iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.46011

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

A Survey on Approach for Efficient and Secure Data Encryption Scheme for Spatial Data

Sneha D P[1], Sumaiya Siddique[2]
[1, 2]*Maharaja Institute of Technology Mysore*

Abstract: ***In spatial applications location data of the users continuously processed in un-trusted servers, this may cause to user privacy. Location information of the users is very sensitive data like their meeting information, residential and official location information's. In present solutions of the un-trusted servers may have the several problems and limitation like data security, data availability, request processing etc. In general cloud environment provides lot of features to solve many problems with low cost. Elastic cloud environment will provide successful solutions for spatial data and user's data. Many security algorithms were proposed and for cloud data security and many Locations Based services (LBS) security functionalities were proposed in many researches. In this paper we survey on various secure location-based techniques and cloud data security architectures.***
Keywords: Spatial Data, Location based service, Euclidean distance, Order-Retrievable Encryption, Dynamic Grid System.

I. INTRODUCTION

In location-based applications the data increases very rapidly of the user locations. The LBS services set up with un-trusted services for storing the data and process the data. By the advantages of cloud computing, so many organizations outsourcing their data in to the cloud for various reasons. Cloud computing mainly provides data confidentiality, data availability, add resource sharing. In recent years the data of the LBS services can't handle by the un-trusted services. They want to move the data and use the services of the cloud to get the user location data confidentiality and availability. By using of the cloud computing, we can elastic the cloud storage even for small scale organizations.

In recent years cloud computing emerging many secure algorithms to secure the users data for getting the user trust and confidentiality. But in the cloud computing, many researches available only for secured the data of user information's like images, files, videos etc. In recent trends cloud computing focus on secure the user location data. Because of normal user data and location data are completely different. User location data depends on user co-ordinate information. Locations we need to retrieve and updated continuously because of user's changing their locations continuously and getting the results according to the user location continuously.

In location-based service cloud computing focus on security for user location data like latitude and longitude data. Here mostly data owner and data owner-based architecture is popular for LBS in cloud computing. Data owners will store the location information for data users. Data users will request the location information and get the nearest location information according the users current location.

In spite of numerous advantages of distributed cloud computing we are redistributing our information into the cloud. The information may delicate data like messages, contact data, wellbeing records, and authority undertaking records. Many cloud specialist organizations previously took the security testing issues of clients and keep the information of the clients safely and give the verification to information to get to appropriately purchase the validated clients. Many cloud benefits additionally give the encryption documentations or innovations for the information security. On account of the scrambled information a few tasks troublesome in cloud like readiness of inquiry record, multi watchword search and so forth. In any case, because of huge measure of information in the cloud we require methods like which we are utilizing in semantic web.

In this survey we focus on the location-based service security survey and functionalities survey and as well as cloud computing techniques of the data owner and data user architecture issues and techniques. In the first we survey on Grid System is completely focus on the query the data server about spatial data which are nearest to his/her locations so how user can secure own location for getting the nearest results. Next, we survey on ORE schema, in this how can users sharing location in location based social networks securely to friends in social groups that location-based service features and techniques we covered here. Last of the LBS survey we survey on the nearest neighbor results, for this which is best technique to calculate the distance among the two locations. Next completely focus on the cloud search techniques in the architecture of the data owner and data user. First, we survey on the Searchable Encryption on the cloud for encrypted data using public key encryption.

We list out the proposed steps of the Searchable Encryption. Next, we survey on the Keyword Search with Access Control architecture is for example of the public key encryption for data sharing between data owner and data user, and data owner set access policies like by whom will access for that there is no need to search the data. At the end we survey on Weighted Search Index, this procedure is data owner will characterize weighted score for keyword information by the data which owner uploading.

II. SURVEY

A. *Dynamic Grid System*

Roman Schlegel et al. [11] proposed a concept for secure location-based service called Dynamic Grid System (DGS) for secure location sharing. This concept includes the Query Server (QS) and location Service Provider (SP) and secure sharing service called KDC. This concept is proposed to overcome the problem of Trusted Third Party problem in LBS [8][9][10].

In this user send query request to Query Server and QS will encrypt the query and forward to Service Provider. According to the user location Service Provider will return k-nearest neighbor results. User will prepare the query according to the grid system and generate the two dummy locations (x_t,y_t) and (x_b,y_b) instead of exact location (x_u,y_u).

Algorithm of DGS

Input: User location (x, y), POI data P

Output: User's POI Query data U(P).

