Enabling Secure Spatial Query Processing on the Cloud

K.RAJESHWARI[1], V.PRADEEP KUMAR[2], DR.M.GOPICHAND3

[1]*M tech PG Scholar, department of CSE B.V. Raju Institute of Technology, Narsapur, Medak, India.*

[2]*Professor department of CSE B.V. Raju Institute of Techn,* [3]*Professor,Hod department of IT Vardhaman Engineering college in Hyderabad, India*

Abstract- Location-based services (LBS) expect clients to ceaselessly report their area to a conceivably endowed server to acquire administrations in view of their area, which can open them to security dangers. Lamentably, existing security saving strategies for LBS have a few restrictions, for example, requiring a completely confided in outsider, offering constrained protection certifications and bringing about high correspondence overhead. In this paper, we propose a client characterized security framework called dynamic lattice framework (DGS); the principal comprehensive framework that satisfies four basic necessities for protection safeguarding preview and constant LBS. (1) the framework just requires a semi-confided in outsider, in charge of doing basic coordinating activities effectively. This semi-confided in outsider does not have any data about a client's area. (2) Secure depiction and consistent area protection is ensured under our characterized enemy models. (3) The correspondence cost for the client does not rely upon the client's coveted security level; it just relies upon the quantity of pertinent purposes of enthusiasm for the region of the client. (4) Although we just spotlight on range and k-closest neighbor inquiries in this work, our framework can be effectively reached out to help other spatial questions without changing the calculations keep running by the semi-confided in outsider and the database server, gave the required hunt territory of a spatial inquiry can be dreamy into spatial locales. Trial comes about demonstrate that our DGS is more proficient than the cutting edge security protecting system for nonstop LBS.

Watchwords- Dynamic framework frameworks, area security, area based administrations, spatial question handling, cryptography.

I. INTRODUCTION

In this day and age of versatility and ever-show Internet network, an expanding number of individuals utilize area based administrations (LBS) to ask for data pertinent to their present areas from an assortment of specialist organizations. This can be the scan for close-by purposes of intrigue (POIs) (e.g., eateries and lodgings), area mindful publicizing by organizations, activity data customized to the thruway and heading a client is voyaging et cetera. The utilization of LBS, nonetheless, can uncover considerably more about a man to possibly conniving specialist co-ops than numerous individuals would unveil. By following the solicitations of a man it is conceivable to construct a development profile which can uncover data about a client's work (office area), medicinal records (visit to master centers), political perspectives (going to political occasions), and so forth.

All things considered, LBS can be exceptionally significant and all things considered clients ought to have the capacity to make utilization of them without giving up their area security. Various methodologies have as of late been proposed for saving the client area security in LBS. By and large, these methodologies can be grouped into two fundamental classifications. (1) Fully-confided in outsider (TTP). The most prominent security protecting procedures require a TTP to be set between the client and the specialist co-op to conceal the client's area data from the specialist organization (e.g., [1]–[8]). The primary errand of the outsider is monitoring the correct area everything being equal and obscuring a questioning client's area into a shrouded territory that incorporates k − 1 different clients to accomplish k-secrecy. This TTP display has three downsides. (an) All clients need to ceaselessly report their correct area to the outsider, despite the fact that they don't buy in to any LBS. (b) As the outsider knows the correct area of each client, it turns into an alluring focus for assailants. (c) The k-secrecy based methods just accomplish low local area security in light of the fact that shrouding a district to incorporate k clients by and by for the most part brings about little shrouding regions. (2) Private data recovery (PIR). In spite of the fact that PIR strategies don't require an outsider, they cause a substantially higher correspondence overhead between the client and the specialist co-op, requiring the transmission of considerably more data than the client entirely (e.g., [9]– [11]).

Just a couple of security saving methods has been proposed for nonstop LBS [2], [7]. These methods depend on a TTP to persistently grow a shrouded region to incorporate the at first appointed k clients. These methods not just acquire the downsides of the TTP show; however they additionally have different constraints. (1) Inefficiency. Ceaselessly growing shrouded zones considerably builds the question handling overhead. (2) Privacy spillage. Since the database server gets an arrangement of back to back shrouded regions of a client at various timestamps, the connection among the shrouded regions would give valuable data to construing the client's area. (3) Service end. A client needs to end the administration when clients at first allocated to her shrouded zone leave the framework.

