

Spread Identity to Achieve Location Privacy in Query Search

Padmaja M Deshpande, Raghvendra Sharma, Swati Sinha

Cite as: Deshpande, P. M., Sharma, R., & Sinha, S. (2024). Spread Identity to Achieve Location Privacy in Query Search. International Journal of Microsystems and IoT, 2(2), 607–613. <https://doi.org/10.5281/zenodo.10809121>




© 2024 The Author(s). Published by Indian Society for VLSI Education, Ranchi, India



Published online: 20 February 2024



Submit your article to this journal: 




Article views: 



View related articles: 



View Crossmark data: 

DOI: <https://doi.org/10.5281/zenodo.10809121>

Full Terms & Conditions of access and use can be found at <https://ijmit.org/mission.php>



Spread Identity to Achieve Location Privacy in Query Search

Padmaja M Deshpande¹, Raghvendra Sharma², Swati Sinha¹

¹Department of Electronics and Communication Engineering, MGM's College of Engineering and Technology, Navi Mumbai, India

²Department of Electronics and Communication Engineering, Amity University Gwalior, Madhya Pradesh, India

ABSTRACT

In present scenario of 4G, 5G communications and IoT development, Location based services are playing important roles for providing the comfort to the consumers. These services provide the nearest locations or location information, based on the user present location and query being asked for. Multiple times queries being asked from the same user can give access regarding the user's day to day activities/habits and leakage of any important information related to his job(s)/work. This will make the user vulnerable to cyber/physical attacks by any social commotion. Multiple methods have been proposed to preserve the users' location privacy. But these methods mostly rely on fixed Trusted Third Party (TTP) and suffer from single point breakdown. For Query privacy few methods have been proposed but is complex for implementation. We propose a novel query privacy method with dynamic allocation of a small group of TTPs which are in the local proximity of the inquirer. In the proposed model, the spread identity concept has been applied to the mobile platform. It has got feature of dynamically selecting a group of people as TTPs, located anywhere in the globe. This dynamic allocation of TTP will give complete query privacy to the user, and at the same time will make more difficult for the hackers to identify the user's location.

KEYWORDS

Trusted Third Party, Spread Identity, Location Based Servers, Query privacy

1. INTRODUCTION

Until last decade, Location Based Services (LBS) for mobile devices was a subject of research. In recent few years, with the advent of wireless technology and IoT, its implementation became a reality[1].LBS is a mobile application which can be downloaded from Google Play Store in any smart phones. This application tracks the user real time geo coordinates and reveals the sensitive information like his/her daily movements, personal choices/lifestyle, health and so on[2].

Location-Based Services, or LBS, are now an essential aspect of our everyday existence. While using LBS for convenience, users run the risk of losing their privacy because any information about them is stored on an untrusted LBS server, which can track them or give their personal information to outside parties. Through LBS query submission, users can take advantage of the convenience that LBS offers. However, because the untrusted LBS server is privy to all of the user's information—including their whereabouts, the queries they ask, what they are doing, and so on—he is able to track users in a number of ways and divulge their personal information to outside parties. Thus, we must give user privacy more consideration[3]. Over the past few years, numerous strategies [4], [5] have been put forth in the literature to address the privacy issue. A centralised location anonymizer is used to submit an LBS-related query to the LBS server in order to achieve k-anonymity [4], [5]. This enlarges the queried location into a larger Cloaking Region (CR), covering many more users (e.g., $k - 1$) geographically. Consequently, the untrusted LBS server faces difficulties in differentiating the user's actual location from the $k - 1$ dummy locations. These k-anonymity methods do have some restrictions, though. Initially, it is primarily dependent on the location anonymizer, which has a single point of failure. All users' privacy will be at risk if the adversary manages to take control of it. Due to the location anonymizer's requirement for

all submitted queries, there is also a performance bottleneck. Secondly, while k-anonymity can be attained by using dummy locations, choosing such locations can be difficult. A virtual circle/grid model [9] or a random walk model [7], which generates dummy locations, are based on the assumption that the adversary has no side information [10], [11], such as the user's query probability related to location and time, and information related to the query's semantics, such as the user's gender and social status.

