VAWKUM Transactions on Computer Sciences
http://vfast.org/journals/index.php/VTCS@ 2023 ISSN(e): 2308-8168, ISSN(p): 2411-6335
Volume 11, Number 1, January-June 2023 *pp: 108-122*

Comparative Analysis of Privacy Preserving Location Based Services Mechanisms

Muzamil Hussain [1], **Fizza Abbas Alvi**[1*], **Ubaidullah Rajput**[1]

[1]Department of Computer Systems Engineering, QUEST Nawabshah, Pakistan

Keywords: *Privacy, Location based Services, attacks, Security*

Journal Info:
Submitted:
February 15, 2023
Accepted:
April 02, 2023
Published:
May 08, 2023

Abstract
Recent trends in computing have enabled the provision of location-based services, offering practicality and convenience to users. Moreover, this has also given rise to new challenges and vulnerabilities that can potentially compromise user privacy. As these services are predominantly used on handheld devices, the risk of security breaches is higher. This research collates existing studies that have conducted quantitative and qualitative comparisons and analyses on how to address related challenges, with a particular focus on protecting user privacy in location-based services.

***Correspondence Author Email Address:**
fizza_alvi@quest.edu.pk

1 Introduction
Now a day in the digital era the number of users of the Internet is increasing day by day. Users are continuously involved to use the internet data for various online activities and also gain various services from any other side of the world. Thus, the private information of the customer has become a difficult task. As the demand for low-cost smart Mobile phones has increased, users have begun using this technology for a variety of internet services. Due to the increasing demand for smart Mobile phone customers, the popularity of location-based services (LBS) has been also demanded. Due to a deficiency of accuracy, Service providers also provide location-based information about the mobile user, this private information is provided by the mobile user. Some of the services provided are the user Location service which are friend finder, Location-based games, place Reviews, and different Applications [1]. The number of users of smart Mobile phones is increasing day by day, in 2013 (74%) of Mobile customers uses LBS services, and in 2015 this percentage increased to 90%. According to the research centers, in 2016 mobile users used to estimate 900B hours at different mobile Applications, which also increase by 150B in 2015 [3]. According to the report of worldwide Revenue, PRNewswire and berg insight LBS data increased from 2.8B in 2009 to 10.73B in 2014, also increasing by 16.6B in 2016 and 2022, this will be expected 80.77B users use the LBS services [4]. This will increase the annual growth rate by 39.3% during the calculated annual period. Although, Location Based Services (LBS) have also been debated regarding privacy. While enjoying

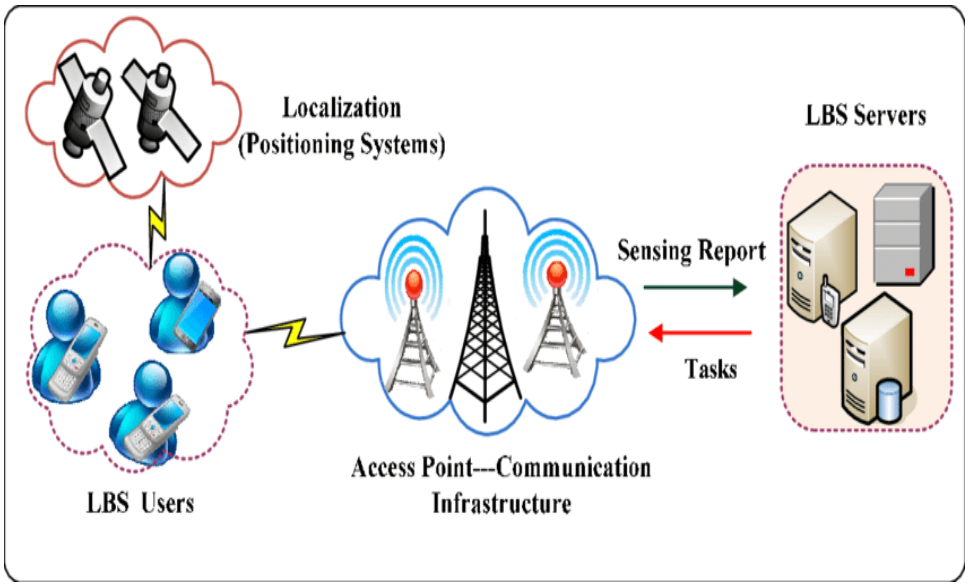

Figure 1. LBS system [2]

Location Based Services, users need to share their location LBS queries with the LBS server. It has been analyzed that the server may intentionally or unintentionally reveal susceptible location information in Location-based service queries [23]. Regarding the Research study of Android applications, e.g., the malicious Attackers breached the Location privacy of security risk [6]. Figure 1 shows the LBS system overview. In this paper, collective surveys on cryptography techniques and different mechanisms of location-based service (LBSs) have been discussed.