Initialization:

i. User Select POI Type P(t), QS Query Server, SP Service Provider.

ii. User set location, defined x, y (Current exact Location).

let $x_u,y_u \in U$,

Map.getBounds(x_u,y_u)

return(x_b,y_b), (x_t,y_t) where b- bottom, t- top

Key Derivation Function KDF()

returns *k* (random key)

Enc(query) = IBE(P(t), k, (x_b,y_b), (x_t,y_t)) // At User side

Enc(query), User data of U ***fwd to*** QS.

Create ID for Query and ***fwd*** Enc(query) to SP

Decrpt(query) at SP,

get (x_c,y_c)= Map.getCenter((x_b,y_b), (x_t,y_t));

while data != nulll

get POI P ∈ P(t),

sort based on dist,

create Query Set U(p).

end while

return Query Set U(p) to QS

At QS, fwd Query Set to User

Decrpt(query set U(P)) at USer,

B. *ORE Schema*

Roman Schlegel et al. [7] proposed a concept in LBS Privacy-Preserving Location Sharing Services [4][5][6] using to share locations of users in online social networks. In this framework proposed new schema called Order-Retrievable Encryption (ORE). This concept is motivated by three-layer architecture of location sharing service of user, TTP, and Database server. Here locations share transfer between users using TTP. The data may have leak in this concept, to overcome this Roman Schlegel et al. proposed PPLSS using ORE scheme.

Here User query location is Q= x_q,y_q;

User requested query,

C ← QGen(SK_G, Q, dist); //Encrypted Query

Where SK_G ← Symmetric key (d+1) x (d+1) invertible matrix. (Sharable to Group members).

According to the SK_G the data decrypt and calculate distance using Euclidean distance. En

C. Euclidean Distance

Euclidean distance is very popular algorithm [12] traditional algorithm for calculating distance between two co-ordinates in geo-metric space. It is also become very famous algorithm for calculate distance between two geo graphical co-ordinates (latitude and longitude).

In the geometry context, one dimension is established by using one metric by taking two points of the line and get the one origin. The distance from the origin and two points is defined as positive direction. In the following algorithms x,y are latitude and longitude values of the user, and x` and y` are the latitude and longitude values of the object may another user or a location of the point.

Euclidean distance Algorithm

Input: x, y, x', y'

Output: Distance d

Initialization

I. theta = y - y';

II. x, y - User Coordinates

III. x', y' - Object Coordinates

Distance d = sin(deg2rad(x)) * sin(deg2rad(x')) + cos(deg2rad (y)) * cos(deg2rad(y')) * cos(deg2rad(theta));

d = arccosine(d);

d = rad2deg(d);

Calculate deg2rad(deg)

return (deg * π / 180.0);

Calculate rad2deg(double rad)

return (rad * 180 / π);

return d;

D. Searchable Encryption

Searchable Encryption proposed by Baojiang Cui et at [14], on the cloud for encrypted data using public key encryption. The suggested Searchable encryption measures are listed below.

1) *Setup(Ω):* While uploading the data at data owner side this step will execute. Based on the data owner properties a secure key will generate by taking the security parameters **Ω**

$$Setup(\Omega) \rightarrow (\Omega(S), \mathscr{b})$$

Where, *S* is a list of data owners. $S \subset \{1,2,3,\dots n\}$;

2) *Encrypt (c, β):* In this step the data owner performs attribute encryption while uploading the data, data owner will encrypt the data $\boldsymbol{\beta}$ using secure key ∂ which is generated by the data owner properties or attributes. While uploading the data, data owner will generate the search keywords for data searching at user side. Those search keywords *k* will form search index, and search index will encrypt by $\boldsymbol{\beta}$. The encrypted search index denoted as *I`*.

$$\boldsymbol{\partial}' \leftarrow Encryt(\boldsymbol{\partial}, \boldsymbol{\beta})$$

3) *Trapdoor(u_k):* Trapdoor is a process in between user and cloud, generally trapdoor will take care about the user search request. When a Trapdoor is raised, a search query will be formed which strikes the cloud.