The LBS server, for example, could be an adversary with such side information, so these dummy generation algorithms might not function properly.

An adversary could easily filter out dummy locations that are poorly chosen, such as those that fall in unlikely places like lakes, swamps, or Rocky Mountains. As a result, it is challenging to successfully ensure the required k-anonymity

The service providers, application developers and the advertisers can easily track the users' location using LBS[3]

Presently, the data rich LBS servers are using the data for commercialization purposes[4], [5], [6], [7].

There are various methods proposed for location privacy. Few of them to be mentioned are Obfuscation based approach[7], Cache-Based Privacy-Preserving (CBPP)[8], [26], block chain[27], [28] K-anonymity based privacy approach [9] etc.

An anonymous communication technique using dummies for location-based[10], [11].

LBS is split into two categories: continuous query and snapshot query. The term "snap query" describes a query in which the user actively enters the query conditions, such as "query the petrol stations nearest to me now." Continuous inquiry refers to the provision of location services by the location service provider (LSP) in response to ongoing changes in the user's position, such as "search for the closest petrol stations while driving." Numerous location-based applications have been created as of late[12]. Applications that are frequently used include map programmes (like Google Maps), interest point finders (like Meituan), location-aware services (like Foursquare), etc. When utilizing these applications, users must reveal their location

information[13].

Users must send location information to the LSP in order to, for instance, "query which Meituan takeaways are near me." Users may receive better location services through LBS if they disclose more location information. The attacker's inference assault on the location data, however, can examine individuals' private information, like their employment and health status[14]. So, finding a balance between location-based services from LBS and user privacy leakage has become a pressing issue[15], [16].

The method proposed in this paper, is based on spread identity. using Geo-specific information, for query-based location privacy. In this method, a close-knit group of 100 users are created. The users collaborate among each other using P2P (Peer

2. SPREAD IDENTITY CONCEPT

A Operation by User group to protect privacy

This section explains how a user group operates while handling location-based queries while maintaining location privacy. For this, a user group of 50–300 (usually 100) users is created. All of these users must have the mobile app "query Anonymizer" installed on their phone. This is how it issued. Take the scenario where a group member (enquirer) requests an LBS service, often asking for information on the "nearest places with certain attributes." Any LBS-related inquiry is always forwarded by the inquirer through a "randomly selected" group member. The group member receiving the question, known as the "forwarder," is required to forward the inquiry as though it were his idea in the first place. Either the forwarder would look for the response in the LBS server or would receive a response from the relevant LBS application. This response must list numerous locations that meet the query criterion.

The list must also include the locations' latitude and longitude, the forwarder's current position, and their names with optional qualifiers. The original inquirer receives a copy of this list along with the relevant information. The 'location and query Anonymizer' mobile app's steps are shown below

Following are the steps of Query Anonymizer mobile app: basic functionality flow

- 1 Form a group of people (members) intending to avail the facility (say 100)
- 2 **Initialization:** Maintain the login status of the user. IP address/ Mobile No./ Current status
- 3 Check whether the LBS query to be raised?
- 4 If yes then go for query program
- 5 Check whether the LBS query has come?
- 5 If yes then go for response program

The list of points of interest together with their geo coordinates is now available to the inquirer. These locations are closer to the forwarder, though. The distances of every location in the list from the inquirer are calculated using the Euclidean distance concept and vector calculations. Multiple forwarders may be used to repeat this process.

In this method, the inquirer receives information that is identical to a direct enquiry while also concealing his or her location by dispersing it across several people. Due to the fact that many members of the aforementioned group ask the same user's query repeatedly, this also gives the inquirer's identify

to Peer) environment[7]. When a user needs LBSs, he sends his query to anyone of his nearest neighbours. The neighbour searches for the reply and shares with the user, along with the latitude and longitude of the locations. The user then uses the Euclidean distance formula to compute the nearest location of the query being asked. In this way, the user gets the reply, without his/her identity being revealed to the LBS[20].

The flow of work is as follows: Section II presents the proposed spread Identity concept. Section III details about the mobile application Query-Anonymizer. Section IV gives the evaluation results. Section V gives the conclusion and future scope.

secrecy.