The rest of the paper is as follows. Section 2 highlights the background study. Section 3 discusses the related work. Section 4 provides the proposed approach. Section 5 shows the results and Section 5 concludes the paper.

2 Background

This section provides a background study of Location-based services.

2.1 Location-based services and their types.

Location-based services (LBS) is a variety of application enabled by a mobile device, providing a communication module and sensing infrastructure. LBS server provides convenient LBS service to the user to enjoy the LBS service. The User can easily submit their queries and attach their location, specifying what they want and where they are respectively. The following are four types of services [24–26].

- Information search services. It provides a search for local content (yellow/White pages) and also provides information about the city guide.
- Navigation and Map. It provides the service of assisted navigation and user can also find the route on the world map.
- Tracking services. It provides a variety of vehicle tracking services and also helps to find the location of friends and family's home location.
- Application. Location-based services are used in social media marketing, Mobile social networks, Vehicle social networks, context advertising, etc.

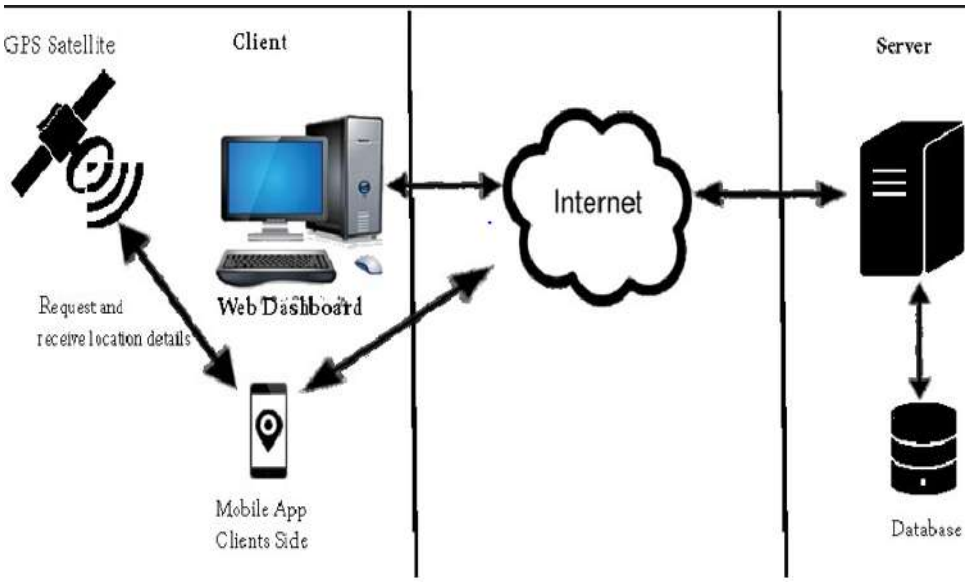

Figure 2. System Server to client Architecture [1]

2.2 System Architecture of Location-based Services

There is different architecture, some architecture is discussed below such as Server-client Architecture, Peer to Peer Architecture, Third Trusted Party Architecture.

2.2.1 Server-client Architecture

The Server-client architecture is shown in Figure 2 Server-client Architecture without any certain component other than the customers' mobile device the large number of users armed with mobile ends to request POI (E.G hotel, restaurant, industry, and parking Areas). It is weak architecture therefore Location based Database server comes back with outcomes assigned with a user request to get such services, the user must unveil their location to the server provider.

2.2.2 Peer-to-Peer Architecture

Peer to Peer architecture is shown in Figure 3. In this setting, the mobile ends and different sensors are enabled terminal to link. Peer-to-peer networks can achieve a large amount of information easily and distribute the handling weight and the network burden compared with the client-server method. Peer to Peer can be used to prefer a software program schemed so that each example of the program may react as both server and client, with similar status and accountability.