4) *Test (u_i, Ω´, ∂):* This test is performed at the cloud side by the request of the Trapdoor. Cloud will encrypt search keywords of the search request of the user, and match with the *I`*, If keyword u_i is match with search keywords then cloud will return the data d.

$$d \leftarrow match(ui, I`)$$

E. KSAC: Keyword Search with Access Control

Zhirong Shen et al. [13] proposed Keyword Search with Access Control architecture is for example of the public key encryption. In this type of encryption, we don't need of encrypted search index, here there are two keys will available of MK and SK, Master key (MK) for the data owners and Secret Key (SK) for the data users. Data owner upload the data with encryption using MK and while uploading the data date owner set the access policies like by whom will access, it consists data area location, and the position of the user should access in hierarchical level. This step we can call it as setting the access policies for data. This condition will user has to be satisfied in parent to child order or root to leaf order like fig 1. According to the user parameters each and every data will verify the access policies using AND, OR operations, if admin set the data access location for all the OR will perform and data owner set any particular position for accessing the data then AND operator will perform.

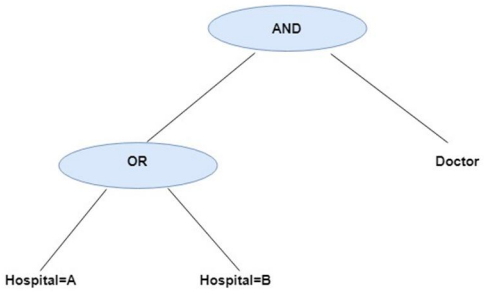


Fig.1 Access Policies Example.

In Fig. 1, AND is Root node, so the accessing user should only Doctor and left side OR operator for location then access policies is User should be a doctor from any hospital.

F. Weighted Search Index

In Weighted Search Index, proposed new method for looking through system in scrambled information. Principle thought of this procedure is data owner will characterize weighted score for keyword information by the information, and ordered catchphrases and weight score of the document in the record document, called Weighted Search Index and re-appropriate the list into cloud. Using of WSI data users will directly search using keywords, and get coordinated positioned results from the cloud. For figuring the positioning in the cloud, no compelling reason to play out any positioning instrument at runtime of the client search, in light of our WSI has positioned record of all document's information. Like a parallel tree, every one of the watchwords and scores of information organized appropriately.

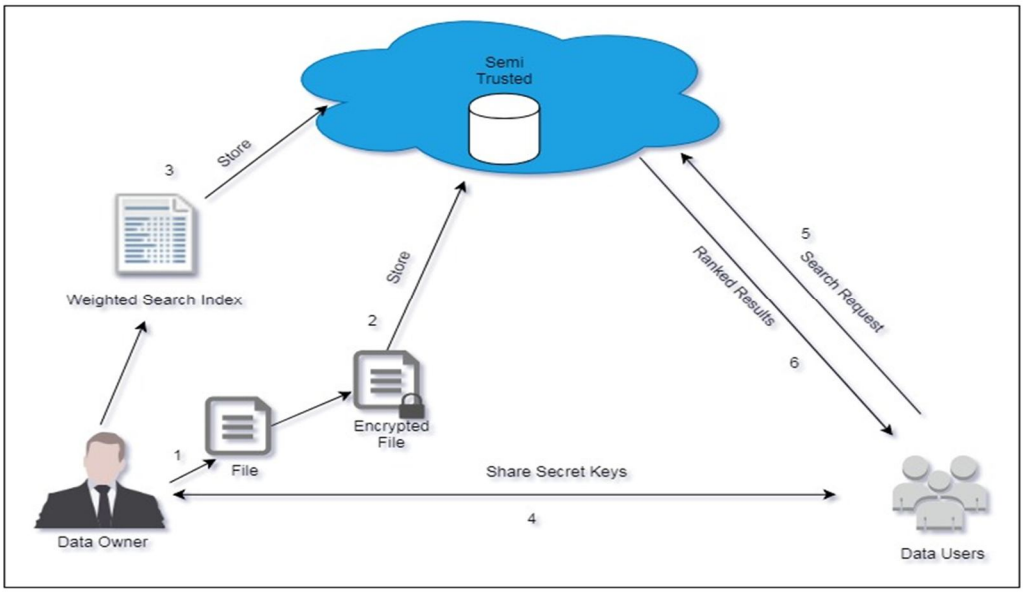


Fig 2: WSI architecture

Fig 2 is an architecture module of the weighted search index cloud architecture. Here there are three main modules, data owners who upload the data, data users who use the data and semi trusted cloud who stores the data. In this architecture we proposed thing developed at the side of data owner. Data owner while uploading the data he/she has to prepare the keywords for that data. After generating the keywords application will calculate the TF-IDF score for the keywords in terms of the data. That keywords with weighted score will for Weighted Search Index. According this WSI user will search from on it and get the ranked search results.