It should be noted that some locations that are far from the forwarder but close to the inquirer might be overlooked. In LBS, this is known as "loss of information or the loss in quality." For the vast majority of real-world applications, this loss is anticipated to be reduced and at an acceptable level.

Each user device needs to have a forwarding subroutine and a query subroutine in order to carry out the aforementioned action. The logic flow for both of the routines is described in the following sections.

2.1 Subroutine Response

It should go without saying that every user must be able to function as a forwarder. The "Forwarder Sub-routine" will first determine whether the user is a member of the TTP group that has been formed, and it will only respond to user-member questions. The forwarder transmits the LBS query to the proper server or application, as specified in section, and then receives the result. The following format may be used to describe how the response is received.

$R_{U_i} = \{ L_{U_i}(\phi, \lambda)_i, t \}$, for $i=1$ to n . Here, L_{U_i} are the searched destinations, along with its respective Latitude ' ϕ ', and Longitude ' λ ', and ' t ' is the time when the response is being sent.

The following are the steps for Response subroutine

1. Verify the origin of the query—is it coming from a group member? If yes
- 2 Process the location-based server request and get.
- 3 Make a list of the locations you searched, along with their corresponding geo coordinates, and send it to the asker.

2.2 Query Forwarder Subroutine

A user sends LBQs (Q) to anyone of the remaining 99 users, along with his geographical coordinates, $Q_{UN} = \{ Q, U\phi, U\lambda, t \}$ to seek the answer, where Q_{UN} is the query sent by the user 'N', ' $U\phi$ ' is the user's latitude, ' $U\lambda$ ' is the user's longitude and ' t ' is the time when the query is being sent.

After receiving the response from the Responder subroutine, which consists of multiple locations name, along with their respective latitude (ϕ) and longitude (λ), the user calculates the distance of the locations wrt to his/her present geographical coordinates using Euclidean distance.

The length of the line segment that separates two points in Euclidean space is known as the Euclidean distance in mathematics. It is sometimes referred to as the Pythagorean

distance because it can be computed using the Pythagorean theorem and the Cartesian coordinates of the points. The smallest distance between pairs of points from two objects is commonly used to define the distance between two objects that are not points. There are known formulas for calculating the separations between various kinds of objects, including the separation between a point and a line. The notion of distance has been extended to abstract metric spaces in advanced mathematics, and distances other than Euclidean have been examined.

Euclidean Distance [14] formula explained below equation 1 :

$$Ed = \sqrt{(\phi_2 - \phi_1)^2 + \left[\frac{\cos(\phi_2) + \cos(\phi_1)}{2} \right] \times (\lambda_2 - \lambda_1)^2} \quad (1)$$

Where, ϕ and λ are the latitude and longitude in radians.

Following are the steps for the Forwarder subroutine.

1. Write the query program.
2. Make a query for a location-based service.
3. Send the inquiry to a random member of the group after choosing that person.
4. Observe for a response: Format for response: Location Name, Lat/Long Geographic Coordinates.
5. Determine the distance in Euclidean terms from the current location.
6. Select a distance below the cutoff point

3. MOBILE APPLICATION

To provide LBS(location based service) with source anonymity, the Query Anonymizer (QA) smartphone application was created. The flutter and dart languages are used to create the mobile application. It is predicted that those who want anonymous location search would organize a user group and utilize the QA mobile application to carry out the plan cooperatively. The QA mobile application must be installed on each member's respective mobile device. A succinct explanation of the same is provided in this section.

A group member initially has two ways to post an LBS query and see if anyone has asked to relay the question. The user can utilize the 'Query' or 'Response' program by choosing the appropriate menu item. Initially a group member has two options of posting a LBS query and check whether any request to relay the query is received. The user may select appropriate menu option use 'Query' or 'Response' program. Fig. 1 shows the initial mobile screen, where the user has to login into his/her account.

Fig 2 and Fig 3 gives Query and response program screens respectively. It may be noted the Query program has 'send invitation' button, acceptance notification and a response window with timeout). On the other hand, the Response program has a live query notification and acceptance button and query completed indication with time out.

