International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-8, Issue-12)

Research Article | **December 2018**

High Reliable Spatial Query Processing Using Secure RC5 Algorithm

Nagamalleswararao T*
Department of Computer Science,
Programmer Analyst,
Trans IT Mpower Labs Pvt. Ltd

Kumaraswamy G
Asst.Professor,
Department of CSE
GITAM Institute of Technology

Abstract—Cloud computing data is stored over the distributed servers, which can be accessed with the help of user queries. In cloud computing, millions of user queries are processed by distributed server with less latency, high availability and high reliability. However, providing confidentiality user queries is still a challenging task due to the high vulnerability exist in the cloud environment. The existing mechanisms suffer from high computational and communication overhead, in addition to vulnerabilities still exists in their security mechanisms. In our proposed approach, any user send the spatial queries to the service provider, then the service provider use these spatial queries to check on the spatial encrypted data. User uses the RC5 key to decrypt the response messages. In this entire process, users is able to protect the data from the data leakage, reduces the communication overhead when compared with other existing mechanisms.

Index Keywords— Encryption Key, Service Provider, User Query, and Decryption.

I. INTRODUCTION

Data owner of the special data needs huge number of computational and storage resources when data owner provides the special data as a service, this is not a practical approach for every data owner. Solution for this problem is to deploy special data in the cloud environment, which is cost effective approach for every Data owner [1-5]. Spatial data outsourcing is an emerging area over the cloud computing. Even cloud computing is cost effective approach, some security challenges also need to be addressed to protect the spatial data from the attackers. The main challenges are preventing data leakage; need to have trust on cloud service provider, and blocking unauthorized access [6-10]. To handle the above challenges, data owner need to provide confidentiality, integrity and availability in outsourced information.

Spatial data refers to all types of data objects or elements that are present in a geographical space or horizon. It enables the global finding and locating of individuals or devices anywhere in the world [10-15]. Spatial data is also known as geospatial data, spatial information or geographic information.

A Hilbert curve (also known as a Hilbert space-filling curve) is a continuous fractal space-filling curve first described by the German mathematician David Hilbert in 1891,as a variant of the space-filling Peano curves discovered by Giuseppe Peano in 1890.

Because it is space-filling, its Hausdorff dimension is (precisely, its image is the unit square, whose dimension is 2 in any definition of dimension; its graph is a compact set Homomorphic to the closed unit interval, with Hausdorff dimension 2) In our proposed approach secure query processing is done among three modules such as Authenticated User (AU), Service Provider (SP) and Data Owner (DO). Our main objective is to secure the communication and maintain minimum the computational and communication overhead.

II. PROPOSED SYSTEM

To provide high security for spatial query processing in cloud computing with minimum computation and communication overhead, the existing mechanisms are inadequate, to overcome this problem we have developed a spatial query processing by Hilbert spatial curve with lightweight encryption algorithm. In our proposed approach secure query processing is done among three modules such as Authenticated User (AU), Service Provider (SP) and Data Owner (DO).

Data Owner provides query processing access rights to all authenticated users through the service provider. Data owner uses Hilbert spatial curve to represent the spatial data, in this approach data owner calculates the cell index and its corresponding data points of spatial data by using Hilbert spatial curve. Here, both index and data points are encrypted before it send to the SP, these encrypted values also shared with AU. DO uses RC5 encryption algorithm to encrypt the index and data points of Hilbert packet list, this process reduces the computational overhead at data owner side and protects the data leakage to SP and unauthorized users.

SP has a list of AUs which are authenticated by DO, with that SP provides spatial query service to all authenticated users. In addition to that, SP only stores the encrypted spatial data and it doesn't have permission to decrypt the data. Initially, it receives the encrypted data from the DO before it provides the service to any AU.

AU initially receives the index information about spatial query, use this information to generate request query and send this query to SP. Upon receiving this query, SP checks the user request is authenticated or not by verifying the current available AU list. If the user is a valid then the user query is processed on encrypted spatial data. Based on the acquired results, SP sends encrypted spatial data as a reply message to user. When user receives encrypted reply from SP, user decrypts the reply by using secret RC5 key which is known to DO and AU.

