Journal of Computer Sciences and Applications, 2015, Vol. 3, No. 6, 127-129
Available online at http://pubs.sciepub.com/jcsa/3/6/3

DOI:10.12691/jcsa-3-6-3

Significance of Processing Queries and Implementation of Cipher in Remote Location

Mishra Suchismita[1], Mishra Bibhuti Bhusan[2,*], Mishra Sambit Kumar[3]

[1]Full Time Research Scholar, Siksha O Anusandhan University, Bhubaneswar
[2]Asst. Professor, Siksha O Anusandhan University, Bhubaneswar
[3]Professor & Head, Department of Computer Sc.& Engg., G.I.E.T., Bhubaneswar
*Corresponding author: sambitmishra@gietbbsr.com

Abstract Confidentiality, Integrity and Availability are the three key attributes in preserving the essence of the data being used in remote exchanges between users & servers. Always there is need of maintaining a balance between the access and the protection of the system dealing with data. The encryption concept also proved as a powerful tool helps in enhancing the integrity of the remote data. The database server, clients and high speed Internet services are very much essential for processing data as well as optimizing queries in remote locations. Therefore security measures must be taken care, while processing private queries. It has been observed that cloud computing plays a vital role of preserving queries while processing and maintaining the privacy of data. In this paper, it is primarily focused regarding the security measures of data while processing queries in remote locations where the position of database server is not known and implementation of cipher in data transfer.

Keywords: *cipher, cloud computing, data abstraction, generalization, encryption, query term*

Cite This Article: Mishra Suchismita, Mishra Bibhuti Bhusan, and Mishra Sambit Kumar, "Significance of Processing Queries and Implementation of Cipher in Remote Location." *Journal of Computer Sciences and Applications*, vol. 3, no. 6 (2015): 127-129. doi: 10.12691/jcsa-3-6-3.

1. Introduction

Now a day's the cloud concept facilitates an alternative means of cheaper, faster and high-end computing power in the hands of the common man, resulting the significant increase in the cloud usage with ever increasing frequency of data access and usage through remote locations. Along with the benefits cloud computing also brings out certain concerns like the security and privacy issues associated with both the user as well as on the data. As the multiple devices and user platforms can have the simultaneous access to the cloud, and due to the lack of a concrete means of authentication, it becomes very difficult to manage the integrity of both user and the stored data. As it is obvious that high speed internet service, efficient server and client nodes as a part of cloud computing are essential for processing queries where the position of database server is not known. During this process, data is the separate and private asset of the database server and therefore it must be protected. While processing a user query, the vital information associated with the client nodes may be easily accessible and visible, so it should be protected in cloud and from other client nodes database servers. So, it is raised as one of the major problem in cloud computing as to protect both, the data privacy and the query privacy. In this case, possibly the vital information may be encrypted before sending to the destination resulting a challenge of tasks may have to base, while dealing with data utilisation services.

2. Review of Literature

People in the context of information security always strived for achieving a better balance between access and protection of the data in the systems, within their approaches various significant achievements are developed regarding the security and privacy issues are follows as

- Tingjian, Ge et.al [1] have focused in their paper user privacy and data privacy is considered together. They have also in their paper analyzed and discussed to enforce data privacy and user privacy over outsourced database service.
- Guo, Yubin et.al [2] have discussed in their paper the techniques to solve private processing of more specific queries. They have also implemented some techniques to public data column and private data column by applying hash (#) join. But join by hashing may not be able to retrieve other specific as well as relevant data columns.
- Jerry Kiernan et.al [3] has discussed in their paper that privacy of data owners and query users are defined as data privacy and user privacy respectively.
- Hu, Haibo et.al [4] have suggested in their paper that highly enhanced developing techniques may be used to improve the efficiency of query processing protocols.
- Kilzer et.al [5] have discussed in their paper about some significant advancement security. They have

used the access control mechanism along with differential privacy. They have worked upon mathematical bound potential privacy violation that prevents information leak beyond data provider's policy.

- Kraft, D.H. et.al [6] in their paper has defined a query as a combination from set of terms and set of Boolean operators. The query set may be defined as set of queries for documents, or the query processing mechanism by which documents can be evaluated in terms of their relevance to a given query.
- Feig M. et.al [7] in their paper have defined analytical query as a mathematical function that maps the readings of a group of atoms to a scalar, vector, a matrix, or a data cube. For the purpose of studying the statistical feature of the system, popular queries in this category generally include density, first-order statistics, second-order statistics, and histograms.
- Chapman A. et.al [8] have focused in their paper about kernel functionalities of DBMSs to meet challenges in scientific data management. It includes work that deals with query language, data storage, data compression, index design, I/O scheduling, and data provenance.
- In Amazon et.al [9] the implementation of VCL has been observed. Most of its characteristics and functionalities are desirable in a cloud. Practically it may have a large intersection with Amazon Elastic Cloud.

3. Problem Formulation

Usually, in a cloud computing environment, database server, client nodes as well as service provider with high speed internet connection are very much essential. Database server may have big data set, and may process the queries in the cloud. The data set may also contain some sensitive attributes that may need to be protected from the cloud. While on the other hand, the client fires queries retrieves the identifiers associated with the data. After the query processing, these identifiers may be used to retrieve data. The query may be needed to be protected against both the database server as well as the cloud.

A cipher may be termed as an algorithm for performing encryption or decryption to be followed as a procedure. For example if q which is a plain text may be required to be encrypted, then positioning the presence of q it may be encrypted as f(q) which equals to (q+t)/(position of q) where t may be the key applied in the function. Similarly while decrypting the function f(q) may be equal to (q-t)/(position of q). In this case q may also be termed as query or set of queries and f(q) may be termed as encrypted or decrypted index value associated with the key. The query users may need to query and exact data from cloud, but the query might disclose some sensitive information, behavior patterns of the user.