2.2.3 Third Trusted Party Architecture

The vital role of a third trusted party is to assemble and process the user's original query to preserve users' susceptible location information by using some privacy-protection techniques and then convey the LBS server. The conclusion, upon collecting these requests, recovers the database and sends requests to the correlated results to the proxy of anonymizing. Then, this proxy forwards these results to another user. By way of instancing, this proxy generates a cache area containing many users, and all the users in this region submit Location Based Service queries with the same cache region [6]. The Third trusted-party Architecture is shown in Figure 4. The way is done is that the customer sends a query by attaching their exact location information sent to CA (central Authority). The CA act as Location Anonymizer this trusted third party performs between the user and the location-based Database Server.

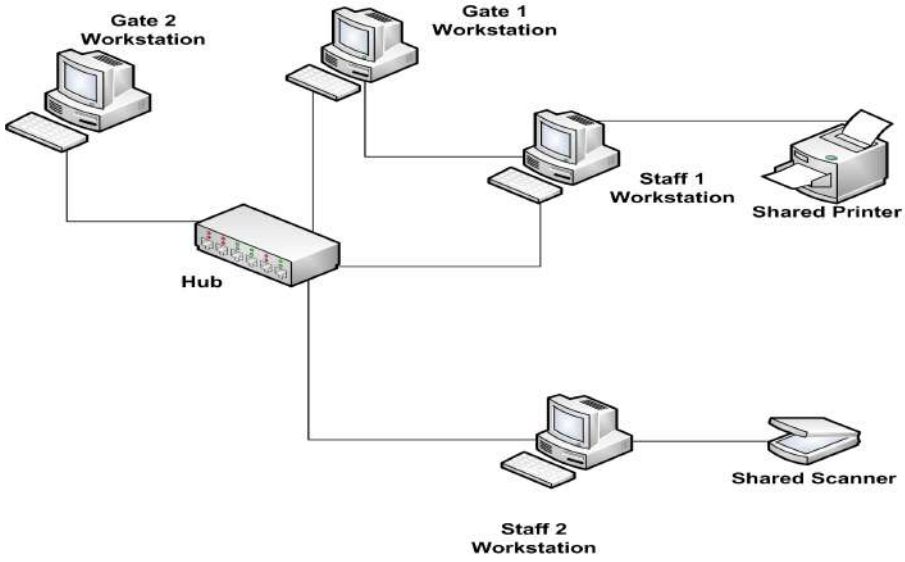

Figure 3. Peer-to-peer Architecture [1]

3 Related Work

In this section, existing work has been discussed.

3.1 Privacy Policy–based Location Privacy-Preserving Mechanism

before accessing user data information. For example, Privacy Personal Working Group. This mechanism defines the object location that summarizes or frames every customer location information and this updated method to become after to prevent a break of the privacy of user location, in which the particular location data is stored, and created. This mechanism offers a private security architecture for GPS services, where user can share their location and distinguish the structure information that will be revealed and the level of vulnerable information. Although, the customer is frequently resistant to managing composite personal policies directly, and is sometimes rejected by participants. Privacy strategy–based mechanisms require the Location Based server to follow the regulatory policies and resist attacks on the system [8]. The privacy strategy system does not impose privacy protection itself but rather relies on social media regulations and static economic regulation. Additionally, personal strategies can be very complicated, and experimental use of them in a constantly updating and excess acts dynamic location in a sensible environment has not been manageable yet. The purpose of private strategy is to prevent malicious disclosures or unintentional private information, and this research area has not yet made substantial breakthroughs or caught up with technology developments [30–32].

3.2 Obfuscation-based Location Privacy-Preserving Mechanism

This Scheme introduced the Time obfuscation Location based Mechanism, where in the whole process the mobile users generated dummy queries randomly chosen for the period. Especially, the location in each dummy query is randomly chosen from several users in a set of user locations D, which have the same location classification as the users. According to the research view, each poi in the dummy query is fully selected from the chosen degree of the classified (POI) pool, consequently, the illegalization is further upgraded. In conclusion, the aims of the assumption attack cannot be carried out effectively on our offered algorithm [7].