A. Secure Spatial Query Processing Using Hilbert Packet List Algorithm

Spatial query Input:

User's Authentication key, U_{Ki}

Spatial Data Points, $D = (d_1,.....,d_s)$

Packet Size, P_s

RC5 Encryption Key-K

Hilbert Packet List = $(P_1,…….,P_p)$, where $P_i = [P_s; P_e; P_c]$

1) *Data Owner:*

foreach $d_i \in D$

Find minimum required space for each d_i

Compute cell index of d_i using filled hilbert and add to C

2) Sort the list C

3) foreach $c_i \in C$

$P_s = c_x$

while size(P_c) < k do

Add d_j to P_c

$P_e = c_y$

4) *Data Owner:* DO Encrypts Hilbert packet list with RC5 key and send to SP

5) *Data Owner*: DO Sends spatial query range and RC5 key to AU by encrypting the AU public key

6) *Authentication User:* AU requests the SP by suing spatial query range

7) *Service Provider:* SP sends encrypted spatial data to the AU as a reply

8) *Authentication User:* AU decrypts the spatial data by using known RC5 key

9) *Service Provider:* SP sends alert message to DO, when it receives number false special query range requested from an AU.

III. PERFORMANCE ANALYSIS

In our proposed approach, unauthorized user is unable to get access from service provider due to it does not have valid key. Even the attacker is able to break the authentication by using brute force approach still the attacker is unable find the mapping of encrypted queries. If number of false queries arrived at SP then SP is informed to DO corresponding AU. DO will either deletes AU from the SP list or sends warn message to the AU. On the other hand, any Service provider sends the fake data, AU detect the fake data easily by using RC5 decryption algorithm.

IV. RESULTS ANALYSIS

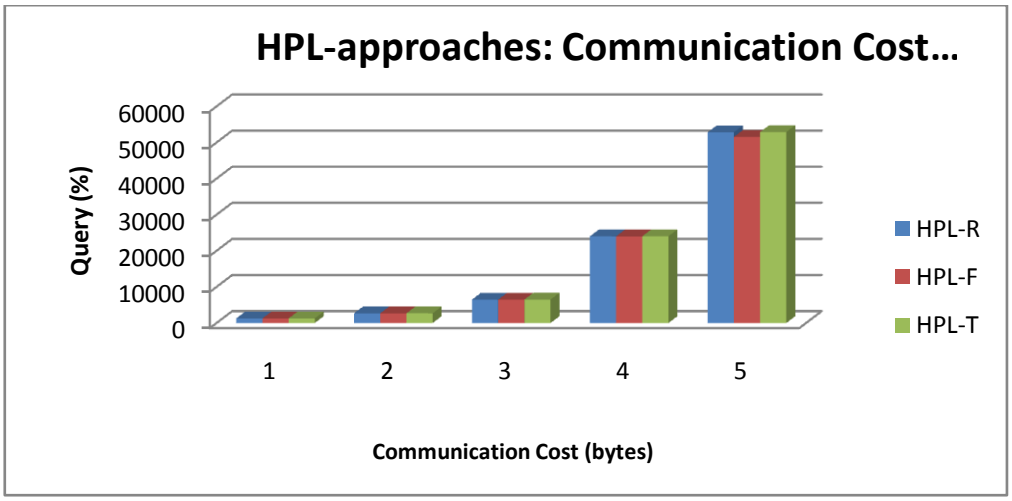

Fig 1:- HPL Approaches Communication Cost

Table I HPL Approaches Communication Cost Variation

	Communication Cost (bytes)		
Query (%)	HPL-R	HPL-F	HPL-T
0.5	1263	1259	1264
1	2684	2682	2694
2	6482	6467	6488
5	24002	23985	24018
10	52838	51553	52893

The query sizes ranging from 0:5% to 10% are used in the experiments. A numerical analysis on the NE dataset; the rest of the datasets follow a similar trend. It is clear that the communication cost increases linearly as the query size increases due to the increase in number of packets returned. We compare the difference in communication cost between the 3 HPL approaches. The resulting cost in bytes in HPL-T and HPL-R is almost identical with a slight variation in HPL-F. HPL-F returns fewer packets as only the filled Hilbert cells are included in the HPL, which ensures that no irrelevant or extra points are returned.

