A NEW TWO-CLOUD SAFE SERVER FOR SQL COLLECTION NUMERIC QUERIES WITH PRIVACY PROTECTION

Dr. T.K. SHAIK SHAVALI
Professor
Department of Computer Science and Engineering,
Lords Institute of Engineering and Technology
Hyderabad,India

Mr. G.KUMAR
Asst Professor
Department of Computer Science and Engineering,
Lords Institute of Engineering and Technology
Hyderabad,India

Mr.SHAIK MAHEBOOB
Asst Professor
Department of Computer Science and Engineering,
Lords Institute of Engineering and Technology
Hyderabad,India

Abstract

Inside the present scenario companies and people are outsourcing database to perform useful administrations and minimum attempt packages. these are buried inside the cloud server, that is out of doors the ability to control of the records proprietor. The sq. Queries require a few comfortable database schemes for its simple working, but this at lengthy closing prompts privacy spillage to the cloud server. For numerical variety inquiry (>,< , and so forth.) these forget to provide ok protection insurance. A portion of the difficulties faced are privacy leakage of statistical attributes, get right of entry to patterns and so on. Likewise, increased number of queries will launch greater statistics to the cloud server. consequently, regarding these issues severa works had been accomplished with the aid of numerous researchers. we've got studied some of these studies works and analyzed the best possible methods to come back to the preferred level of privateness renovation inside the case of cloud computing. some of the works studied are the fuzzy good judgment, range queries, CryptDB order maintaining encryption and multi-cloud structure.

Keywords *— cloud computing, database, privacy preserving, range query*

1. Introduction

within the present occasions as it could be seen cloud has taken the control over the IT commercial enterprise with its innumerable advantages. It holds the opportunity to exchange an intensive section of the IT enterprise, making software significantly greater appealing as an service. Cloud computing [1] is alluded to as SaaS (software as a carrier) because it renders the packages as administrations over the net and the hardware and structures software program in the records centres that offer the ones administrations. The hardware of statistics centre and software program is referred to as a cloud today the clouds can be open/public and further non-public. non-public clouds are related to the internal datacenters of a enterprise or different association, not made available to the general public. Cloud computing in this way can be compressed as a mix of saas and application computing, booting out the records centre (little + medium expected). protection is the chief issue of the cloud computing. Cloud clients confront safety dangers each from outdoor and inside the cloud. protective the facts from the server itself is the pro of the main problems associated with it. The server will with the aid of definition manipulate the "bottom layer" of the product stack, which accurately goes around most recognised

security techniques. As said the cloud server is prevalent as semi-depended on (sincere-but-curious). CryptDB [5], a framework that gives confidentiality to programs that make use of database management frameworks (DBMSes). CryptDB permits to perform queries over encrypted records, likewise the sq.'s very tons characterized set of operators, and queries over encrypted data. CryptDB tends to the danger of an inquisitive database administrator (DBA) who endeavors to examine private facts (e.g., fitness books, monetary articulations, individual facts) by preserving an eye fixed on the DBMS server by keeping the DBA from getting to know personal records. It makes use of a few devices to perform this safety functionality. one of the devices being the Order retaining encryption (OPE) [11, 12] is normally applied as part of databases to manner sq. Questions over encrypted records. It allows to carry out order operations on ciphertext just like the plaintext for e.g. statistics server can fabricate index carry out variety queries [10] and type the encrypted records just like the plaintext. no matter going to the security cause well, regardless of everything it uncovers the order of the ciphertext. consequently, the goal of security protection of the outsourced information to a cloud server is delicate by means of partitioning the touchy information into elements and shop them in non-colluding clouds.

moreover, a comfortable database provider architecture is mentioned by way of utilizing non-colluding clouds wherein the records getting to know and question intent is split into two clouds. Henceforth, perceiving just a single cloud can not help uncovering non-public data. apart from a progression of intersection protocols to offer numeric-associated sq. variety queries [1] with privacy renovation is additionally performed and it won't uncover order related data to any of the two non-colluding clouds.

2. System Architecture

Our proposed secure database gadget consists of a database administrator, and two non-colluding clouds. on this model, the database administrator may be applied on a patron's aspect from the attitude of cloud service. the two clouds (consult with Cloud A and Cloud B), because the server's side, provide the storage and the computation service. It briefly depicts the architecture of our outsourced cozy database machine in our scheme. the 2 clouds work collectively to respond every query request from the purchaser/legal users (availability). For privateness issues, those clouds are assumed to be non-colluding with every different, and they may comply with the intersection protocols to preserve privacy of records and queries (privacy). In our scheme, the know-how of stored database and queries is partitioned into parts, respectively saved in one cloud. The mechanism guarantees that knowing both of those elements cannot obtain any beneficial privacy records.