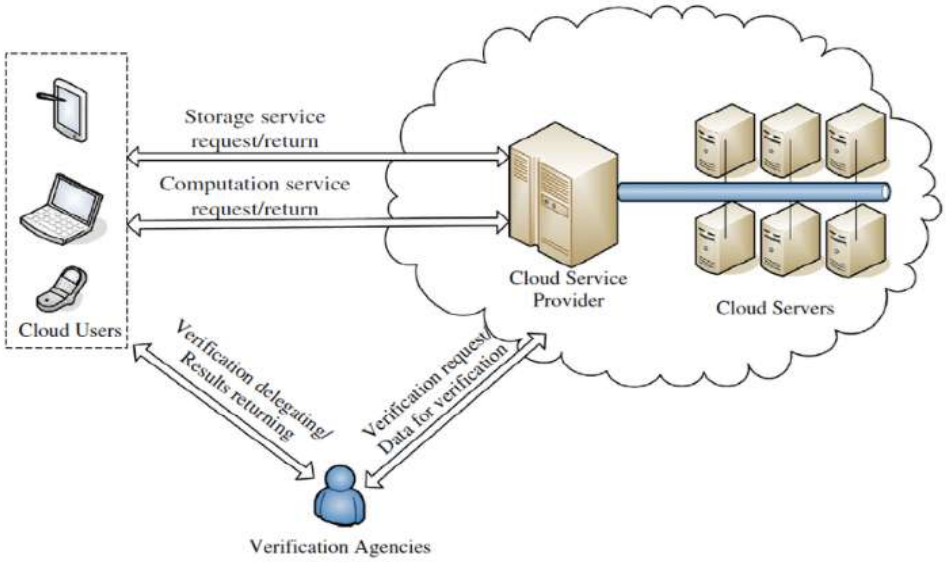

Figure 4. Third Trusted Party Architecture [1]

3.3 Cryptography-based Location Privacy-Preserving Mechanism

This cryptography-based mechanism processes the important data. This important data is processed by the common data preserving regulation(CDPR) and retrained the assembly of homogenous regulation. Privacy-protection cryptographic protocols are essential, like secure fully homomorphic encoded (FHE) and many-party calculation (MPC) may provide a solution to this query [9]. The purpose of cryptography is to protect information and communication by using codes so that only the intended recipients can read or process them. For example, unavoidable algorithms are used for generating cipher text keys, digital signal signing, and verifying privacy data for web browse processing, credit card transactions, and email correspondence. Cryptography and cryptanalysis are closely related disciplines. Nowadays, cryptography is mostly correlated with undisciplined plaintext (ordinary text, also called clear text) into encrypted text (a process called encoded), then reversing the process (decryption).

3.3.1 Homomorphic encryption -based technique of location privacy-preserving

In this framework, a homomorphic encryption scheme is used to encrypt the lead method to protect personal location and customer locations. This technique covers six steps as shown in Figure 5. The first step, the user Registration, mentions the crowd user's in the server Registration SR, using the homomorphic encoded Scheme, which encrypts its location space and sends the encoded location to the service provider. Before saving in a secure KD tree, it will guide all user locations. In the second step, 6 for daily task Submission, the user submits their task location in the same encoded way. In the third step, interval Computation, the Server computation SC compares the interval between the task location and user location without determining the original locations using this method or technique. In the fourth step, Assignment of Task, Central Server SC assigns the work to the nearest user according to the computed distance. In the fifth step, notification of the task, RS informs the user about the task that she/he is necessary to execute. In the last step, the user knows the location to authorize the order, and the user encodes the location task with the user's public key and provides it to its worker [13].

3.3.2 Block chain-based technique of location privacy-preserving

This technique used includes privacy preserver and blockchain. The structure of a blockchain network is broken into three different components which are fully knowledge sensing crowd Networks(FKSCN), blockchain, and confusion method as shown in Figure 6 [27]. The full knowledge-sensing crowd network