In this paper, we propose a client characterized security framework called dynamic network framework (DGS) to give protection saving depiction and ceaseless LBS. In DGS, a questioning client initially decides an inquiry region, where the client is agreeable to uncover the way that she is some place inside this inquiry region. The inquiry zone is separated into parallel estimated matrix cells in light of the dynamic network structure indicated by the client. At that point, the client scrambles an inquiry that incorporates the data of the question region and the dynamic matrix structure, and encodes the character of every framework cell meeting the required hunt zone of the spatial question to create an arrangement of encoded identifiers. Next, the client sends a demand including (1) the scrambled question and (2) the encoded identifiers to Service Provider (SP). For each chose POI, SP scrambles its data, utilizing the dynamic framework structure determined by the client to discover a matrix cell covering the POI, and encodes the phone personality to create the encoded identifier for that POI. The encoded POIs with their relating scrambled identifiers are come back to the client a subset of encoded POIs whose comparing identifiers coordinate any of the encoded identifiers at first sent by the client. After the client gets the scrambled POIs, he/she unscrambles them to get their correct areas and processes an inquiry reply.

II. RELATED WORK

Spatial shrouding methods have been generally used to save client area protection in LBS. The vast majority of the current spatial shrouding procedures depend on a completely confided in outsider (TTP), more often than not named area anonymizer, that is required between the client and the specialist organization (e.g., [1]– [8]). At the point when a client buys in to LBS, the area anonymizer will obscure the client's correct area into a shrouded region with the end goal that the shrouded territory incorporates at any rate k – 1 different clients to fulfill k-secrecy. The TTP show has four noteworthy downsides. (an) It is hard to locate an outsider that can be completely trusted. (b) All clients need to constantly refresh their areas with the area anonymizer, notwithstanding when they are not bought in to any LBS, so the area anonymizer has enough data to process shrouded territories. (c) Because the area anonymizer stores the correct area data all things considered, bargaining the area anonymizer uncovered their areas. (d) k-secrecy normally uncovers the surmised area of a client and the area protection relies upon the client circulation. In a framework with such local area security it is troublesome for the client to determine customized protection prerequisites. The inclination based approach [12] reduces this issue by finding a shrouded region in light of the quantity of its guests that is at any rate as well known as the client's predefined open area. Cryptographic instruments were utilized to ensure outsourcing information. A request saving encryption conspire [13] utilizes a container based encryption E with the end goal that E(x) < E(y) for each match of qualities for which x < y. Be that as it may, there does not appear to be a clear method to extend it to secure spatial information. Another approach portrayed in [36] for outsourcing information utilizes homomorphism encryption to empower total SQL inquiries over encoded databases. The degree concentrates just on basic numerical areas and total inquiries in SQL. This approach has additionally been appeared to be uncertain in [14].

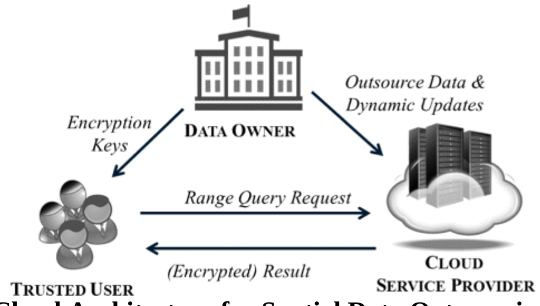
Likewise examined for security in LBS are techniques which take a shot at scrambled or changed information. For instance, Khoshgozaran and Shahabi proposed a framework which utilizes Hilbert bends to delineate into an alternate space and after that understands NN inquiries in the changed space [15]. A comparative approach however utilizing encryption was proposed by Wong et al. in [16]. Their work centers around outsourcing a database in encoded arrangement to a specialist organization and enables clients to perform k-NN questions on the scrambled database. Their concentration, be that as it may, is more on securing the database rather than the protection of the clients. Comparable work was done in [17].