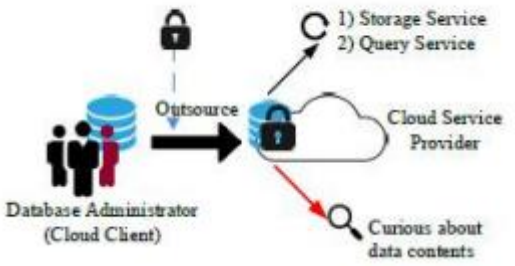

Figure 1. Outsource Database and Services

As shown in to behavior a cozy database, records are encrypted and outsourced to be stored in a single cloud (Cloud A), and the private keys are stored inside the different one (Cloud B). For each query, the corresponding understanding consists of the data contents and the relative processing good judgment. We make use of a prototype of know-how partition, dividing application logic into two components, which is bristly proposed with the aid of Bohli et al. In [16]. The utility good judgment, as a mystery knowledge, is partitioned into components, every of which is handiest known to at least one cloud. This prototype. Intuitively, this -cloud structure

increases some complexity to a degree, and we are able to examine and point out that this overhead is acceptable.

3. Related Work

This Paper analyzes current studies associated with unmarried or multiple cloud safety and addresses viable solutions. studies on using multi-cloud providers to keep safety has been found to acquire much less interest from the studies community than the usage of individual clouds. This paintings aims to promote the usage of more than one clouds way to its capacity to reduce safety dangers affecting the person of cloud computing. We gift new preprocessing techniques that allow obtaining interactive question times in huge text collections (100 GB of text, served with the aid of a unmarried system). recollect two similarity measures, one in which the query phrases coincide with similar terms in the collection (for instance algorithm of set of rules suits or vice versa) and one wherein the question terms coincide with phrases with a similar prefix inside the series (as an example, Alori corresponds to the set of rules). The latter is vital when we need to show the results right away after each keystroke (search even as writing). all the algorithms had been completely integrated into the complete search engine.

on this Paper, we define and remedy the look for key phrases categorised as effective but protected on statistics encrypted inside the cloud. We use order retaining symmetric encryption to shield records within the cloud. even though many research techniques are available, they do not offer green search consequences. for example, the hunt results generated 40 records and in the ones 30 data are relevant and the last 10 information generate inappropriate information. This paper focuses mainly on research strategies as a way to improve the effectiveness of studies. We use search methods primarily based on keywords and concepts to retrieve relevant search standards. This method will repair files primarily based on broader conceptual entities, so as to enhance the performance of the quest .

4. 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 expose the private statistics of facts contents, such homes themselves are already sensitive and private for the consumer. Order retaining Encryption(OPE), that is extensively used in building the relaxed database, with assist of range queries, immediately exposes the statistical statistics within the encryption field. moreover, the leakage of statistic homes is part of the nature of outsourced cloud database service: the cloud can examine the statistical homes (like order) via repeated question requests. as an example, It describes such an attack: After easy queries over one same column, the order relationship of some records in positive column can be decided. There also are some different direct and indirect situations to leak statistical homes. in this way, even though the order assets isn't always exposed to the semi-depended on cloud at the beginning, the cloud can regularly discover the order facts after many question 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.

5. Conclusion

on this paper, we offered a -cloud architecture with an intersection for outsourced database service, which guarantees the privateness renovation of information contents and sq. range query sample. at the identical time, with the support of range queries, it not best protects the confidentiality of static records, however additionally addresses ability privateness leakage in statistical houses or after large quantity of query approaches. safety evaluation shows that our scheme can meet the privateness protection necessities. moreover, overall performance evaluation result shows that our proposed structure are efficient. To achieve the assurances of cloud statistics integrity and availability and put in force the great of dependable cloud storage service for users, we endorse an powerful and flexible dispensed scheme with explicit dynamic statistics guide, which includes block replace, delete, and append. we depend on erasure-correcting code in the document distribution preparation to offer redundancy parity vectors and assure the facts dependability.

References

[1] *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, 2012, pp. 5490–5499.*

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

[3] *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.*

[4] *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.*

[5] *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, 2004, pp.563–574.*

[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.