ISSN 2278-3091
Volume 8, No.3, May - June 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse82832019.pdf
https://doi.org/10.30534/ijatcse/2019/82832019

Secure *k-NN* query on encrypted cloud data with multiple keys

Bulusu Rama[1*], K Sai Prasad [2], P Sreeja[3]
[1] Department Of Computer Science, MLR Institute Of Technology, Hyderabad, India
Bulusurama1967@gmail.com
[2] Department Of Computer Science, MLR Institute Of Technology, Hyderabad, India
Saiprasad.kashi@gmail.com
[3]Department Of Computer Science, MLR Institute Of Technology, Hyderabad, India
Sreeja.poka@gmail.com

ABSTRACT

The K-nearest neighbors (k-NN) query is a core relating for occupying space and being using many channel for communication in the database. It has large-scale of appeal in the location-based utility, grouping and collection and soon. With the assurance of confidentiality and solitude, enormous amount of facts are growing and service are being obtained in a contract way from various suppliers in a formation of code. Which will leads to favorable being fit in the cloud system. Freshly, numerous strategies are kept forward to transfer the converted facts. Yet previous work expect that where all the clients are completely believed that they are going to get the uni facts with the key, where it is used to convert the facts and make it available for the clients to get it. This way of transfer of facts seems to be impracticable where many clients are not truthful nor significant in using the key, in this issue we prefer paperback logic for it, data owner and query user has it assess and identical keys, and they don't share it with one-other meantime, the DO convert and make outsourced data using it with their own key. Our logic is created and a set of rules are fixed in order to provide and safeguard the facts and issue seclusion and it will carry downloaded facts, in regarding of safety and production.

Key words: Cloud Computing, Data Integrity, Data Sharing, Key-Aggregate.

1. INTRODUCTION

Recently cloud computing has turn out to be an more popular carrier for its flexibility which will drive numerous agencies establishments with the favor of many groups. Need to contract fact offerings on the platform in a equal schedule more interest which is being invested in order to increase the level of unique certainty and seclusion troubles in contract cloud and it is defend facts confidentiality and statistics proprietor in order encrypt the touchy records of contract facts which include degree of fitness statistics private photos earlier than related sets and transfer to cloud platform on the opposite way information proprietor additionally proposal to reckon on the cloud platform for processing the data facts saved in it and also retention and control will be performed. Massive quantities of relaxed logic were being provided to guide over the records which are encrypted. The basic functionality in relating and multimedia facts. It goals at establishment of handy points given by the question factor from the bygone year fact finding has suggested to diverse the techniques in order to deal with the safety and solitude problems on encrypted statistics acts. The preferred method to convert the information earlier than contract where complicates collection i.e. encryption and decryption need to be done in a short Spain of time duration before processed enactment. We take up an example the effort proposes a uneven where it has only magnitude retaining it holds the question from the quantity having direction as well as magnitude of certain distance as a substitute of discovery genuine accessible next permit of cloud celebration roughly its primarily found a set of rules. All suggest hardback treaty an encrypted record primarily based on some model for occurrence, every aspect need clinical records for a sickness categorization examine or a provider accessible to medical doctor. Thus docs can seek the k-NN occurrence with a few comparable biological records to assist deal with sufferers. Encryption and decryption will be done by the doctors based on index which is being provided by the keys. With the help of multiple key we try to provide certainty to the facts which are present in the cloud. With the key sharing way to nevertheless a long way from being sensible in most instance.

1. It has availability for convert and make outsourced facts, based on this we have several issues in the real work.

2. There are some native rules are being introduced for note worthy benefaction on our handout in this paper.

2. RELATED WORK

Here our fulfill duties are an exception sort of uncertainty action on converted facts, it has acquired expected amount of pivot. Lately, mostly when it comes to the using of the internet it depends on the servers and process the facts in the cloud, where the data owner does not want to outsource the facts. Current action essentially examine the patronage facet, Conventional SQL query will find for query scale. Here in this segment we mostly analysis in contemporary attainment in it. Where preceding action, unspecified logic is being suggested in order to resolve issues related to it. Mostly cloud data is being categorized in multiple groups depends on client will be able to split the key and logic to remain the logic in private.

2.1 Annular Scale Seek On Encrypted Relating Records

Searchable encryption is one of the most important and frequently used search effect, which will give the convince for the client to search a particular word easily. Here it will also safeguard the facts from unauthorized individuals every operation will be done by using SQL queries, where based on the request from the client the query will processed and most of the facts gathering is done on SQL. Circular range search is most widely used and it gives us the accurate result depends on the client requirements. Searching process will be done based on location of the particular word, in order to overcome the drawback we have introduced two novel similar keys for supporting circular range search. Our logic can easily find whether the points inside a circle on converted facts without showing the facts security, for the cloud server it is of semi-honest we have defined some rules to protect the present logic and we need to manifest that our facts are safe from un-trusted attacks. Where many experiments are being done on the real time platform in this case we briefly explain about searching process in a secure circular effect. We present a hardback logic to carry circular effect search on converted spatial facts.