A couple of securities safeguarding systems have endeavored to utilize the TTP show for ceaseless LBS [2], [7], [18]. The possibility of [2] is to continue extending an underlying shrouded zone to incorporate in any event a similar k clients, [7] is to foresee a client's impressions and obscure every impression into a k-anonym zed zone, and [18] is to utilize a blend zone to make the clients situated in there in the meantime undefined. The TTP display has been reached out to secure the protection of an anonym zed gathering of clients by summing up their spatial question locales to make their inquiries unclear [19] and certification that the quantity of their asked for benefit esteems is in any event m to accomplish m-invariance [20]. Worldly shrouding and encryption methods are utilized for total activity information gathering [21], yet they can't give protection safeguarding ceaseless LBS.

Another strategy proposed to secure consistent LBS is utilizing sham questions together with a genuine inquiry [22]. Be that as it may, this system issues a larger number of questions than the client truly needs. In our framework a client never transmits real area data (aside from the inquiry territory, which is just observed by the specialist organization and which can be picked self-assertively huge), and the kind of POI in a question must be perused by the specialist organization. The inquiry server has even less data accessible, it doesn't know the question region nor the sort of POI looked for.

III. SYSTEM IMPLEMENTATION

System Architecture

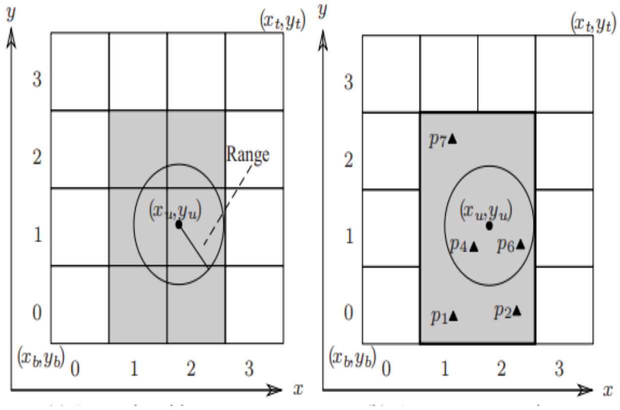


Cloud Architecture for Spatial Data Outsourcing

Cloud computing offers on-demand delivery of various computing resources by outsourcing data to entrusted cloud servers and allowing access only to authorized users. The data owners have to be aware of security concerns while achieving higher scalability and lower cost by outsourcing databases to the cloud. The cloud architecture model (Figure 1) comprises of 3 main entities, namely the Data Owner, Service Provider and Trusted User. The data owners have the two-dimensional spatial data points that have to be outsourced to a server that cannot be trusted. They deploy the required cloud service and guarantee security by transforming and encrypting the database before outsourcing to the service provider. Moreover, the authenticated users are provided with the transformation key as well as the decryption key. The TU utilizes the transformation key to issue encrypted range queries to the SP. The query is processed on the encrypted database at the SP and the results are returned to the user. The TU decrypts the query response using the key to obtain the actual data points.

Dynamic Grid System (DGS)

Our DGS has two main phases for privacy-preserving continuous range query processing. The first phase finds an initial (or a snapshot) answer for a range query, and the second phase incrementally maintains the query answer based on the user's location updates.



(a) Dynamic grid structure (b) Answer computation

Example of range query processing in DGS.

Range Query Processing

As described aforementioned a continuous range query is defined as keeping track of the POIs within a user-specified distance Range of the user's current location (x_u, y_u) for a certain time period. In general, the privacy-preserving range query processing protocol has six main steps.