In Fig 3 the prospective places listing with GPS coordinates is being seen. Using these GPS coordinates the inquirer calculates the location distance wrt his/her present geo coordinates. And selects the nearest one, as desired. This is shown in fig 4. In this instance, Prathmesh requests that Sahil send the theatres in Andheri, as indicated by the query

programme in Figure 2. The number of theatres in Andheri, along with the corresponding latitude and longitude locations, will then be sent by Sahil to Prathamesh, as indicated in figure 3 (Response program screen). Lastly, Prathmesh will compute the closest locations in ascending order using the Euclidean distance formula at his end, as shown in figure 4 (forwarder screen).

Fig. 1 Initial mobile screen

Fig. 2 Query program

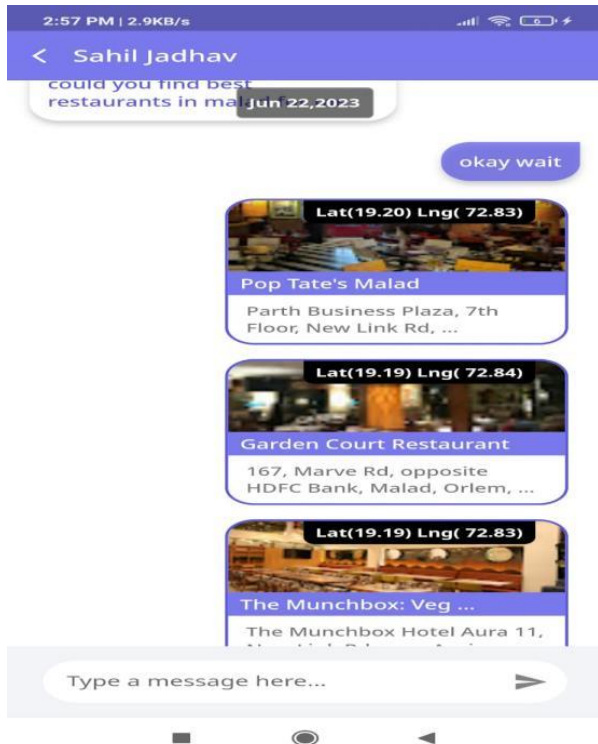


Fig. 3 Response program screen

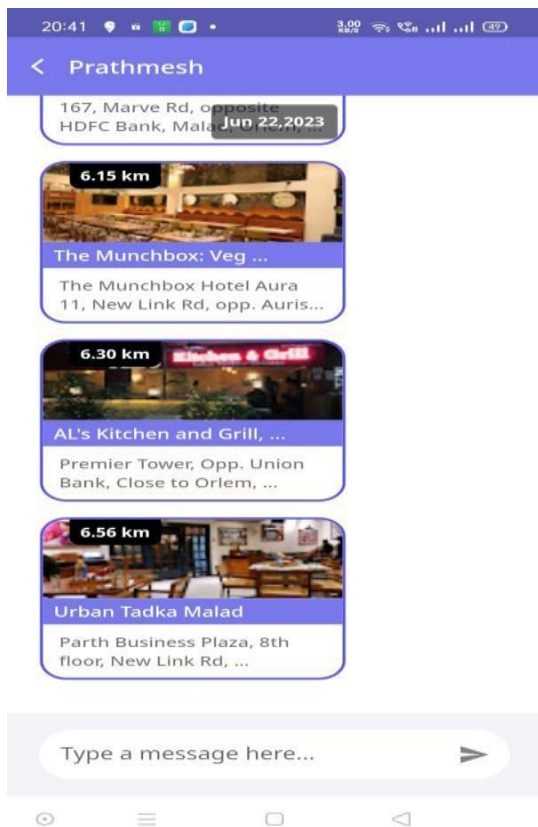


Fig. 4 Forwarder screen (After the query has been answered)

4. RESULTS

This section provides a graphic of the LBS outcome as well as the simulation exercise outcomes. This data will be visualized on a Google map in the application's final form. In Fig. 5, locations of the group members are denoted by hollow dots with the names M1 to M6, while the prospective locations are denoted by an identifiable triangular symbol. It can be observed that 7 potential locations have been determined. As a result of the relatively great distance, 4 of them are extremely valuable and 3 are of lesser utility. Additionally, it should be highlighted that this programme overlooked two nearby potential locations. This is unimportant in a lot of real-world situations. However, in the traditional sense, this is "information loss."