1. Scheming round effect searchable converted can be attain by the faster-than-linear search with the contemplate with the fact evidence.

2. Here we also enhance the information in order to get the clearness for common geometric queries.

2.2 Secure k-NN Schemes with Key Sharing

To conquer fault of indispensable spilt logic with this firm logic where indispensable kept in secret. Action are performed with similar logic and confidential trace will change the key, issue will not give the key, alternatively interchange of facts. Where owner require question mark conversion without the uncertainty that signify it endure in online for all the clients. Logic will carry the offline facts also. Although, with the performed actions where every key coincide same code behind the main scheme of the key sharing is to only provide the unci facts to the clients by using this methodology. Nevertheless it acts depends on trusted client.

3. PREPARATORY

Here in this part, we mainly initiate essentially opening conception, such that k-d tree. In the liberal arts it shows the fundamentals of it and the logic which facility the source of information.

3.1 K-d Tree

K-d tree which is mainly useful for finding the margin separation it gives us the format of arranging points in a k-extent capacity. It will make our more easy in the process of searching a particular item. Which is in the binary form where every node is a k-dimensional point, here non-leaf node can view and absolutely create a gap between the two points. Certainly it uses the divide and conquer plan in order to spilt it in many segments.

4. SYSTEM ARCHITECTURE AND DESIGN GOAL

Here, we put it short extent of the construction of the stable K-NN structure and delineation the ultimatum copy and sketch aim.

4.1 System Architecture

Our structure it largely had of wet type of entities: we have they are key generation center and

KGC: This is super user of the application where he can login into the application with standard user name and password and give permission to user and owner to access their application.

CP: In this module cloud platform can login as standard user name and password after login as cloud platform can check the user queries and send request to CSP to cross check the keys and get the result and send to user.

CSP: Where it provides the services for the client based on the issues related to the facts. This process will be happened in a security way.

DO: Where DO has the capability to get the key and decode the information QU, where QU has the possibility to request the query from the cp it can give us the key related to the related to the content with the help of that we can decode the facts. Only the client who has consent they are allowed to retrieve the information and it is easy for access control to execute competently in our structure. The only logic behind the structure is to make the client authenticity, where only trusted client are allowed to get the facts. In other way the client who have proceed authentication steps are allowed to access the structure, yet we have many issues related to the authentication where the attacker will try to fetch the facts. In this case we introduced a way that is traditional single cloud platform. The main aim of this logic to provide the security to the facts. The initial thing that the client needs to do is to decode the information from the cloud platform.

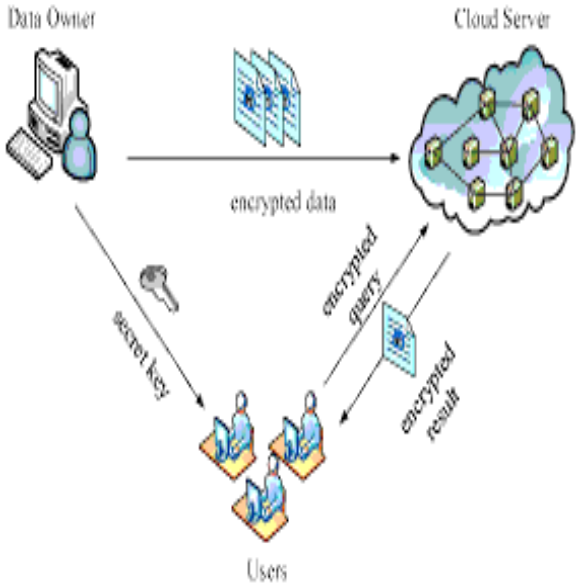

Figure 1: System Architecture

5. PROPOSED SYSTEM

When we view overhead of the troubles the awareness that we have obtained without k-NN query on encrypted data without any of the key establishment. When we spread the two trapdoors public key cryptosystem we construct deposit treaty at ease of multiple birthday celebration computation that could pre-owned us sub exercises offer logic.

Here we recommend singular comfortable k-NN logic with multiple key in order to cope the issues where here many query has its own encrypt and decrypt key are available which they doesn't share it with query user here we are considering a simple logic where celebration of two birthday parties, where we analyze the every aspect of the issue.

1. To our facts the primary painting research released k-NN query on encrypt information with two-keys. Where our logic is most effective and will not be safeguard the confidentiality and safeguard the confidentiality and seclusion to the information proprietor, with the key it will completely resolve issued caused with the aid of customer.