Step1. Dynamic grid structure (by the user). The idea of this step is to construct a dynamic grid structure specified by the user. A querying user first specifies a query area, where the user is comfortable to reveal the fact that she is located somewhere within that query area. The query area is assumed to be a rectangular area, represented by the coordinates of its bottom-left vertex (x_b, y_b) and top-right vertex (x_t, y_t). Notice that the user is not necessarily required to be at the center of the query area. Instead, its location can be anywhere in the area. However, our system can also support irregular spatial regions, e.g., the boundary of a city or a county, by using a minimum bounding rectangle to model the irregular spatial region as a rectangular area. The query area is divided into m × m equal-sized grid cells to construct a dynamic grid structure, where m is a user-specified parameter. Each grid cell is identified by (c, r), where c is the column index from left to right and r is the row index from bottom to top, respectively, with $0 \leq c, r < m$. Given the coordinates of the bottom-left vertex of a grid cell, (x_c, y_c), the grid cell identity can be computed by **$(c,r) =(| x_c-x_b/(x_t-x_b)/m | , |y_c-y_b/(y_t-y_b)/m|)$**. Fig. 2 gives a running example for privacy-preserving range query processing, where the querying user is located in the cell (2, 1), m = 4, and the circle with a radius of the range distance Range specified by the user constitutes the query region of the range query.

Step2. Request Query generation (by the user). An encrypted query for a specific SP is prepared as:

Query ← AES_Enc (POI-type, (x_b, y_b), (x_t, y_t) ,K)

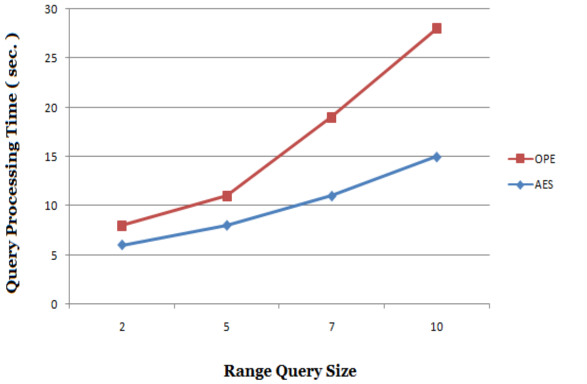
Where AES_Enc(·) is Advanced Encryption Standard (AES) under key size-128 bit. In the encrypted query, POI-type specifies the type of POIs, K is the encryption key which is shared by data owner, and the personalized dynamic grid structure is specified by (x_b, y_b), and (x_t, y_t).

Step3. Query processing (by SP). SP decrypts the request to retrieve the POI-type, the encryption key K selected by the user in the request generation step (Step 2), and the query area defined by (x_b, y_b), and (x_t, y_t). SP then selects a set of np POIs that match the required POI-type within the user specified query area from its database. For each selected POI j with a location (x_j, y_j)) ($1 \leq j \leq np$), SP computes the identity of the grid cell in the user specified dynamic grid structure covering j by **$(c_j, r_j) = (| x_c-x_b/(x_t-x_b)/m | , |y_c-y_b/(y_t-y_b)/m|)$**.Finally, SP sends the set of selected PO is back to TU in the following form:

$<POI_j = (C_j, l_j, \sigma_j)>$, where j = 1… np.

Step 4. Response computation (by the user). Suppose that there are μ matched POIs received by the user. For each of these matched POIs, say hl$_j$, σ$_{ji}$, the user decrypts lj using encryption key K and gets access to the exact location (x_j, y_j) of the POI. In the running example (Fig. 2b), the user receives five POIs from SP, where the range query answer includes two POIs, i.e., p4 and p6.

Performance Analysis



(a): Range Query Size vs. Query Processing Time (ms)

Fig. 3.2.2 (a) shows the time taken to process range queries at the Service Provider i.e., searching the encrypted DGS at the SP. The range query sizes vary from 5% to 30% and the query processing time is measured in milliseconds (ms) for all DGS approaches. The most efficient in terms of time is DGS, due to the fact that in this approach, the DGS is searched only once for all Hilbert cells included in the query. DGS is the most time-consuming as a range of cells have to be checked in each packet for every cell. As the size of the query increases, the time taken to process the query also increases. The difference between DGS approaches is significant when the query range extent is greater than 5%, as this increases the number of times the DGS has to be searched.

AES with EX-OR Operation:

The SP generates encryption key K randomly and encrypts the query results with an appropriate symmetric block cipher (we have used the AES for encryption purposes). The result is an encrypted query results (C). Subsequently, the SP generates keys K1and K2 for every user and deletes K, it means not stored in anywhere. The following process will be explain, how to share the keys to users.

