International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
568 – 572

Implementation of Space-Filling Curves on Spatial Dataset: A Review Paper

Ms. Vaishnavi Prashant Patil
Computer Science & Technology
Department of Technology, Shivaji University
Kolhapur, India
vshnvpatil3@gmail.com

Ms. Amrita A. Manjrekar
Computer Science & Technology
Department of Technology, Shivaji University
Kolhapur, India
aam_tech@unishivaji.ac.in

***Abstract*—** Cloud computing is the most recent innovative achievement that everybody ought to know about independent of whether you are a provider or a purchaser of innovative technology. Financial benefits are the essential driver for the Cloud, since it ensures the diminishment of capital utilize and operational utilize. The widespread use of the cloud has lead to the rise of database outsourcing. Privacy and security are the main considerations in the database outsourcing. Most of the conventional approaches provide security to outsourced data either by existing cryptographic techniques or using spatial transformation schemes. Here we propose a system which will implement and compare two space-filling algorithms (Hilbert curve and Gosper curve) on spatial data.

Keywords- *Database Outsourcing, Spatial data, Hilbert curve, Gosper curve, AES*

*****

I. INTRODUCTION

Cloud computing simply infers securing and getting to data and projects over the Internet as opposed to your PC's hard drive. Cloud computing[27] is a cutting edge innovation which offers plenty of advantages to the clients including adaptability, effectiveness and economical advantages to private and public entities. Monetary advantage provided by cloud is key purpose behind its selection by the majority of the clients today. Thus it is quickly changing the scene of data innovation, and at last transforming the long-held guarantee of utility processing into a reality. As of late, cell phones and navigational frameworks have progressed toward becoming exceedingly normal and this created the need for Location Based Services (LBSs) [28], which is an inspiring application for database outsourcing. This thus has prompted an expansion in spatial information which must be overseen and looked after viably. Spatial information in LBS incorporates the area data which require gigantic capacity limit. Location based administrations utilize ongoing geo-information or spatial information from a cell phone or Smartphone to give data, stimulation or security. Spatial databases are one of the core foundations of any GIS program. The spatial data gives information about the location, shape and size of an object on planet Earth. Location-based services provide street maps, 360° panoramic view of the streets which helps the users to find the exact location in fraction of seconds. This huge amount of spatial information should be maintained and processed by high-speed data management system which is beyond the capabilities of small business and individuals.

Efficient query processing is utmost important in location-based services. As the cloud computing services and location-based devices are progressing, a large amount of spatial data needs to be outsourced to the cloud, hence the privacy of this data is the major issue of concern for industry and academia.

Most of the conventional approaches provide security to outsourced data either by existing cryptographic techniques or using spatial transformation with the a significant number of the plans there is an involve between information secrecy and security. In this system, a balance between efficient query processing and obscuring data at the service provider is obtained. Here two space-filling algorithms (Hilbert curve and Gosper curve) applied to the spatial data and the most efficient one is used. The retransmission of lost packet is provided at the service provider through the use of truncated binary exponential back-off algorithm. This system also guarantees data integrity.

II. LITERATURE REVIEW

Hilbert-curve based cryptographic transformation scheme for protecting data privacy on outsourced private spatial data[1] proposed by H.-I. Kim, S.-T. Hong, and J.-W. Chang consists of a spatial data cryptographic scheme which is grid-based. Spatial database outsourcing has become common with cloud computing. Hence privacy and security of geographical data is important.

In this plan, the information proprietor encodes the spatial information purposes of every framework cell by utilizing an advanced mark calculation (DSA). Next, a cryptographic change conspire (CRT) which encodes every hub of built R-tree by utilizing AES (Advanced Encryption Standard) calculation is given. The current cryptographic change conspire gives high information security, however it causes the high inquiry handling cost. In this paper a Hilbert-bend based cryptographic change Scheme is proposed which brings down the correspondence cost

 ISSN: 2454-4248
568 – 572

while question handling in outsourced database. This plan utilizes Hilbert collection record as opposed to utilizing a tree structure with a specific end goal to improve the effectiveness of the question preparing. The proposed technique limits the extent of correspondence message by performing nearby information gathering in light of Hilbert-bend arrange. The HAI comprises of <ID, shv, ehv>, where shv and ehv mean the begin Hilbert-curve esteem and end Hilbert-curve estimation of the HAI record, individually and ID is a recognizable proof of the HAI record and

Frequency-hiding and Dependency-preserving Encryption for Outsourced Databases[2] is presented by Boxiang Dong and Wendy Wang. Here the author proposed a frequency hiding, FD-preserving probabilistic encryption scheme, named F2, that enables the service provider to discover the FDs from the encrypted dataset. The latest advancements in technology have made cloud computing a huge success. This has led to the practice of database outsourcing. Data dependency in the outsourced data is an important aspect in many data management tasks. This arises the issue of protecting sensitive data while preserving data dependency. Two attacks are considered, namely the frequency analysis (FA) attack and the FD-preserving chosen plaintext attack (FCPA), and it is shown that the F2 encryption scheme can defend against both attacks with formal provable guarantee. The empirical study demonstrates the efficiency and effectiveness of F2, as well as its security against both FA and FCPA attacks

A Spatial Transformation Scheme for Enhancing Privacy and Integrity of Outsourced Databases[3] displayed by Hyeong-Il Kim, Deul-Nyeok Youn, and Jae-Woo Chang comprises of a spatial change plot that makes utilization of shearing change with revolution moving for assurance of information. The development of cloud innovation has prompt the basic routine with regards to database outsourcing. It is extremely useful for spatial information proprietors as it lessens the cost of keeping up and dealing with the database. This plan abuses a min-max standardization strategy with a parceling system for supplying the changed information. Shearing change is solid against general assaults yet halfway against nearness assaults. To enhance execution against both assault models, the shearing change conspire incorporates turn annoyance, which is sufficiently protected if the first database is obscure.

Trusted Data Sharing over Untrusted Cloud Storage Providers[4] is a bit of work by Gansen Zhao, Chunming Rongy, Jin Liz, Feng Zhangx and Yong Tang. Distributed computing gives stockpiling administrations to clients, where clients can approach expansive volume of capacity. Information continued mists can likewise be shared by clients giving that the sharing is approved by the information proprietors. Initially the information proprietors have a restricted control over the cloud foundation. Also, the cloud specialist organizations have unnecessary benefits which enables them to change client's IT framework and information. The plan proposed in this paper tries to build up a system to address this issue by enabling clients to have put stock in information stockpiling and sharing over untrusted distributed storage suppliers. The general thought of the proposition system is to scramble the information before putting away on the cloud. On sharing the information, the encoded information will be re-scrambled without being unscrambled first. The re-scrambled information will then be cryptographically open to the approve client as it were.

Hoi Ting Poon and Ali Miri proposed A Privacy-Aware Search and Computation Over Encrypted Data Stores[5] wherein a different method for searching over unintelligent data is proposed. Anonymization is a technique which eliminates personally identifiable data such as unique numbers and names from user data. But it does not provide adequate protection. An option to this is encryption which has well defined security. Hence all the data owners mostly encrypt their data before uploading it to cloud. Different techniques to perform search over encrypted data are proposed here. The four categories of searchable encryption schemes are discussed: private-private, public-public, private-public and public-private. The schemes proposed here are encrypted indices, bloom filter, email filtering scheme, identity based encryption.

Modified Binary Exponential Backoff Algorithm to Minimize Mobiles Communication Time[6] by Ibrahim Sayed Ahmad comprises of a way to deal with explain the issues looked in remote neighborhood). Here a strategy to limit the time cycle of the data between mobiles moving in a Wi-Fi by changing the paired exponential back-off calculation is proposed. Paired Exponential Backoff (BEB) alludes to a crash determination system utilized as a part of irregular access MAC conventions. This calculation is utilized as a part of Ethernet (IEEE 802.3) wired LANs. In Ethernet organizes, this calculation is normally used to plan retransmissions after crashes.

Security Analysis For Hilbert Curve Based Spatial Data Privacy-Preserving Method[7] is proposed by F. Tian, X. Gui, P. Yang, X. Zhang, and J. Yang in the 2013 IEEE tenth International Conference on High Performance Computing and Communications and 2013 IEEE International Conference on Embedded and Ubiquitous Computing. IEEE, 2013, pp. 929– 934. Notwithstanding the likelihood that Hilbert curve is comprehensively used as a piece of security affirmation for spatial data, the security examination of standard Hilbert curve (SHC) isn't generally considered. In this paper, the characteristics of the reasons for interest (POI) documents worked by SHC are inspected

 ISSN: 2454-4248
568 – 572

and the records are imagined to consider the effect of the invalid regard divides. A list change system (SHC*) for SHC is proposed, which can for the most part harm the division shielding property of SHC, with a specific end goal to improve security. The attack show is moreover portrayed, in the trials, the assessed datasets are envisioned for unequivocally considering, and the estimation twisting exhibits that SHC* is more secure than SHC.

In the Study on Improved Truncated Binary Exponential Back-off Collision Resolution Algorithm[8] by Yongfa Ling and Deyu Meng published in the IJCSNS International Journal of Computer Science and Network Security, VOL. 6 No.11 the widely used collision resolution method is discussed. The truncated binary exponential back-off collision resolution algorithm is an algorithm used to remove rehashed retransmissions of the similar information. The investigations completed utilising the proposed approach demonstrate that this algorithm is effective and stable and has better throughput curve.

III. NEED OF WORK

The existing approaches ensure the security of the outsourced data using conventional cryptographic techniques or spatial transformation schemes. However, there is a comprise between faster query processing and confidentiality of data. To overcome this drawback, two algorithms for transformation – Hilbert Packet List and Gosper curve are applied to the data. The one which gives the best result is utilized. Then the transformed data is converted into unintelligible text using the encryption technique. Encryption ensures the security of outsourced data while another layer of security is added by transformation algorithm.

The proposed model consists of three main units, namely the Service Provider(SP), Data owner(DO) and the Authenticated User(AU).

IV. OUTLINE OF PROPOSED WORK

The proposed approach can be applied to any location based service to locate different landmarks in a city. A spatial database D representing physical locations using spatial data points is maintained at the DO side.

- First the information owner applies the Hilbert Packet List and Gosper curve to the spatial informational collection independently. In the Hilbert bend, HPL is built and the order-preserving encryption is applied to the HPL using function E_K to make OPE datasets. Gosper bend is a recursive bend developed by recursively supplanting a dotted arrow, called the initiator, by seven arrows, called generator.

- In the second step, the two are thought about and the most effective among them is connected to the spatial dataset. This information is scrambled and transferred
to the service provider.

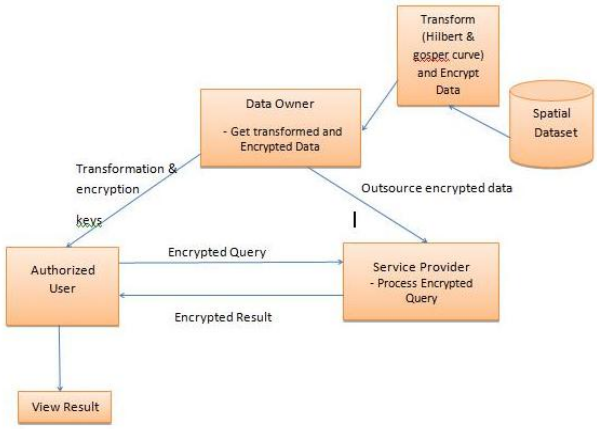

Fig 1: Block diagram of system architecture

The SP processes incoming encrypted query from the AU. The SP provider implements the truncated binary exponential back-off algorithm to retransmit the lost packets. It maintains a retransmission packet log database.

The AU converts the range query request to a set of 1D Hilbert indices. This integer set is converted into unintelligible format with the help of key K and sent to the SP to be executed over the HPL. The resulting response set, $R = (E_K(d1),\ldots,E_K(d_r))$, is returned to the AU where it is then decrypted using the key.

A. Hilbert Curve

A space-filling bend is a strategy for mapping the multi-dimensional space into the one-dimensional space. It acts like a string that experiences each telephone part (or pixel) in the D-dimensional Space with the objective that each curve is passed by correctly once.

The approach is to execute Hilbert curve and Gosper curve calculation. Hilbert bend based cryptographic change conspire (HCT) for protecting the security of spatial information in the outsourced databases in the cloud system is proposed here. Hilbert curve maps the two dimensional data into one dimensional. The proposed method can diminish the amount of message transmission for query dealing with and can limit the span of message used in communication. Subsequently the general time and cost is reduced.

 ISSN: 2454-4248
568 – 572

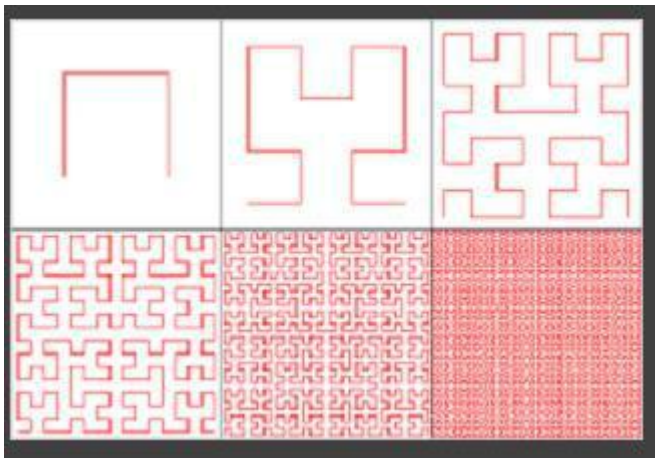

Fig 2: Hilbert curve formation

B. Gosper Curve

The Gosper curve is a self-similar fractal joining the hexagons into the composite called the Gosper island, which covers its bounding area and represents the hexagon-like tile filling the whole space.