2. The existing fixed treaty we try to assemble secure k-NN logic with two-keys. We present realistic relevant blend via good sized demonstration to use the actual data item.

5.1 Algorithm used in Project

This is the algorithm which has being used to built in this project.

Algorithm 1 SecDist$([p_i]_{pk_o}, [q]_{pk_u}) \rightarrow [\|p_i - q\|^2]_{pk}$

Require: CP has $([p_i]_{pk_o}, [q]_{pk_u}), SK^{(1)}, pk, pk_u, pk_o$;
CSP has $SK^{(2)}, pk$.

1. CP:
   (a) Choose random $r_1, r_2 \in \mathbb{Z}_N (r_1 \neq r_2)$, compute $R = r_1 - r_2$.
   (b) $X \leftarrow [p_{i,1}]_{pk_o} \cdot [r_1]_{pk_o}, Y \leftarrow [q_1]_{pk_u} \cdot [r_2]_{pk_u}$, $X_1 \leftarrow \mathbf{PDO}_{SK^{(1)}}(X), Y_1 \leftarrow \mathbf{PDO}_{SK^{(1)}}(Y)$.
   (c) Send X, X_1, Y, Y_1 to CSP.
2. CSP:
   (a) $X_2 \leftarrow \mathbf{PDT}_{SK^{(2)}}(X_1, X), Y_2 \leftarrow \mathbf{PDT}_{SK^{(2)}}(Y_1, Y)$.
   (b) $S_1 \leftarrow [X_2 - Y_2]_{pk}, S_2 \leftarrow [(X_2 - Y_2)^2]_{pk}$.
   (c) Send S_1, S_2 to CP.
3. CP:
   (a) $S_3 \leftarrow S_1 \cdot [R]_{pk}^{N-1}$.
   (b) $Z_1 \leftarrow S_2 \cdot S_3^{N-2R} \cdot [R^2]_{pk}^{N-1} = [(p_{i,1} - q_1)^2]_{pk}$.
4. CP and CSP:
   (a) Repeat Step 1 – Step 3 to calculate $Z_2 = [(p_{i,2} - q_2)^2]_{pk}, \ldots, Z_m$.
5. CP:
   (a) $[\|p_i - q\|^2]_{pk} \leftarrow \prod_{j=1}^{m} Z_j$.

Algorithm 2 SecMin$(([a_i]_{pk}, [i]_{pk}), ([a_j]_{pk}, [j]_{pk})) \rightarrow ([min(a_i, a_j)]_{pk}, [l_{min(a_i,a_j)}]_{pk})$

Require: CP has $([a_i]_{pk}, [i]_{pk}), ([a_j]_{pk}, [j]_{pk}), SK^{(1)}, pk$; CSP has $SK^{(2)}, pk$.

1. CP:
   (a) Flip a coin s randomly(i.e. $s = 1$ or $s = 0$).
   (b) **if** $s = 1$ **then**
   $[l]_{pk} = [a_i]_{pk} \cdot [a_j]_{pk}^{N-1}$
   else
   $[l]_{pk} = [a_j]_{pk} \cdot [a_i]_{pk}^{N-1}$
   end if
   (c) Chooses a random number r, s.t. $\mathcal{L}(r) < \mathcal{L}(N)/4$, $X = [l]_{pk}^{r} = [r \cdot l]_{pk}, X_1 = \mathbf{PDO}_{SK^{(1)}}(X)$.
   (d) Send X, X_1 to CSP.
2. CSP:
   (a) $X_2 \leftarrow \mathbf{PDT}_{SK^{(2)}}(X_1, X)$.
   (b) **if** $\mathcal{L}(X_2) > \mathcal{L}(N)/2$ **then**
   $u = 1$
   else
   $u = 0$
   end if
   (c) Encrypt u with pk and send $[u]_{pk}$ to CP.
3. CP:
   (a) **if** $s = 1$ **then**
   $[u^*]_{pk} = [u]_{pk}$
   else
   $[u^*]_{pk} = [1]_{pk} \cdot [u]_{pk}^{N-1} = [1 - u]_{pk}$
   end if
   (b) Choose random $r_1, r_2 \in \mathbb{Z}_N$.
   (c) $Y = [u^*]_{pk} \cdot [r_1]_{pk}, T = [a_i]_{pk} \cdot [a_j]_{N-1}^{pk} \cdot [r_2]_{pk}$, $Y_1 \leftarrow \mathbf{PDO}_{SK^{(1)}}(Y), T_1 \leftarrow \mathbf{PDO}_{SK^{(1)}}(T)$.
   (d) Send Y, Y_1, T, T_1 to CSP.
4. CSP:
   (a) $Y_2 \leftarrow \mathbf{PDT}_{SK^{(2)}}(Y_1, Y), T_2 \leftarrow \mathbf{PDT}_{SK^{(2)}}(T_1, T)$.
   (b) $S \leftarrow Y_2 \cdot T_2$.
   (c) Send $[S]_{pk}$ to CP.
5. CP:
   (a) $S_1 \leftarrow [S]_{pk} \cdot ([a_i]_{pk} \cdot [a_j]_{pk}^{N-1})^{N-r_1} \cdot [u^*]_{pk}^{N-r_2} \cdot [r_1 - r_2]_{pk}^{N-1} = [u^* \cdot (a_i - a_j)]_{pk}$.
   (b) $[min(a_i, a_j)]_{pk} \leftarrow [a_j]_{pk} \cdot S_1 = [a_j + u^* \cdot (a_i - a_j)]_{pk}$.
6. CP and CSP:
   (a) Calculate $[l_{min(a_i,a_j)}]_{pk} = [j + u^* \cdot (i - j)]_{pk}$ refer to Step 3(b) – Step 5.