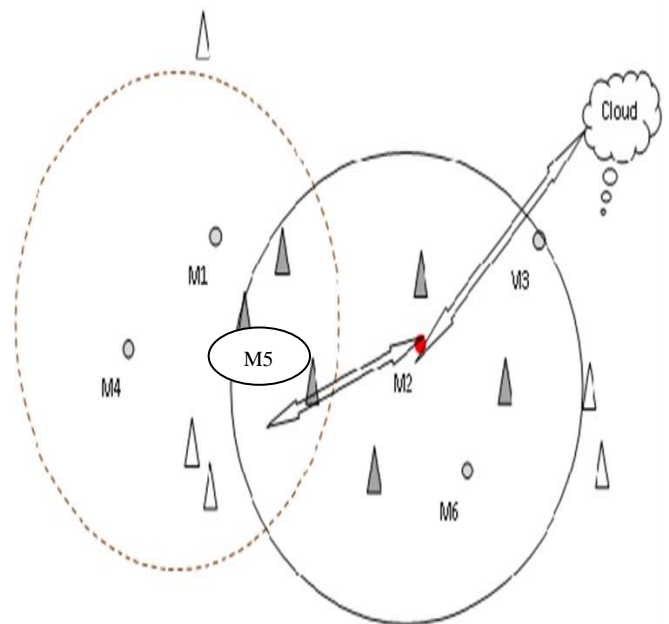


Fig. 5 Spread Identity

Table. 1 shows features comparison with other prominent methods. In the most of the existing methods, location privacy is being emphasized upon specially using TTP. This makes them vulnerable to the single point breakdown. Few methods like Cache based privacy preserving method[24] has worked upon query privacy separately using I-Diversity. This makes the method complex. In the proposed Spread Identity method, both query privacy and location privacy are being taken care simultaneously. This makes the method simple and easily executable.

Table. 1: Features Comparison

5. CONCLUSION AND FUTURE WORK

Sr. No.	Privacy Features	Obfuscation based approach[7]	Cache-Based Privacy-Preserving (CBPP)[8]	K-anonymity based privacy approach [9]	An anonymous communication technique using dummies for location-based[10][11]	Spread Identity [Proposed Method]
1	Query Privacy available	No	Yes, uses I-Diversity method separately for providing the Query Privacy, along with micro TTPs for location privacy.	No	No	Yes
2	Location Privacy available	Yes	Yes	Yes	Yes	Yes
3	Usage of TTP (suffers from single point failure, which can lead to the complete system crash for that duration)	Yes	No	Yes	No	No
4	Usage of Cache	No	Yes	No	No	No
5	Usage of blockchain [27]	No	No	No	Yes	No

By employing this technique, it can be observed that the QA programme has protected location privacy by concealing the 'enquirer'. An additional advantage of this approach is anonymity. As a result, the user's desire for security is strengthened. However, there are few limitations in the approach. From Fig. 5, it can be seen in the current case that while 7 potential locations were found, two helpful locations were overlooked. Additionally, if the "TTP" had been M1, all the key locations would have been recorded. There won't be any information loss in that scenario. As a result, the choice of the TTP in relation to the potential locations determines the information loss. Another possible limitation is that at any given time the GPS for a group of people (2 to 3) in near

proximity of the inquirer may be 'off'. In this case the question may be diverted to the TTPs, who are geographically separated by a large distance. In that case the geospatial query may give erroneous result. Future research may be conducted to establish a "figure of merit" for the information loss and then explore alternative tactics for maximizing the performance of this loss with regard to query execution time. Also, in future, dynamic selection of the TTPs same as 5G[25], [26], [27] concepts can be implemented, instead of implementing with a 'fixed close knit group