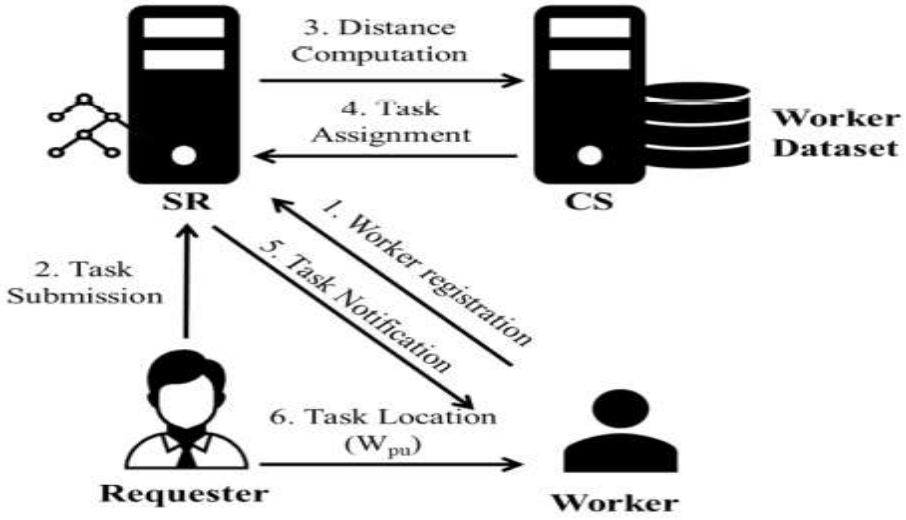

Figure 5. Homomorphic encryption -based of location privacy-preserving [1]

has two types of nodes, the first node is an ordinary user that contains customer information and the second one is a minor node. The essential role of MN (Miner Node) is to provide a fresh block location. The confusion method is extended to preserve the crowd user information by encrypting node information based on the Confusion Method Encryption Algorithm (CMA-E) and the Confusion Method Decryption Algorithm (CMA-D). Each piece of CMA-E encryption of user node information involves personal identity, generation, longitude, latitude, gesture, poster, and Profession. The last part is the blockchain where the main function is to protect the user information from intruders. The main structure of the blockchain was exchanged by generating the Merkle Tree and Currency Assignment using the double-SHA256 hash method algorithm. Fig. 4 represents the function method and deal components. First, the server broadcasts a sensing data task and then takes the sensing data to the task user in the full knowledge sensing crowd Networks. Therefore, the task sensing data confusion method is a space block where each block consists of nine customer nodes and one reserve node. Second, the blockchain backs up the user's information and presents the user with a fictitious coin in exchange for the user incentivizing and then withdrawing the money. Finally, the server retrieves the user information from the blockchain [15].

3.4 Collaboration and Caching-based Location Privacy-Preserving Mechanism

The number of relationships with LBS servers is possible to reduce by the foundation of the collaboration and caching-based procedure. The customer sent several query requests to the LBS server, there will be a greater chance of the adversary exposing susceptible information [10]. To initiate the first caching structure to protect personal privacy. In this structure work, the LBS user request to promote queries to the server to acquire the service data within that region. As a conclude, the mobile customer can hunt for point-of-interest POIs regionally without sending further requests to the server. however, users inescapable require to cache a large number of service data for a large regional area due to the heuristic caching technique and the aïve caching Technique, which is consequentially storage overhead and steer to deficiency in answering the query [11]

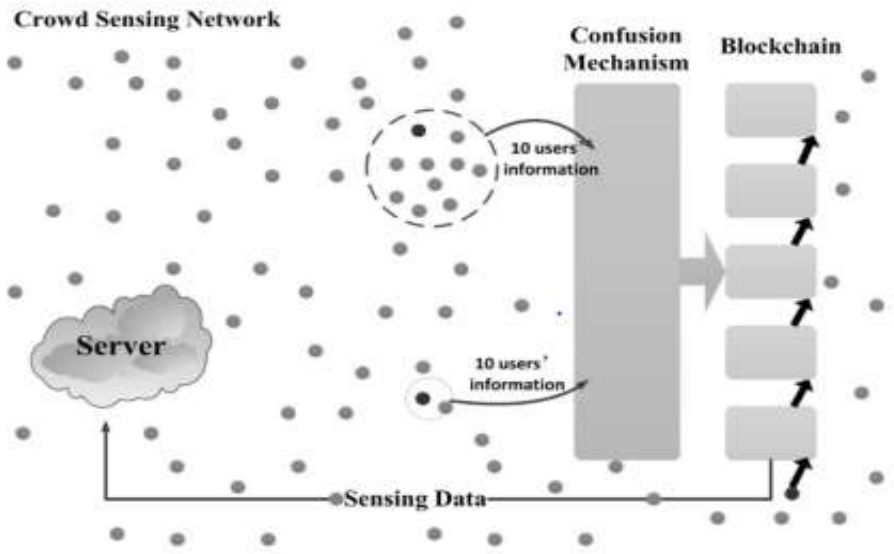

Figure 6. Block chain-based of location privacy preserving [15]

3.5 Clustering-based Techniques of Location privacy-preserving

The spatial distribution of this algorithm could be implemented into two different modes, on-demand mode, and proactive mode as shown in Figure 7. In Proactive Mode, the distributed Clustering Algorithm supports the peer-to-peer communication relationship within a single hop, which workers can do online register a timely. this mode gives a quick response as compared to on –Demand mode, it has the largest communication overhead. In on-Demand mode, the server can accept the request of online registered workers, and the LBS server will broadcast the request clustering signal received from the worker then the worker can stay to work on this Algorithm. After that, the worker can start work on the algorithm. Clustering is introduced by everyone who is connected, with every worker selecting a number between 1 and 0. Finally, the cluster head is choosing between the workers if the choosing number is below the threshold level. For blockchain, the cluster head starts broadcasting the request message in a cluster to join the non-head workers. If the workers received the requested commercial packet from two different clustering heads, therefore, she/ he should select the nearest Cluster-Head and join them. Especially, the C-head know all worker's places or location in the group. Finally, the member of this cluster can easily share their location and execute the task [14].

3.6 Dummy-based technique of location privacy-preserving

These techniques are intensively used in this method to create a different user's location by creating the false data position(dummies) by the user to provide the SP (service provider) from the attacker. The service provider responds to the relevant collection of filtered position data, this data can be obtained from different workers who generate the false location data and original filtered data, and the service provider responds to the important data. Through this Scenario, a maximum number of workers have conserved in the personal location since the service provider cannot be compared between original data and incorrect data position. The dummy-based technique can be caused by a third party or the maximum worker, where the middleware is not accessible in the decentralized Architecture [13]. using a dummy-based purposed method, the DCentroid was designed to solve the problem of personal location in SC. Through this Technique, the SC server obtains a Dummy location from clustering workers in place of the original location. The main scenario is consisting of three different components SC-server, interests, and crowed worker. The working flow of DCentroid consists of different steps. First, by using Dummy based algorithm, the

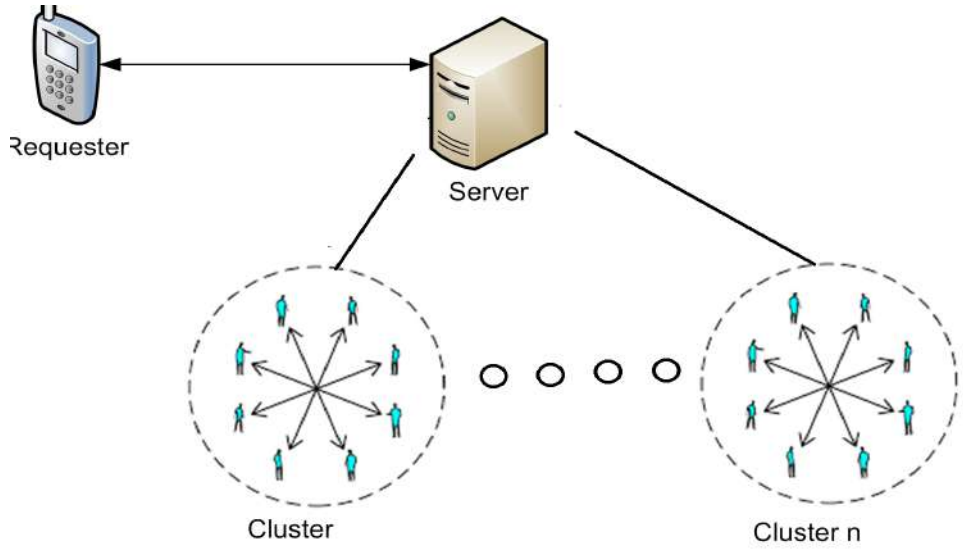

Figure 7. clustering based location privacy-preserving [1]

workers generate the four dummy locations on each side of the original location. These methods create sixteen positions for the worker to realize all possible dummy nodes. Consequently, this method removes the selected point to establish a uniform choice of location selection [12].

3.7 k-anonymity -based technique of location privacy-preserving

Personal Location is implemented against various personal threats using a k-anonymity structure as shown in Figure 9. To support private locations with sensitive personalization k-anonymity acquires multiple customer personalization frameworks that need to be defined. following the framework, each mobile node in the Network is defined, and it considers the low degree of k-anonymity, and highest spatial and dimensional resolutions, this k-anonymity protection location-based services (LBSs) help to receive when sent. A personal location security broker on a trusted server initializes the Mobile client's location un detectable and transmits it individually through a packet scrambling mechanism, such as local cellular location place information. by proving Location-based service, the risks, and challenges should be mitigated [17].