G. Fuzzy Keyword Search

In this strategy, it is another sort of pursuit approaches in cloud computing. They center around giving a course means search bearing to information clients that how to look through information and best information recovery like semantic web keyword recommendations type. Fuzzy Keyword search fundamental objective is setting up the quest record for document information as per the document information utilizing term recurrence and alter remove. Term Frequency is idea of discovering terms which are happened all the more every now and again in the record information, this is utilized for finding the more significant keywords extraction in document information which we are redistributing to the cloud. Edge Distance is an idea of checking and looking through proper significant catchphrases in a file or any arrangement of watchwords not in record information. In Edit Distance we can do such activities like Insertion, Deletion and Replacing to discover pertinent watchwords. This is most helpful instrument to catchphrase search, spelling revision and watchwords proposals.

Input: keyword1 = "cloud", keyword2 = "clouds"

Output: 1

We can convert keyword1 into keyword2 by **inserting** a character's'.

Input: Keyword1 = "paper", keyword2 = "papar"

Output: 1

We can convert Keyword2 into Keyword1 by **replacing** character 'a' with character 'e'.

Input: keyword1 = "Cloud's", keyword2 = "Cloud"

Output: 2

We can convert keyword1 into keyword2 by **deleting** a character "'s".

Fig 3: Edit Distance

Before outsourcing the data, data owner should prepare the index using Edit distance features and technique.

$$\text{Files: } D \leftarrow \{d_1, d_2, d_3 \ldots . d_n\}$$

$$\text{Encrypted Files: } \mathbb{E} \leftarrow \{e(d_1), e(d_3), e(d_3) \ldots . e(d_n)\}$$

$\mathbb{i}$ are index words of the files a $\mathbb{F}$,

$$\mathrm{I} \leftarrow \{i_1, i_2, \mathrm{i}_3 \ldots . i_n\}$$

$\mathbb{W}$ is distinct TF words of the file a d,

$$\mathbb{W} \leftarrow \{\mu_1, \mu_2, \mu_3 \ldots . \mu_n\}$$

Edit Distance of Keyword selection,

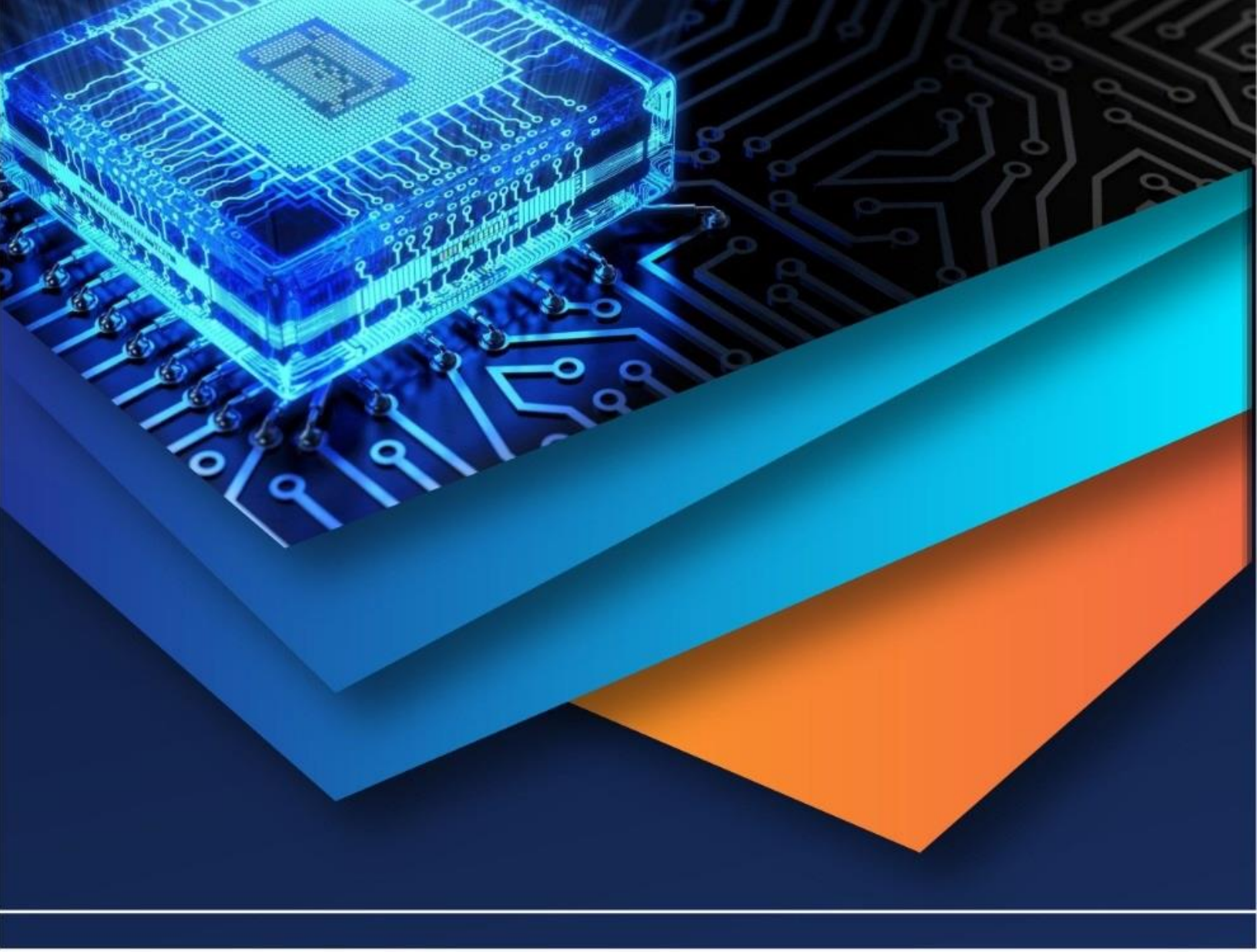
$$\mathbb{ed}(i, \mu_n) \leq threshold\ \theta$$