User Key Share K1: K1 is computed for each of the users as follows:

K2=Random ().nextInt (100000),

K1 = K ⨁ K2.

Where K1 can send to requested user email and K2 is store in database.

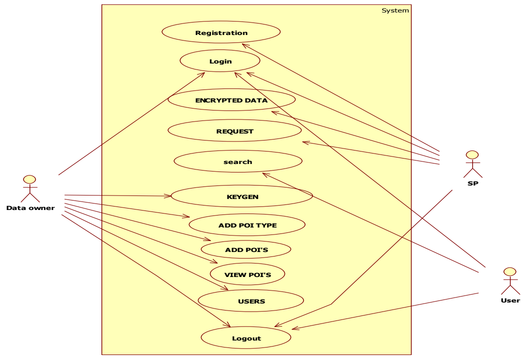
User Decryption Query Results:

K = K1⨁ K2.

Where user can enter K1 key which is sent to user email and K2 can be retrieve from database with user identity and performing the EX-OR operation between two keys then they get original key K and decrypt the encrypted query results with encryption key K.

IV. SYSTEM DESIGN

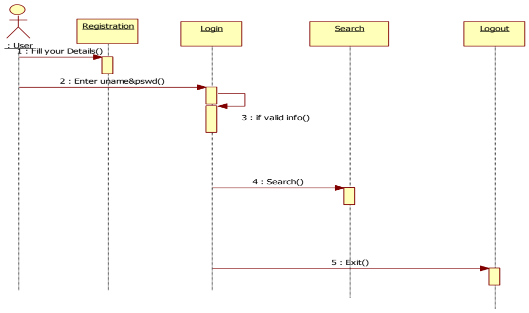
UTILIZE CASE DIAGRAM



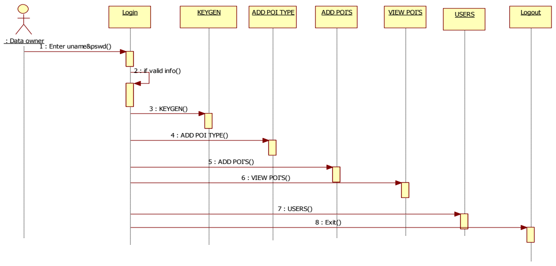
Project User Case

Description:-A use case diagram inside the Unified Modeling Language we utilized as a part of our Project Development is Star (UML) could be a kind of social outline depicted by and created utilizing a Use-case examination. Its motivation is to blessing a graphical format of the good judgment gave by a framework to the degree performing pros, their objectives (tended to as utilize cases), and any conditions between those utilization cases. The most clarification behind a utilization case graph is to demonstrate what structure limits are played out that on-screen character.

SEQUENCE DIAGRAM



User Sequence



Data owner Sequence

Description:-A social affair outline in Unified Modeling Language we utilized as a part of our Project Development is Star (UML) could be a sensibly affiliation diagram that shows anyway outlines work with each other and in what engineer. It's a maker of a Message Sequence Chart. Movement charts are frequently known as occasion plots, occasion conditions, and fleeting methodology diagrams.

V. CONCLUSION AND FUTURE WORK

Database outsourcing is a prominent worldview of distributed computing. In this work, we are endeavoring to accomplish a harmony between information confidentiality at the server and efficient question preparing. We propose to change the spatial database by applying the Hilbert curve. Next, we make it more secure by applying encryption to the changed information. We define a few assault models and demonstrate that our plan gives solid security against them. This permits a harmony between the security of information and quick reaction time as the questions are handled on encoded information at the cloud server.

Besides, we contrast and existing methodologies on expansive datasets and demonstrate that this approach diminishes the normal inquiry correspondence cost between the approved client and specialist organization, as just a solitary round of correspondence is required by the proposed approach. Therefore, the double change strategy secures the information as well as empowers the confirmed clients to recover spatial range inquiry reactions efficiently.