5.2 Scalability

In this section, here we additionally investigate the consequence and we try to find the client who is having effective ability in order to get the content from the cloud. The basic logic behind this quantity of the clients will determine the issues on consistence. When the quantity of issues related to clients changes then the production of issues of value of m reaction interval is almost depends on client issues. Become different from to for meanwhile the query reaction. Interval grow linearly it is prominent than from a longer time multithread programming capability is being used in order to upgrade the query effectiveness in language protocol the scheme is that every client will have computing power in CPU, to raise the consistency of it we need to enlarge the CPU time interval. When consistency is under a definite portal. Formerly it will enlarge the coincident explorer source the delaying of CPU came with around an enlargement of query reaction interval. It is foremost to know the consistency and the performance of the CPU appliance, some software framework will supply a substructure to enhance consistency to allocate the amount of work done into a dump of computers, such application are behind the extent of this action.

As specified in advance high production can be attain with the most effective way. To stimulate the assert we appliance a contrast of query retaliation time between fundamental and most effective logic, which has optimum ability. Here every query has its own immensity the device may be prolonged to combine the changes accomplished inside the present application to improve the high quality for the future works this is to be performed on the software.

5.3 Further Discussion

In above, state test we centre on the assessment of computation price and transmission price. Where the computations price will be controlled and transmission price is unmanageable. We can also admit it will render prolonged plan to accomplish the issues empirical cloud domain. The transmission where it is state of existing is the centre for additional action.

A straightforward instance is being explained, we have the horizontal line and a vertical line in it. Where the points are divided into subsets it with equal number of elements of set and a horizontal will break the occurring subset in more distant way, where the image is being split into seven equal parts.

6. CONCLUSION

The main idea that we want to share is that we have actually targeted on endless complication of reinforce the K-nearest neighbors suspicion a top convert threat facts. Where an individual is accountable for a fact assert, where the facts cannot be issued to the query client. So that developer had introduced a latest technique where with the help of the multiple keys we can break the pivotal allocation query completely. Where the model is at edge, developer ceaselessly in the form of twin-cloud. We have displayed a conceptual survey where our model can save the facts are kept in secret and questions are kept in isolation. Eventually large no of experimental assessment has being done and we have given the practical exhibition and explanation of the potency and the capacity to be changed in the model. In the mean time we try increase our action, in order to carry the facts retrieving assignment like to categorizing and with the same computation.

REFERENCES

1. Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, "De-duplication on encrypted big data in cloud," IEEE Transactions on Big Data, vol. 2, no. 2, pp. 138–150, 2016.
https://doi.org/10.1109/TBDATA.2016.2587659
2. S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat DDOS attacks in clouds?" IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245–2254, Sept 2014.
https://doi.org/10.1109/TPDS.2013.181
3. S. Yu, S. Guo, and I. St Ojmenovic, "Can we beat legitimate cyber behavior mimicking attacks from botnets?" in 2012 Proceedings IEEE INFOCOM, March 2012, pp. 2851–2855.
4. M. Li, S. Yu, W. Lou, and Y. T. Hou, "Toward privacy-assured cloud data services with flexible search functionalities," in 2012 32nd International Conference on Distributed Computing Systems Workshops. IEEE, 2012, pp. 466–470.
5. H. Cui, X. Yuan, and C. Wang, "Harnessing encrypted data in cloud for secure and efficient image sharing from mobile devices," in 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015, pp. 2659–2667.
https://doi.org/10.1109/INFOCOM.2015.7218657
6. N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy preserving query over encrypted graph-structured data in cloud computing," in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 393–402.
https://doi.org/10.1109/ICDCS.2011.84
7. E. Kabir, A. Mahmood, H. Wang, and A. Mustafa, "Micro aggregation sorting framework for k-anonymity statistical disclosure control in cloud computing," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2015.
https://doi.org/10.1109/TCC.2015.2469649