III. CONCLUSION

In this survey, we survey on the two types of domains, one for location-based search schema for location sharing literature and another for data sharing and searching in the model of both data user and data owner architecture. For LBS purpose on we survey on Dynamic Grid System, ORE schema. Euclidean distance and for Data owner and user model architecture search techniques we survey on Searchable Encryption, Keyword Search with Access Control.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in WWW, 2008.
[2] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.
[3] B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.
[4] L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers, "From awareness to repartee: Sharing location within social groups," in Proceedings of the ACM Conference on Human Factors in Computing Systems, 2008.
[5] E. Toch et al., "Empirical models of privacy in location sharing," in Proceedings of the ACM International Conference on Ubiquitous Computing, 2010.
[6] S. Consolvo et al., "Location disclosure to social relations: Why, when, & what people want to share," in Proceedings of the ACM Conference on Human Factors in Computing Systems, 2005.
[7] R. Schlegel, C.-Y. Chow, Q. Huang, D. S. Wong, "Privacy-preserving location sharing services for social networks", *IEEE Trans. Services Computation.*, vol. 10, no. 5, pp. 811-825, Sep./Oct. 2017.
[8] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in WWW, 2008.
[9] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.
[10] B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008
[11] Schlegel, R., Chow, C., Huang, Q., Wong, D.: User-defined privacy grid system for continuous location-based services. Trans. Mob. Comput. 14(10), 2158–2172 (2015)
[12] Leo Liberti, Carlile Lavor, Nelson Maculan, and Antonio Mucherino, Euclidean Distance Geometry and Applications, Leo Liberti, Carlile Lavor, Nelson Maculan, and Antonio Mucherino SIAM Review 2014 56:1, 3-69
[13] Zhirong Shen; Jiwu Shu; Wei Xue (2017) Keyword Search With Access Control Over Encrypted Cloud Data, *IEEE Transactions*, 17(4) 858 – 868, DOI: 10.1109/TCC.2017.2709316
[14] Baojiang Cui, Zheli Liu, Lingyu Wang (2016) Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, *IEEE Transactions*, *65*(8), 2374 – 2385, DOI: 10.1109/TC.2015.2389959
[15] Xiaofeng Ding, Peng Liu and Hai Jin, (2017), Privacy-Preserving Multi-keyword Top-kSimilarity Search Over Encrypted Data, *IEEE Transactions*, 16(2), 344 – 357, DOI: 10.1109/TDSC.2017.2693969
[16] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in ACM SIGMOD, 2009.
[17] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," VLDB Journal, vol. 19, no. 3, pp. 363–384, 2010.
[18] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix zones over road networks," in IEEE ICDE, 2011.
[19] S. Mascetti, C. Bettini, X. S. Wang, D. Freni, and S. Jajodia, "ProvidentHider: An algorithm to preserve historical k-anonymity in LBS," in MDM, 2009.
[20] R. Dewri, I. Ray, I. Ray, and D. Whitley, "Query m-Invariance: Preventing query disclosures in continuous location-based services," 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. Ban, "Enhancing privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines," IEEE TMC, vol. 11, no. 5, pp. 849–864, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY