al Derawi [14] first presents an attack model and the main relevant challenges of data security, encryption overhead, key management, and integration footprint. This paper had proposed a method of query over encrypted data in database that can work with many data types. It uses open source database and add a layer above any kind of DBMS, this layer have the responsibility to manage the way to query over encrypted data. The client will work over the layer which will contact with DBMS. In this paper authors used AES-256 to encrypt the preselected column that's usually contains a high important data that is needed to be secured, the key will created according to standards and will kept on the server side. Also hash map concept is used in this paper.

Kumar Verma, Ravindra Kumar Singh [21] discusses the performance analysis of RC6, Twofish and Rijndael block cipher algorithms on the basis of execution time and resource utilization. In this research paper RC6, Twofish and Rijndael block cipher algorithms were compared by using C# program. CPU utilization and memory utilization both are considered for determining resource utilization. A comparative analysis of RC6, Twofish & Rijndael is performed to provide some measurements on the encryption and decryption. Effects of several parameters such as number of rounds, block size and the length of secret key on the performance evaluation criteria are investigated. Result also concludes that performance of all these three algorithms is inversely proportional to keysize, if keysize will increase the performance will decrease and vice-versa.

Encryption of data prevents unauthorized users, including intruders breaking into a network, from viewing the sensitive data. As a result data keeps protected even in the incident that database is successfully attacked or stolen. Rama Roshan Ravan, Norbik Bashah Idris, Zahra Mehrabani [23] presents a variety of search methods in encrypted databases and documents and some examples are reviewed and evaluated. It is seen that the number of records, which is retrieved to respond to client's query in which it is often more than the records that have been requested. Therefore, after decrypting data in the client side, there is a need to perform queries in decrypted values for finding the results in which it forces computational overhead to the client, and also, the client should be able to work with relational values.

Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan[27] presents CryptDB, a system that explores an intermediate design point to provide confidentiality for applications that use database management systems (DBMSes). CryptDB's approach is to execute queries over encrypted data, and the key insight that makes it practical is that SQL uses a well-defined set of operators, each of which are able to support efficiently over encrypted data. CryptDB meets its goals using three ideas: running queries efficiently over encrypted data using a novel SQL-aware encryption strategy, dynamically adjusting the encryption level using onions of encryption to minimize the information revealed to the untrusted DBMS server, and chaining encryption keys to user passwords in a way that allows only authorized users to gain access to encrypted data.

3. Comparative Table

Paper	Algorithm	Performance	Result
[1] Query Processing Performance on Encrypted Databases by Using the REA Algorithm	Cryptographic support REA	The performance measure of query processing will be conducted in terms of query execution time.	The results of a set of experiments show the superiority of the REA over other encryption algorithm AES with regards to the query execution time. REA can reduce the cost time of the encryption/decryption operations and improve the performance
[2] Evaluating The Performance of	AES (Rijndael), DES, 3DES, RC2,	A comparison has been conducted for those	3DES still has low performance compared to algorithm DES. And RC2,

Symmetric Encryption Algorithms	Blowfish, and RC6	encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/ decryption speed.	has disadvantage over all other algorithms in terms of time consumption. Also AES has better performance than RC2, DES, and 3DES.
[3] Evaluating the Performance of Reverse Encryption Algorithm (REA) on the Databases	Cryptographic support, REA	The performance measure of query processing will be conducted in terms of query execution time.	The results of a set of experiments show the superiority of the REA over other encryption algorithm AES with regards to the query execution time. REA can reduce the cost time of the encryption/decryption operations and improve the performance
[4] Query Processing Performance and Searching over Encrypted Data by using an Efficient Algorithm	Ontology/ OBSERVER. XML data sources	Query processing problem on heterogeneous data sources. The research work presents a solution which improves not only the performance of searching but also quickly retrieves data as compared to the existing techniques.	The proposed algorithm efficiently eliminates the limitations of the existing techniques for fuzzy match and range queries.
[5] A critical overview of existing query processing systems over heterogeneous data sources	XQuery Based processing system, OBSERVER	Heterogeneity and physically separated of data sources are studied	Different approaches that treated the query processing problem on heterogeneous data sources
[7] Querying Encrypted Character Data in DAS Model	X	This paper presented techniques to support query over encrypted character data. For the most commonly used characters data type, double filtration method and positions encryption method are proposed.	The experiments results indicated that these methods avoid needless decryption and data transfer, which achieve better query performance and support fuzzy search efficiently
[9] Security Analysis of Reverse Encryption Algorithm for Databases	Reverse Encryption Algorithm (REA)	The encryption and decryption time results showed that the proposed encryption algorithm REA has a very good performance compared to other encryption algorithms.	The security (information entropy) results show that the proposed encryption algorithm REA and AES have a better secure than DES, 3DES, RC2, and Blowfish.
[14] A New Method of Query over Encrypted Data in Database using Hash Map	AES-256	Test query execution time through comparing two different query approaches. The first is to decrypt all encrypted character data before querying them. The second way, which is to decrypt the result records after filtering the records not related to querying conditions.	Good comparable response time, the performance of is better than the traditional way to query over encrypted data

