

PRIVACY PRESERVING SPATIO - TEXTUAL SKYLINES BASED ON LOCATION AGGREGATION

¹ Srilatha Puli, ² Dandem Ajay Kumar, ³ Kenche Vaishnavi, ⁴ Baddam. Rithvik Reddy, ⁵ Cheera Kavya

Assistant Professor in Department of CSE Sreyas Institute Of Engineering And Technology

srilatha.puli@sreyas.ac.in

^{2,3,4,5} UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

¹ ajaydandem123@gmail.com, ³ vaishnavikenche563@gmail.com, ⁴ baddamrithvik@gmail.com,

⁵ Kavyacheera25@gmail.com

Abstract: To achieve cost-savings, data owners outsource their spatiotextual query services to public cloud, which, however, may bring serious privacy issues. In this paper, we define and study the problem of privacy-preserving spatio-textual skylines in cloud environments. To address the problem, we first transform the locations and texts of each data object and query request into vectors and encrypt the vectors based on an vector based encryption method to protect the data privacy. Exploiting the group of query locations to accelerate the query processing, we further present a location-aggregation-based query request generation method. Based on encrypted aggregated query requests, we present a corresponding query processing algorithm for privacy-preserving spatio-textual skylines. Finally, we present analysis to show the security guarantee of the proposed methods, and conduct thorough experiments on real datasets to show the performance of our algorithms.

I INTRODUCTION

With the rapid development of the mobile Internet, users of mobile Internet applications are motivated to search some points based on their interests leveraging both spatial proximity and textual relevance over spatio-textual data, which are defined by merging geographical locations and textual descriptions [1]. Spatio-Textual Skylines (STS) allow users to find points of which the locations are near a group of spatial query locations and the descriptions are relevant to a set of keywords. For enjoying the great cost-savings of cloud platforms, more data owners choose to outsource their location-based services to the public cloud, however, the direct outsourcing may arouse serious privacy concerns. Since sensitive or private locations and texts are contained in both spatio-textual dataset and users' query requests, which may be utilized by adversaries to imply the user privacy, such sensitive information must not be learnt by an untrusted third party, the cloud service provider. Therefore, for securely providing services on locations, it is necessary to address the privacy-preserving spatio-textual skylines (PSTS) problem under encryption

settings. In the existing studies, only a few focus on the privacy-preserving problem of spatio-textual queries on untrusted cloud platforms. In our previous work, Su et al. [2] proposed a privacy-preserving top-k spatio-textual query scheme in cloud environments. Recently, Cui et al. [3] proposed a privacy-preserving boolean spatial keyword queries under encryption settings. Since both of these two works only consider the relevance measuring on single query request, they cannot solve the PSTS problem. Other related works focus on the primary problems of PSTS separately, i.e., privacy-preserving spatial queries and privacy-preserving textual queries. To this end, we define and study PSTS queries in cloud environments. To protect the privacy of objects in spatiotextual dataset, we transform the locations and texts of each object into vectors and encrypt the vectors based on Asymmetric Scalar-Product-Preserving Encryption (ASPE) [4], an vector-based encryption method [3] proved secure against known background threat model. To address the privacy issues of query requests with a group of query locations, we further present a location-aggregation-based query request generation method, in which the group of query locations is aggregated into Minimum Bounding Rectangles (MBRs) according to the distributions of the locations. Together with the query texts, the query request and the aggregated MBRs are transformed into vectors and encrypted by ASPE. At last, we present the query processing algorithm of PSTS, where the encrypted aggregated MBRs are utilized to help prune the dominated objects before the dominance tests over each query request. Analysis shows the security guarantee of the proposed methods, and thorough experimental results on real datasets show the performance of our algorithms. In summary, the contributions of this paper are as follows, x We define and study the privacy-preserving spatio-textual skylines (PSTS) problem in semi-trusted cloud environment. x To address this problem, we first encrypt spatio-textual objects and query requests with ASPE to protect the data privacy. Exploiting the group of query locations to improve the query efficiency, we further present a location-aggregation-based query request generation method. At last, we present the query processing algorithm of privacy-preserving spatio-textual skylines. x Analysis shows the security guarantee of the proposed methods, and thorough experimental results on real datasets show the performance of our algorithm. we define PSTS problem and present our system model, threat model and necessary preliminaries.