3.1. Goals for cipher

Every security system should have a number of security functions to assure the secrecy of the system. These functions are usually referred to as the goals of the security system like authentication, secrecy or confidentiality, integrity, as well as service reliability and availability.

3.2. Pseudocode-1 (Encryption mode)

```
cipher.init(Cipher.ENCRYPT_MODE, secKey);
String newtextFile = "newtext.txt";
String ciphergeneratedtextFile
= "ciphertextSymm.txt";
InputfileSt = new InputfileSt(newtextFile);
OutputfileSt= new OutputfileSt(newtextFile);
CiphergeneratedStream
= new CiphergeneratedStream(OutputfileSt,
cipher);
byte[] block = new byte[8];
int i;
while ((i = InputfileSt.read(block)) != -1) {
cos.write(block, 0, i);
}
String cleartextAgainFile
= "cleartextAgainSymm.txt";
```

3.3. Pseudocode-2 (Decryption mode)

```
cipher.init(Cipher.DECRYPT_MODE, secKey);
fis = new InputfileSt(ciphertextFile);
InputcipherSt = new InputcipherSt(fis, cipher);
fos = new OutputfileSt(cleartext);
while ((i = cis.read(block)) != -1) {
fos.write(block, 0, i);
}
```

3.4. Performance Evaluation Methodology

It defines the mechanisms to evaluate the performance of the cipher.

The experiments have been already conducted. The simulation program is compiled using the default settings in .NET 2003. It has been observed that to evaluate the performance of the cipher the parameters associated with the cipher should be determined, and also it is dependent on mechanism to encrypt or decrypt the data blocks.

It has been experimented by having key size 64 bits, 192 bits and the block size with 64 bits and 128 bits along with 20527 and 45911 input size.

Since the security features of each algorithm as their strength against cryptographic attacks is already known and discussed. The chosen factor here to determine the performance is the algorithm's speed to encrypt/decrypt data blocks of various sizes.

While simulating it may accept three inputs, i.e. algorithm, Cipher Mode and data block size. After a successful execution, the data generated, encrypted, and decrypted may be represented. It has been observed that most of the characters may not appear since they may not have character representation. After successful encryption/decryption process it may be assured that all the data are processed in the right way by comparing the generated data.

It is observed that either to outsource data or to make privacy on reserved or personal data, solutions associated with the appropriate queries may be achieved along with secure traversal framework and encryption scheme. The framework may be scalable to the large datasets. By

analyzing the performance of large data sets associated with the framework it is seen that that computation time as well as the query response time are interdependent with different types of queries.

4. Conclusion

Apart from this security and privacy issue regarding the data and the queries, the research is being ongoing on Cloud computing concepts like virtualization, distributed computing, utility computing etc. This implies flexibility, on the demand services as well as reduced information technology overhead for the end-user computing systems. Along with the assumption of relevant set of queries along with the query terms, also the non query terms associated with the set of queries have been investigated. It has been observed that the finding of the optimal range of non query terms associated with the set of queries may be more difficult to accomplish rather than for query terms associated with the set of queries.

Related Work

The application of the data abstraction mechanism, which is seen as a generalisation principle may be used for preserving the data and maintaining the privacy of the usage. Regarding the privacy of the user data there are many solutions available, out of which encryption may be a feasible solution for the remote security. As the nature implies that the data inconsistency, redundancy and misuse in the cloud is quite possible. It has been suggested for implementation of encryption mechanisms on data with heterogeneity is also required. It is understood that the aggregate functions on various data may be rewritten and processed in encrypted form so that the protection level may be enhanced in the remote processing. While implementing the retrieval mechanism, the conditions associated with the queries may be masked to provide the enhanced privacy and confidentiality.

References

[1] TingjianGe, Stanley B. Zdonik, and Stanley B. Zdonik. Answering aggregation queries in a secure system model. In VLDB, pages 519-530, 2007.

[2] Guo, Yubin, et al. "A solution for privacy- preserving data manipulation and query on nosql database." Journal of Computers 8.6 (2013): 1427-1432.

[3] Jerry Kiernan, RakeshAgrawal, RamakrishnanSrikant, and YirongXu. Order preserving encryption for numeric data. In Proceedings of the 2004 ACM SIGMOD international conference on Management of data, SIGMOD' 04, pages 563-574, New York, NY, USA, 2004. ACM.

[4] Hu, Haibo, "Processing private queries over untrusted data cloud through privacy homomorphism." Data Engineering (ICDE), 2011 IEEE 27th International Conference on. IEEE, 2011.

[5] Kilzer, Ann, Emmett Witchel, Indrajit Roy, Vitaly Shmatikov, and Srinath T.V. Setty. "Airavat: Security and Privacy for Map Reduce."

[6] Kraft, D.H., Bordogna, G., and Pasi, G.: Fuzzy Set Techniques in Information Retrieval, in Bezdek, J.C., Didier, D. and Prade, H. (eds.), Fuzzy Sets in Approximate Reasoning and Information Systems, vol. 3, The Handbook of Fuzzy Sets Series, Norwell, MA: Kluwer Academic Publishers, 1999.

[7] Feig M, Abdullah M, Johnsson L, Pettitt BM (1999) Large scale distributed data repository: design of a molecular dynamics trajectory database. Future Generation Computer Syst16 (1):101-110.

[8] Chapman A, Jagadish HV, Ramanan P (2008) efficient provenance storage. In: SIGMOD Conference. ACM, Vancouver, BC, Canada. pp 993-1006.

[9] Amazon Elastic Compute Cloud (EC2): http://www.amazon.com/gp/browse.html? Node=201590011, accessed Dec 2008.