REFERENCES

- Lu, D., Han, Q., Zhang, K., Zhang, H., & Gull, B. (2019). A novel method for location privacy protection in LBS applications. *Security and Communication Networks*, 2019. <https://doi.org/10.1155/2019/1914038>
- Peng, T., Liu, Q., Wang, G., & Xiang, Y. (2016). Privacy preserving scheme for location and content protection in location-based services. *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings* 9, 26–38. https://doi.org/10.1007/978-3-319-49148-6_3
- Sung, K. Y. (2020). The Limits of Location Privacy in Mobile Devices. <https://doi.org/10.7275/17627979>
- Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1), 46–55. 10.1109/MPRV.2003.1186725. <https://doi.org/10.1109/MPRV.2003.1186725>
- Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, 31–42. <https://doi.org/10.1145/1066116.1189037>
- Kido, H., Yanagisawa, Y., & Satoh, T. (2005). An anonymous communication technique using dummies for

- location-based services. ICPS'05. Proceedings. International Conference on Pervasive Services, 2005., 88–97. <https://doi.org/10.1109/PERSER.2005.1506394>
7. Ardagna, C. A., Cremonini, M., di Vimercati, S. D. C., & Samarati, P. (2009). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing*, 8(1), 13–27. <https://doi.org/10.1109/TDSC.2009.25>
 8. Cui, Y., Gao, F., Li, W., Shi, Y., Zhang, H., Wen, Q., & Panaousis, E. (2020). Cache-based privacy preserving solution for location and content protection in location-based services. *Sensors*, 20(16), 4651. <https://doi.org/10.3390/s20164651>
 9. Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2014). Achieving k-anonymity in privacy-aware location-based services. *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 754–762. <https://doi.org/10.1109/INFOCOM.2014.6848002>
 10. Qiu, Y., Liu, Y., Li, X., & Chen, J. (2020). A novel location privacy-preserving approach based on blockchain. *Sensors*, 20(12), 3519. <https://doi.org/10.3390/s20123519>
 11. Amoretti, M., Brambilla, G., Medioli, F., & Zanichelli, F. (2018). Blockchain-based proof of location. *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 146–153. <https://doi.org/10.1109/QRS-C.2018.00038>
 12. Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR)*, 54(1), 1–36. <https://doi.org/10.1145/3423165>
 13. Akbari, M., Rezvani, A., Shahriari, E., Zúñiga, M. A., & Pouladian, H. (2020). Acceptance of 5 G technology: Mediation role of Trust and Concentration. *Journal of Engineering and Technology Management JET-M*, 57. <https://doi.org/10.1016/j.jengtecman.2020.101585>
 14. Saeed, M. M., Hasan, M. K., Obaid, A. J., Saeed, R. A., Mokhtar, R. A., Ali, E. S., Akhtaruzzaman, M., Amanlou, S., & Hossain, A. K. M. Z. (2022). A comprehensive review on the users' identity privacy for 5G networks. *IET Communications*, 16(5), 384–399. <https://doi.org/10.1049/cmu2.12327>
 15. Zhang, S., Mao, X., Choo, K.-K. R., Peng, T., & Wang, G. (2020). A trajectory privacy-preserving scheme based on a dual-K mechanism for continuous location-based services. *Information Sciences*, 527, 406–419. <https://doi.org/10.1016/j.ins.2019.05.054>
 16. Zhu, X., Chi, H., Niu, B., Zhang, W., Li, Z., & Li, H. (2013). Mobicache: When k-anonymity meets cache. *2013 IEEE Global Communications Conference (GLOBECOM)*, 820–825. <https://doi.org/10.1109/GLOCOM.2013.6831174>
 17. Shokri, R., Theodorakopoulos, G., Papadimitratos, P., Kazemi, E., & Hubaux, J.-P. (2013). Hiding in the mobile crowd: Location privacy through collaboration. *IEEE Transactions on Dependable and Secure Computing*, 11(3), 266–279. <https://doi.org/10.1109/TDSC.2013.57>
 18. Rajendran, K., Jayabalan, M., & Rana, M. E. (2017). A study on k-anonymity, l-diversity, and t-closeness techniques. *IJCSNS*, 17(12),
 19. Kern, M. (2013). Anonymity: A formalization of privacy-l-diversity. *Proceeding Zum Seminar Future Internet (FI), Innovative Internet Technologien Und Mobilkommunikation (IITM) Und Autonomous Communication Networks (ACN)*, 49. https://doi.org/10.2313/NET-2013-08-1_07
 20. Liberti, L., Lavor, C., Maculan, N., & Mucherino, A. (2014). Euclidean distance geometry and applications. *SIAM Review*, 56(1), 3–69. <https://doi.org/10.1137/120875909>
 21. Dokmanic, I., Parhizkar, R., Ranieri, J., & Vetterli, M. (2015). Euclidean distance matrices: essential theory, algorithms, and applications. *IEEE Signal Processing Magazine*, 32(6), 12–30. <https://doi.org/10.1109/MSP.2015.2398954>
 22. Huang, Z., & Xia, C. (2009). A kind of algorithms for euclidean distance-based outlier mining and its application to expressway toll fraud detection. *2009 International Asia Conference on Informatics in Control, Automation and Robotics*, 414–417. <https://doi.org/10.1109/CAR.2009.43>
 23. Pirinen, P. (2014). A brief overview of 5G research activities. *1st International Conference on 5G for Ubiquitous Connectivity*, 17–22. <https://doi.org/10.4108/icst.5gu.2014.258061>
 24. Kao, H.-W., & Wu, E. H.-K. (2023). QoE Sustainability on 5G and Beyond 5G Networks. *IEEE Wireless Communications*, 30(1), 118–125. <https://doi.org/10.1109/MWC.007.2200260>
 25. Satka, Z., Ashjaei, M., Fotouhi, H., Daneshtalab, M., Sjödin, M., & Mubeen, S. (2023). A comprehensive systematic review of integration of time sensitive networking and 5G communication. *Journal of Systems Architecture*, 138, 102852. <https://doi.org/10.1016/j.sysarc.2023.102852>
 26. Sun, B., Kloda, T., Arribas Garcia, S., Gracioli, G., & Caccamo, M. (2023). Minimizing Cache Usage for Real-time Systems. *Proceedings of the 31st International Conference on Real-Time Networks and Systems*, 200–211. <https://doi.org/10.1145/3575757.3593651>

27. Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, 14(2), 117. <https://doi.org/10.3390/info14020117>
28. Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for

Internet of Things. *IEEE Internet of Things Journal*, 10(7), 5898–5922. <https://doi.org/10.1109/JIOT.2023.3237893>

AUTHORS



Padmaja M Deshpande received her BE degree from REC Bhalki, VTU Belgaum Karnataka, India in 2004 and MTech degree electronics from Sir MVIT Bangalore, VTU Belgaum, India in 2007. She is currently pursuing PhD at the Department of Electronics and Communication Engineering, Amity University Gwalior, Madhya Pradesh, India. Her areas of interest are wireless communication, mobile communication and network security.

Email: padmajagreen@yahoo.co.in



Raghvendra Sharma is currently the Head of Department and Professor, of Electronics and communication Department ASET Amity University Gwalior, Madhya Pradesh, India. He is Fellow, IETE (Member No.: F-501955) Member MT Research & Educational

Services (MTRES) (Member No.: IM – A0005) Life Member, Institution of Engineering and Technology (IET) (Member No. :1100621188) Life Member, Institution of Engineers (IEI) India (AM095276-4)Senior Member, International Engineering and Technology Institute (IETI) (Member No.:2015082514) His research interest are digital signal processing.

Email: rsharma3@gwa.amity.edu



Swati Sinha received a PhD degree in electronics and communication from Birla Institute of Technology Pilani Dubai Campus. Her areas of interest are radar engineering, microelectronics engineering, mixed-signal design, application-specific integrated circuit design, embedded system design, cardiac pacemaker, internet of things, artificial intelligence & machine learning, and computational intelligence. She is currently working as Professor and Head of IT dept MGM CET Navi Mumbai

Corresponding author Email: mgm.hod.it@gmail.com