II LITERATURE SURVEY

Queries over spatio-textual data have been studied for several years [1], of which various types have been proposed such as spatial keyword top-k query [5-7], boolean spatio-textual query [8], etc. Shi et al. [9] first proposed the spatio-textual skyline query method over indices, where the spatio-textual dominance

is first defined. However, only a few works study the privacy protection problem of spatio-textual queries in untrusted cloud environments. In our previous work, Su et al. [2] proposed a privacy-preserving top-k spatio-textual query scheme in cloud environments. Cui et al. [3] proposed a privacy-preserving boolean spatial keyword queries under encryption settings. Both of these two works cannot solve the PSTS problem. Other related works focus on the primary problems of PSTS separately, i.e., privacy-preserving spatial queries and privacy-preserving textual queries.

A. Privacy-preserving Spatial Queries. Privacy-preserving queries over spatial data has been addressed in some recent works. Focusing on the secure kNN problem, Wong et al. [4] first proposed Asymmetric Scalar-product-Preserving Encryption (ASPE). Through ASPE, Wang et al. [10] proposed a secure index \hat{R} -tree to support secure half-space range queries. Hu et al. [11] proposed a method based on privacy homomorphism to solve the secure kNN problem on the R-tree index, in which the encryption function and decryption function are carried out on the user-side and the server-side respectively. Elmehdwi et al. [12] proposed a secure kNN protocol based on Paillier cryptography system. Chen et al. [13] proposed an efficient query result verification algorithm for skyline queries in the cloud environment, ensuring the resulting security of skyline queries. Liu et al. [14] proposed a skyline query protocol based on semantic security encryption mechanism to solve the skyline query problem on encrypted data.

B. Privacy-preserving Textual Queries. For privacy-preserving textual queries, the formal definition of searchable encryption and a secure index structure based on the inverted file is proposed in [15]. Wang et al. [16] solved the problem of result ranking in secure keyword queries by using the encryption on keyword frequency and order retention. A file index structure for similarity query based on LSH is proposed in [17]. Cao et al. [18,19] proposed a privacy-preserving multi-keyword query algorithm based on symmetric encryption. Fu et al. [20] proposed an accurate and efficient multi-keyword fuzzy search scheme over encrypted outsourced data.

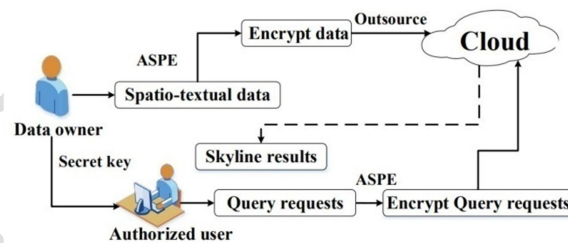
III EXISTING SYSTEM

In the existing studies, only a few focus on the privacy preserving problem of spatio-textual queries on untrusted cloud platforms. In our previous work, Su et al. [2] proposed a privacy-preserving top-k spatio-textual query scheme in cloud environments. Recently, Cui et al. [3] proposed a privacy-preserving boolean spatial keyword queries under encryption settings. Since both of these two works only consider the relevance measuring on single query request, they cannot solve the PSTS problem. Other related works focus on the primary problems of PSTS separately, i.e., privacy preserving spatial queries and privacy-preserving textual queries

IV PROPOSED SYSTEM

We define and study PSTS queries in cloud environments. To protect the privacy of objects in spatiotextual dataset, we transform the locations and texts of each object into vectors and encrypt the vectors based on Asymmetric Scalar-Product-Preserving Encryption (ASPE) [4], an vector-based encryption method [3] proved secure against known background threat model. To address the privacy issues of query requests with a group of query locations, we further present a location-aggregation-based query request generation method, in which the group of query locations is aggregated into Minimum Bounding Rectangles (MBRs) according to the distributions of the locations. Together with the query texts, the query request and the aggregated MBRs are transformed into vectors and encrypted by ASPE. At last, we present the query processing algorithm of PSTS, where the encrypted aggregated MBRs are utilized to help prune the dominated objects before the dominance tests over each query request. Analysis shows the security guarantee of the proposed methods, and thorough experimental results on real datasets show the performance of our algorithms.

V ARCHITECTURE



System Architecture

VI METHODOLOGY

In the threat model, we assume the cloud and its service provider follow a semi-honest model, in which the cloud, acting in “honest but curious” fashion, will correctly execute the user-designed protocols, and try to collect and analyze the valuable information from the data and query requests. We adopt the security model of the encryption as Known Background Model, which has been applied in existing research [3]. For the scheme presented in the paper, we focus on following design goals on the privacy protection.

Data privacy. The spatio-textual data, containing sensitive and private information on locations and texts, cannot be utilized in plaintext when being outsourced to the cloud. Therefore, the privacy of spatio-

textual data should be protected in our system. Query privacy. The spatio-textual query requests consist of users' locations and interested keywords, which are related to user privacy. Besides, the intermediate results during the query processing may leak privacy information. Thus, the query privacy should be considered in our system

We designed the model to be both security and efficiency. The details are as follows:

- 1) The data owner first encrypts the data and then sends the ciphertext data to the cloud server. Nevertheless, the cloud server does not have access to the plaintext data throughout the process.
- 2) During the query process, the query request sent by the users does not contain any private data, and the cloud server sends the query result in the form of ciphertext to the data user.
- 3) As a query processing model, efficiency should be one of the most important criteria to measure its performance. Although the entire query is done on the ciphertext, it should be guaranteed that the query efficiency is not reduced too much.

VII IMPLEMENTATION

Data owners: the data owner, the authorized user and the cloud. The data owner manages the spatio-textual data and encrypts such data using the secret key to ensure the security. After that, the data owner outsources the encrypted spatio-textual data to the cloud for providing the query services.

Cloud servers: The cloud server has a huge capacity for storage and computing and provides data storage and computing services

Users: The user, authorized by the data owner, issues a spatio-textual skyline query with his/her locations and query keywords. To protect the privacy, the authorized user encrypt the query requests using secret key offered by the data owner, and sends the encrypted query requests to the cloud. By receiving the encrypted requests, the cloud executes the privacy-preserving spatio-textual skyline query processing over the encrypted data without decryption, and returns the skyline results back to the corresponding user in cipher text.

VIII RESULTS

Privacy-preserving Spatio-Textual Skylines Based on Location Aggregation

Home Login User Registration Owner Registration

Login Here

Login Register

Copyright © 2024 by IJESR

f p in bi

Privacy-preserving Spatio-Textual Skylines Based on Location Aggregation

Home Login User Registration Owner Registration

User Registration Form

Enter date of birth

Location

Privacy-preserving Spatio-Textual Skylines Based on Location Aggregation

Home Login User Registration Owner Registration

Data Owner Registration Form

Enter date of birth

Location



Business & Enterprise Cloud Service Pricing

Personal Plans **Business Plans** Billed: ☐ monthly ☒ yearly (save 2 months)

About Business Plans

- 21 years of service, 99.99% uptime
- Better features & lower pricing
- Business security & compliance
- Fast support
- 25% off for non-profit organizations

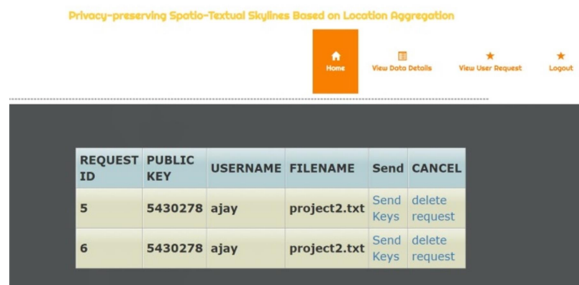
Detailed Business Features

Watch a video about Plans & Pricing

	Business Basic	Business Plus	Enterprise	Custom Plan
Business Basic	\$4 per month 3 to 25 users	\$10 per month 25 or more users	\$15 per month 25 or more users	Custom Price Open & 750 3 or more users
	Order	Order	Order	Order
	Free Trial	Free Trial	Free Trial	Free Trial

Main Features of DriveHQ Enterprise Cloud IT Service

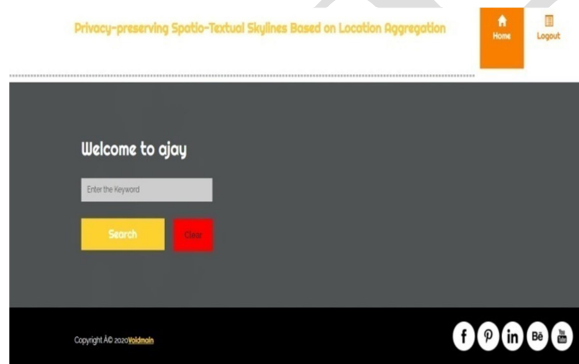
Personal Features and Common Features	Business Basic	Business Plus	Enterprise	Custom Plan
Cloud Drive Mapping	✓	✓	✓	✓
DriveHQ FileManager, Folder Sync and Online Backup	✓	✓	✓	✓



Privacy-preserving Spotio-Textual Skylines Based on Location Aggregation

[Home](#) [View Data Details](#) [View User Request](#) [Logout](#)

REQUEST ID	PUBLIC KEY	USERNAME	FILENAME	Send	CANCEL
5	5430278	ajay	project2.txt	Send Keys	delete request
6	5430278	ajay	project2.txt	Send Keys	delete request



Privacy-preserving Spotio-Textual Skylines Based on Location Aggregation

[Home](#) [Logout](#)

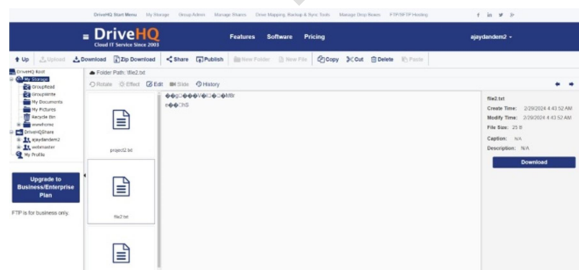
Welcome to ajay

Enter the keyword

[Search](#) [Clear](#)

Copyright © 2024 [Bodduna Sriveni](#)

[f](#) [p](#) [in](#) [be](#) [t](#)



DriveHQ Cloud IT Service Since 2003

Cloud Drive Mapping

Folder Path: /ajay

Files: project2.txt, folder

Details:

File Name: project2.txt
File Size: 21 B
Created Time: 2/20/2024 4:42:12 AM
Modified Time: 2/20/2024 4:42:12 AM
Caption: N/A
Description: N/A

[Download](#)

IX CONCLUSION

In this paper, we define and study the problem of privacy-preserving spatio-textual skylines in cloud environments. To address the problem, we first transform the locations and texts of each data object and query request into vectors and encrypt the vectors based on the vector-based encryption method to protect the data privacy. Exploiting the group of query locations to accelerate the query processing, we further present a location-aggregation-based query request generation method. Based on encrypted aggregated query requests, we present a corresponding query processing algorithm for privacy-preserving spatio-textual skylines. Analysis shows the security guarantee of the proposed methods, and experimental results on real datasets show the performance of our algorithms

REFERENCES

1. Srilatha Puli, A Machine Learning Model For Air Quality Prediction For Smart Cities, Design Engineering || Issn: 0011-9342 | Year 2021 - Issue: 9 | Pages: 18090 – 18104
2. Srilatha Puli, Quality Risk Analysis For Sustainable Smart Water Supply Using Data Perception, International Journal Of Health Sciences Issn 2550-6978 E-Issn 2550-696x © 2022, <https://doi.org/10.53730/Ijhs.V6ns5.9826>, 18 June 2022
3. Srilatha Puli, Urban Street Cleanliness, Journal Of Algebraic Statistics Volume 13, No. 3, 2022, P. 547-552, <https://publishoa.com>, Issn: 1309-3452
4. Srilatha Puli, Self-Annihilation Ideation Detection, Neuroquantology | June 2022 | Volume 20 | Issue 6 | Page 7229-7239 | Doi: 10.14704/Nq.2022.20.6.Nq22727
5. Srilatha Puli, Crime Analysis Using Machine Learning, Ymer|| Issn: 0044-0477, April 2022
6. Srilatha Puli, N-Grams Assisted Youtube Spam Comment Detection, Ymer || Issn: 0044-0477, April 2022
7. Srilatha Puli, Analysis Of Brand Popularity Using Big Data And Twitter, Ymer|| Issn: 0044-0477, April 2022
8. Srilatha Puli, Cyber Threat Detection Based On Artificial Neural Networks Using Event Profiles, The International Journal Of Analytical And Experimental Modal Analysis, Issn No:0886-9367

9. 5. Srilatha Puli, Face Mask Monitoring System, The International Journal Of Analytical And Experimental Modal Analysis, Issn No:0886-9367
10. Srilatha Puli, Iot Based Smart Door Lock Surveillance System Using Security Sensors, Advanced Science Letters E-Issn:1936-7317
11. Srilatha Puli, Safety Alerting System For Drowsy Driver, 9th International Conference On Innovations In Electronics & Communication Engineering (Iciece-2021), Page – 40
12. N. Swapna Suhasini, Srilatha Puli, Big Data Analytics For Malware Detection In A Virtualized Framework, Journal Of Critical Reviews, Issn:2394-5125 Vol.7, Issue 14, July – 2020
13. Srilatha Puli, Block Chain Based Certificate Validation, International Journal Of Science And Research (Ijsr), Issn: 2319-7064 Sijf (2022): 7.942, Volume 11 Issue 12, December 2022, Paper Id: Sr221219113003, Doi: 10.21275/Sr221219113003, www.ijer.net
14. Mrs. Srilatha Puli, Energy Efficient Teaching-Learning-Based Optimization For The Discrete Routing Problem In Wireless Sensor Network, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022.
15. Mrs. Srilatha Puli, A Hybrid Block Chain-Based Identity Authentication Scheme For Multi- Wsn, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022
16. Mrs. Srilatha Puli, Implementation Of A Secured Watermarking Mechanism Based On Cryptography And Bit Pairs Matching, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022
17. Mrs. S.Sunitha, Mrs. Srilatha Puli, Multilevel Data Concealing Technique Using Steganography And Visual Cryptography, International Journal Of Early Childhood Special Education (Int-Jecse) Doi:10.48047/Intjecse/V15i1.1 Issn: 1308-5581 Vol 15, Issue 01 2023
18. Mrs. Srilatha Puli, Blood Bank Management Donation And Automation, Specialusis Ugdyas / Special Education 2022 1 (43), <https://www.sumc.lt/index.php/Se/Article/View/1995>

19. N. S. Suhasini And S. Puli, "Big Data Analytics In Cloud Computing," 2021 Sixth International Conference On Image Information Processing (Iciip), Shimla, India, 2021, Pp. 320-325, Doi: 10.1109/Iciip53038.2021.9702705.
20. Mrs. Srilatha Puli, Key-Aggregate Proxy Re-Encryption With Dynamic Condition Generation Using Multilinear Map, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages - 2679-2685, E-Issn: 2368-7487.
21. Mrs. Srilatha Puli, Mrs. Sunitha Surarapu, Deep Learning-Based Framework For Robust Traffic Sign Detection Under Challenging Weather Conditions, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2650-2657, E-Issn: 2368-7487.
22. Mrs. Srilatha Puli, Mrs. Sunitha Surarapu, License Plate Image Analysis Empowered By Generative Adversarial Neural Networks (Gans), Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2693-2698, E-Issn: 2368-7487.
23. Mrs. Srilatha Puli, Mrs. Sunitha Surarapu, Food Calorie Estimation Using Convolutional Neural Network, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2665-2671, E-Issn: 2368-7487.
24. Mrs. Sunitha Surarapu, Mrs. Srilatha Puli, An Integrated Architecture For Maintaining Security In Cloud Computing Based On Blockchain, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2608-2616, E-Issn: 2368-7487.
25. Mrs. Sunitha Surarapu, Mrs. Srilatha Puli, Two Level Lstm For Sentiment Analysis Using Lexicon Embedding And Polar Flipping, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2750-2756, E-Issn: 2368-7487.
26. Mrs. Sunitha Surarapu, Mrs. Srilatha Puli, Task Failure Prediction In Cloud Data Centers Using Deep Learning, Journal Of Survey In Fisheries Sciences 10(1) 2023, Pages – 2742-2749, E-Issn: 2368-7487.
27. Mrs. Srilatha Puli, Human Computer Interaction Based Head Controlled Mouse. International Journal Of Early Childhood Special Education. (Int-Jecse), Doi :10.48047/Intjecse/V15i4.60, Issn: 1308-5581 Vol 15, Issue 04 2023

27. Mrs. Srilatha Puli, The Breakout Ball Game Using Java, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V15i4.84 Issn: 1308-5581 Vol 15, Issue 04 2023, Pages: 766-772.

28. Mrs. Srilatha Puli, Data Duplication Removal Technology Using Aws Services, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V15i4.67 Issn: 1308-5581 Vol 15, Issue 04 2023, Pages: 651-659.

29. Mrs. Srilatha Puli, Human Computer Interaction Based Head Controlled Mouse, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V15i4.60 Issn: 1308- 5581 Vol 15, Issue 04 2023, Pages: 584-590