In this paper, we proposed a dynamic network framework (DGS) for giving protection safeguarding ceaseless LBS. Our DGS incorporates the specialist co-op (SP), and cryptographic capacities to partition the entire question preparing errand into two sections that are performed independently by SP. We additionally composed effective conventions for our DGS to help both constant k-closest neighbor (NN) and range inquiries. To assess the execution of DGS, we contrast it with the best in class procedure requiring a TTP. DGS gives preferred protection ensures over the TTP plot, and the trial comes about demonstrate that DGS is a request of greatness more productive than the TTP conspires, regarding correspondence cost. As far as calculation cost, DGS additionally dependably beats the TTP conspire for NN inquiries; it is equivalent or marginally more costly than the TTP plot for extend questions.

VI. REFERENCES

[1]. B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting mysterious area questions in portable situations with PrivacyGrid," in WWW, 2008.

[2]. C.- Y. Chow and M. F. Mokbel, "Empowering private consistent questions for uncovered client areas," in SSTD, 2007.

[3]. B. Gedik and L. Liu, "Securing area protection with customized kanonymity: Architecture and calculations," IEEE TMC, vol. 7, no. 1, pp. 1– 18, 2008.

[4]. M. Gruteser and D. Grunwald, "Mysterious Usage of Location-Based Services Through Spatial and Temporal Cloaking," in ACM MobiSys, 2003.

[5]. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Avoiding area based character derivation in mysterious spatial inquiries," IEEE TKDE, vol. 19, no. 12, pp. 1719– 1733, 2007.

[6]. M. F. Mokbel, C.- Y. Chow, and W. G. Aref, "The new casper: Query handling for area administrations without trading off protection," in VLDB, 2006.

[7]. T. Xu and Y. Cai, "Area namelessness in persistent area based administrations," in ACM GIS, 2007.

[8]. "Investigating authentic area information for obscurity protection in area based administrations," in IEEE INFOCOM, 2008.

[9]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.- L. Tan, "Private inquiries in area based administrations: Anonymizers are a bit much," in ACM SIGMOD, 2008.

[10]. M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Productive unmindful expanded maps: Location-based administrations with an installment dealer," in PET, 2007.

[11]. R. Vishwanathan and Y. Huang, "A two-level convention to answer private area based questions," in ISI, 2009.

[12]. T. Xu and Y. Cai, "Feeling-based area security assurance for locationbased administrations," in ACM CCS, 2009.

[13]. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Request safeguarding encryption for numeric information," in ACM SIGMOD, 2004.

[14]. E. Mykletun and G. Tsudik, "Accumulation questions in the database-as-aservice demonstrate," in DBSec, 2006.

[15]. A. Khoshgozaran and C. Shahabi, "Dazzle assessment of closest neighbor questions utilizing space change to safeguard area protection," in SSTD,2007.

[16]. W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN calculation on scrambled databases," in ACM SIGMOD, 2009.

[17]. M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Empowering seek benefits on outsourced private spatial information," VLDB Journal, vol. 19, no. 3,pp. 363– 384, 2010.

[18]. B. Palanisamy and L. Liu, "Mobimix: Protecting area security with blend zones over street systems," in IEEE ICDE, 2011.

[19]. S. Mascetti, C. Bettini, X. S. Wang, D. Freni, and S. Jajodia, "ProvidentHider: A calculation to safeguard recorded k-namelessness in LBS," in MDM, 2009.

[20]. R. Dewri, I. Beam, I. Beam, and D. Whitley, "Inquiry m-Invariance: Preventing question divulgences in consistent area based administrations," in MDM, 2010.

[21]. B. Hoh, T. Iwuchukwu, Q. Jacobson, D. Work, A. M. Bayen, R. Herring,J. C. Herrera, M. Gruteser, M. Annavaram, and J. Boycott, "Upgrading protection and exactness in test vehicle-based movement observing by means of virtual outing lines," IEEE TMC, vol. 11, no. 5, pp. 849– 864, 2012.

[22]. A. Pingley, N. Zhang, X. Fu, H.- A. Choi, S. Subramanian, and W. Zhao, "Assurance of question protection for nonstop area based administrations," in IEEE INFOCOM, 2011.