V. CONCLUSION

In this paper, we have proposed a secure spatial query processing using hilbert packet list algorithm to provide confidentiality, integrity and availability to the spatial data, which is deployed in the cloud environment. Based on our server, we found that the existing mechanisms suffer from high computational and communication overhead, in addition to vulnerabilities still exists in their security mechanisms. To reduce the computational overhead, we use RC5 keys to encrypt the spatial data, and to reduce the communication overhead, Data owner stores the encrypted spatial data in service provider. We have done the performance analysis of proposed algorithm in the hostile environment. Eventually, we found that our proposed algorithm is able to protect against from data leakage, unauthorized access and fake data identification attacks.

REFERENCES

[1] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials,, vol. 15, no. 2, pp. 843–859, 2013.

[2] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The VLDB Journal, vol. 19, no. 3, pp. 363–384, 2010.

[3] P. Wang and C. V. Ravishankar, "Secure and efficient range queries on outsourced databases using r-trees," in 2013 IEEE 29th International Conference on Data Engineering (ICDE). IEEE, 2013, pp. 314– 325.

[4] A. M. Talha, I. Kamel, and Z. A. Aghbari, "Enhancing confidentiality and privacy of outsourced spatial data," in 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2015, pp. 13–18.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE Infocom, 2010 proceedings. IEEE, 2010, pp. 1–9.

[6] H. Xu, S. Guo, and K. Chen, "Building confidential and efficient query services in the cloud with rasp data perturbation," IEEE transactions on knowledge and data engineering, vol. 26, no. 2, pp. 322–335, 2014.

[7] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in IEEE 27th International Conference on Data Engineering. IEEE, 2011, pp. 601– 612.

[8] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted data sharing over untrusted cloud storage providers," in IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2010, pp. 97–103.

[9] H. Hacigum¨ us, B. Iyer, and S. Mehrotra, "Providing database as a ¨ service," in 18th International Conference on Data Engineering, 2002. Proceedings. IEEE, 2002, pp. 29–38.

[10] E. Damiani, S. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing confidentiality and efficiency in untrusted relational dbmss," in Proceedings of the 10th ACM conference on Computer and Communications Security. ACM, 2003, pp. 93–102.

[11] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query integrity assurance of location-based services accessing outsourced spatial databases," in Advances in Spatial and Temporal Databases. Springer, 2009, pp. 80– 97.

[12] A. Khoshgozaran and C. Shahabi, "Private buddy search: Enabling private spatial queries in social networks," in International Conference on Computational Science and Engineering, 2009 (CSE'09)., vol. 4. IEEE, 2009, pp. 166–173.

[13] Anil Kumar Uppula , Srinivasulu Tadisetty ," Achieving better Authentication and Copyright protection Using DWT and SVD Based Watermarking Scheme,"International Journal of Computer Engineering In Research Trends.,vol.3,no.9,pp.487- 491,September 2016.

[14] Venkata Srinivasu Veesam, Bandaru Satish Babu," Evaluation of Captcha Technologies towards Graphical Password Scheme," International Journal of Computer Engineering In Research Trends.,vol.2,no.1,pp.98-106,February 2015.

[15] D.J. Ashpin Pabi, N.Puviarasan, P.Aruna," Fast Singular value decomposition based image compression using butterfly particle swarm optimization technique (SVD-BPSO)," International Journal of Computer Engineering In Research Trends.,vol.4,no.4,pp.128-135,April 2017.