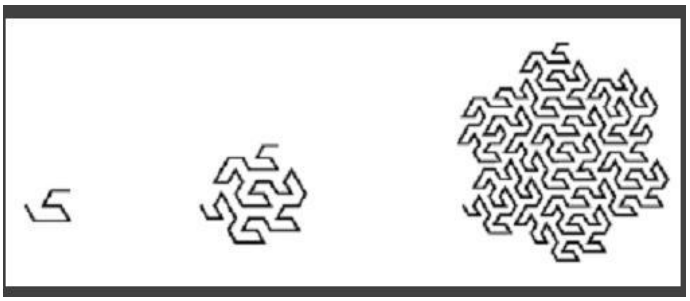

Fig 3: Gosper curve formation

C. Comparison

Parameter	Space-filling curve algorithms	
	Hilbert curve	**Gosper curve**
Complexity	Simple	Complex
Grid	Square or rectangular grid	Hexagonal grid
Conversion method	Every corner of the curve is replaced by 4 new corners	Order 1 gosper curve is used to replace the segment of the curve
No. of segments	Hilbert curve of order d consists of 4d points and 4d-1 segments of length 1/2d	Gosper curve of order d consists of 7d segments of length 1/(p7)d

V. CONCLUSION

The vast majority of the cloud clients opt for database outsourcing. In this manner, researches about queries on spatial information security in outsourced databases have been considered effectively. The proposed framework tries to accomplish a harmony between information privacy and effective query processing. Change on the spatial query is applied utilizing space filling curves. Later the ideal changed information is encoded utilizing the AES to handle the security ruptures. Subsequently the trade-off between the information security and speedier query retrieval is disposed of.

REFERENCES

[1] H.-I. Kim, S.-T. Hong, and J.-W. Chang, "Hilbert-curve based cryptographic transformation scheme for protecting data privacy on outsourced private spatial data," in 2014 International Conference on Big Data and Smart Computing (BIGCOMP). IEEE, 2014, pp. 77–82.

[2] Boxiang Dong, Wendy Wang "Frequency-hiding and Dependency-preservingEncryptionforOutsourced Databases" 2017 IEEE 33rd International Conference on Data Engineering

[3] Hyeong-Il Kim, Deul-Nyeok Youn, and Jae-Woo Chang "A Spatial Transformation Scheme for Enhancing Privacy and Integrity of Outsourced Databases " Springer-Verlag Berlin Heidelberg 2014 G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang,

[4] "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.

[5] Hoi Ting Poon and Ali Miri "Privacy-Aware Search

 ISSN: 2454-4248
568 – 572

and Computation Over Encrypted Data Stores" Springer International Publishing

[6] Ibrahim S Ahmad "Modified Binary Exponential Backoff Algoayedrithm to Minimize Mobiles Communication Time" - I.J. Information Technology and Computer Science, 2014, 03, 20-29

[7] F. Tian, X. Gui, P. Yang, X. Zhang, and J. Yang, "Security analysis for hilbert curve based spatial data privacy-preserving method," in 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. IEEE, 2013, pp. 929–934.

[8] Yongfa Ling and Deyu Meng "Study on Improved Truncated Binary Exponential Back-off Collision Resolution Algorithm", IJCSNS International Journal of Computer Science and Network Security, VOL. 6 No.11

[9] 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.

[10] C. Gentry et al., "Fully homomorphic encryption using ideal lattices" in STOC, vol. 9, 2009, pp. 169–178.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.

[11] Ayesha M. Talha, Ibrahim Kamel "Facilitating Secure and Efficient Spatial Query Processing on the Cloud", IEEE Transactions on Cloud Computing

[12] 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.

[13] "Openstreetmap," http://www.openstreetmap.org/.

[14] H. Hacigumus, B. Iyer, and S. Mehrotra, "Providing database as a service," in 18th International Conference on Data Engineering, 02. Proceedings. IEEE, 2002, pp. 29–38.

[15] E. Damiani, S. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati m, "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.

[16] Gansen Zhao, Chunming Rongy, Jin Liz, Feng Zhangx and Yong Tang "Trusted Data Sharing over Untrusted Cloud Storage Providers"

[17] Hyeong-Il Kim, Deul-Nyeok Youn, and Jae-Woo Chang "A Spatial Transformation Scheme for Enhancing Privacy and Integrity of Outsourced Databases"

[18] Boldyreva, N. Chenette, Y. Lee, and A. Oneill "Order-preserving symmetric encryption," in Advances in cryptology- EUROCRYPT Springer, 2009 pp 224-241