4. Approach

When surveyed and studied the thirty four papers, it comes to conclusions that when we tried to encrypt database, there is a compromise between the degree of security provided by encryption and the efficient querying of the database, because the operations of encryption and decryption greatly degrade query performance. So our approach towards security and performance is by using REA algorithm along with RC6 algorithm because REA encryption algorithm provides maximum security and limits the added time cost for encryption and decryption so as to not degrade the performance of a database system. And the performance measure of query processing will be conducted in terms of query execution time.

5. Conclusion

The goal of this survey is to the query processing on encrypted database in order make understand a user convenience. We review the various papers for query processing over encrypted database and comparisons have been conducted for those encryption algorithm. The survey brings us the detail information of how the query processing performs on encrypted database by using various algorithms. Most of the researchers focused on the encryption of database by considering the time delay. Researches show that most current methods just provide equality query type on encrypted database, and time delay with cost. We have noticed that the encryption algorithm used by most of the researcher are REA which provides maximum security and limits the added time cost for encryption and decryption so as to not degrade the performance of a database system. Also table shows the comparisons among various papers related to algorithms and performance with result.

References

[1] Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie, Osama Faragallah, "Query Processing Performance on Encrypted Databases by Using the REA Algorithm", *International Journal of Network Security, Vol.14, No.5, PP.280-288, Sept. 2012*

[2] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", *International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010*

[3] Ayman Mousa, Osama Faragallah, Elsayed Nigm, and Elsayed Rabaie, "Evaluating the Performance of Reverse Encryption Algorithm (REA) on the Databases", *The International Arab Journal of Information Technology, Vol. 10, No. 6, November 2013*

[4] Manish Sharma Atul Chaudhary Santosh Kumar, "Query Processing Performance and Searching over Encrypted Data by using an Efficient Algorithm", *International Journal of Computer Applications (0975 – 8887) Volume 62– No.10, January 2013*

[5] Naoual MOUHNI, Abderrafiaa EL KALAY, "A CRITICAL OVERVIEW OF EXISTING QUERY PROCESSING SYSTEMS OVER HETEROGENEOUS DATA SOURCES", *Journal of Theoretical and Applied Information Technology*
20th February 2014. Vol. 60 No.2

[6] Arvind Arasu, Ken Eguro, Raghav Kaushik, Ravi Ramamurthy, "Querying Encrypted Data", *978-1-4673-4910-9/13/$31.00 © 2013 IEEE 1262 ICDE Conference 2013*

[7] Nian Liu, Yajian ZhOU, Xinxin Niu, Yixian Yang, "Querying Encrypted Character Data in DAS Model", *2010 International Conference on Networking and Digital Society*

[8] Lianzhong Liu and Jingfen Gai, "A Method of Query over Encrypted Data in Database", *2009 International Conference on Computer Engineering and Technology, 978-0-7695-3521-0/09 $25.00 © 2009 IEEE*

[9] Ayman Mousa, Osama S. Faragallah and S. EL-Rabaie, E. M. Nigm, "Security Analysis of Reverse Encryption Algorithm for Databases", *International Journal of Computer Applications (0975 – 8887) Volume 66– No.14, March 2013*

[10] Ling Feng, "Experimental Evaluation of Query Processing on Encrypted Telemedicine Data", *978-1-4244-9166-7/10 $26.00 2010 IEEE*

[11] Dongxi Liu Shenlu Wang, "Programmable Order-Preserving Secure Index for Encrypted Database Query", *2012 IEEE Fifth International Conference on Cloud Computing, 978-0-7695-4755-8/12 $26.00 © 2012 IEEE*

[12] Purushothama B R, B B Amberker, "Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation", *2012 International Symposium on Cloud and Services Computing, 978-0-7695-4931-6/12 $26.00 © 2012 IEEE*

[13] Dr.A.Venumadhav, "A Survey on Security of Data outsourcing in Cloud", *International Journal of Scientific and Research Publications, Volume 3, Issue 10, October 2013,ISSN 2250-3153*

[14] Mohammed Alhanjouri, Ayman M. Al Derawi, "A New Method of Query over Encrypted Data in Database using Hash Map", *International Journal of Computer Applications (0975 – 8887) Volume 41– No.4, March 2012*

[15] Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, "An improved RC6 algorithm with the same structure of encryption and decryption", *ISBN 978-89-5519-139-4 Feb. 15-18, 2009 ICACT 2009*

[16] Sheetal Charbathia and Sandeep Sharma, "A Comparative Study of Rivest Cipher Algorithms", *International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1831-1838*

[17] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, "The RC6 Block Cipher", *M.I.T. Laboratory for Computer Science, RSA Laboratories. August 1998*

[18] Stallings W., *Cryptography and Network security Principles and practice, Prentice Hill-2005*

[19] T.Gunasundari, Dr. K.Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms" *International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 2, February- 2014, pg. 78-83*

[20] Thenmozhi.C & Kishore Sonti, "*Analyzing the performance of RC6 using Complex Vedic Multiplier*"

[21] Harsh Kumar Verma, Ravindra Kumar Singh, "Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms", *International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012*

[22] Diaa Salama Abdul Minaam1, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" *International Journal of Network Security, Vol.11, No.2, PP.78*

[23] Rama Roshan Ravan, Norbik Bashah Idris, Zahra Mehrabani, "A Survey on Querying Encrypted Data for Database as a Service"

[24] "Database Security and Encryption a Survey Study"

[25] Stephen Tu M. Frans Kaashoek Samuel Madden Nickolai Zeldovich, "Processing Analytical Queries over Encrypted Data", *VLDB Endowment, Vol. 6, No. 5, 2013*

[26] Zheli Liu, Jingwei Li, Chunfu Jia, "Format-Preserving Encryption for Character Data", *JOURNAL OF NETWORKS, VOL. 7, NO. 8, AUGUST 2012*

[27] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing", *SOSP '11, October 23–26, 2011, Cascais, Portugal.*

[28] Narendra Chandel, Sanjay Mishra, Neetesh Gupta, Amit Sinhal, "Creation of Secure Cloud Environment using RC6", *2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 978-1-4799-0317-7/13/ 2013 IEEE*

[29] E. Surya C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", *ISSN:2249-5789, International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477*

[30] Milind Mathur, Ayush Kesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", *Proceedings of National Conference on New Horizons in IT - NCNHIT 2013, ISBN 978-93-82338-79-6*

[31] Ernesto Damiani, Sabrina De Capitani di Vimercati, Mario Finetti, "Implementation of a Storage Mechanism for Untrusted DBMSs"

[32] Michael L. Rupley, Jr., "Introduction to Query Processing and Optimization"

[33] Z. Wang, A. Tang and W. Wang, "Fast Query over Encrypted Data Based on b+ Tree", *International Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), 23-25 Oct. 2009.*

[34] P.Mohan Kumar, T.K.Das, DR.J.Vaideeswaran "Survey on Semantic Caching and query Processing in Databases", *Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013*

Author Profile

Rajendra Rathod received the B.E. degree in Computer Science and Engineering from Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Sant Gadge Baba University in 1994. Now pursuing M.E. from Prof.Ram Meghe Institute of Technology & Research, Badnera-Amravati, India. During 1996-2004, he stayed in the service of Lecturer at SHHJB Polytechnic, Chandwad, Nashik. He is now with Dr.Panjabrao Deshmukh Polytechnic, Amravati, India

Dr.C.A.Dhote is a Professor at Prof.Ram Meghe Institute of Technology & Research in Information Technology Dept., Badnera-Amravati. His educational qualification is M.S., Ph.D., having experience of more than 27 years in the teaching field.