3.8 Private Information Retrieval (PIR) -based technique of location privacy-preserving

Another type of cryptography technique used to retrieve personal information, private data retrieval can ensure that when a server cannot recognize the subject of the queries. when user queries are entered into server the database, thus saving the server from resolving the user workers and further eliminating the user's personal information It is a feature based on personal information retrieving based on the optimal path calculation. Retrieving personal information retrieval provides reliability and trust throughout the communication process, such as Data retrieval, client requests, and interaction results. Although, there are two key challenges to retrieving personal information that needs to be addressed. The first is the calculated overhead and inordinate storage overhead. Designing basic retrieval policies and successive structures is the core issue in implementing personal information. Another challenge is controlling storage place and prescription retrieval to make personal information retrieval currently only useful at the shortest spatial extent, as the Owner of the LBS Database maps the Point of interest and maps data throughout the

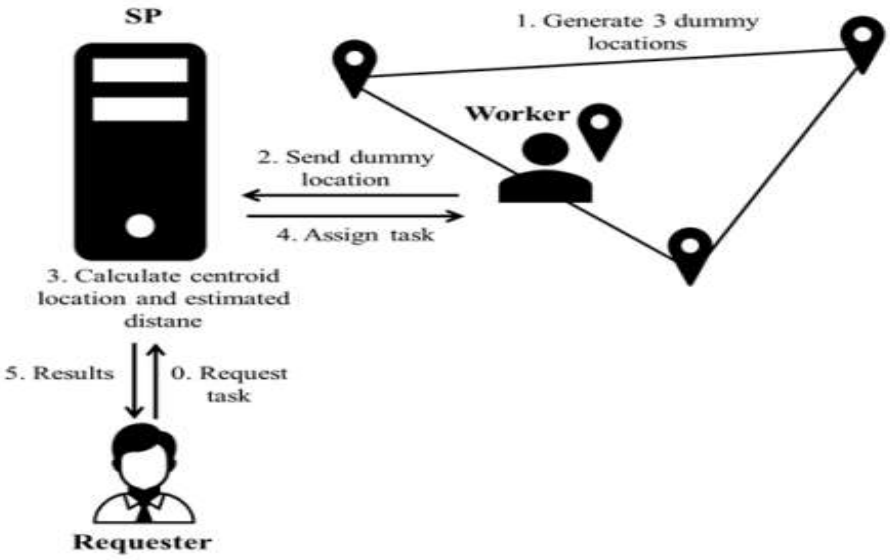

Figure 8. dummy-based location privacy-preserving [1]

region. A map must be stored Hence, this will be considered if a Location-based service provider installs cryptographic or Encryption systems at the exhibit [18].

The various mechanism or techniques discussed above are used in different research papers while collecting data related to LBS. These techniques were used in the implementation and provided services according to the defined scenario. Table no 1 discusses relevant research works, the use of the mechanisms, and their limitation.

4 Issues ad Challenges of Privacy-Preserving Location-based Services

Challenges associated with personal location protection. The main focal point of our analysis lies in four different preferred areas: the fifth generation is the most popular generation of social mobile communication, such as machine learning, the Internet of Things, and social networks. The emergence of big data in these regions has bought about changes in structural data and a variety of interdependencies, which is different from the traditional Location based service. A hot topic right now is the fifth generation of social mobile communications, with both expectations and concerns. In addition to the Internet of Things, smart health care, smart transportation, smart homes, virtual reality, and augmented reality (VR/AR), it will cover a range of new use instances and applications. The increasing accessibility of advanced location acquirement technology admits the link interest graphical information to remaining Social Networks (SN), thus leading to the appearance of Location-Based-Service-Networks. The interconnection of Social Networks and Location-based services calls for various distinct characteristics such as activities, attention, behavior, shared regular locations, and so on, which can provide well-off experienced knowledge for competitors [20]. The correctness and precision procedure are not recommended. The cipher attacks can easily break down the client's confidentiality through this method. Malicious organizations or servers directly expose private information. The open challenge is still the issue of managing the personal location and protection that are software bugs or design flaws. therefore, the password is widely used, and then he /the password is outdated. A password can be easily cracked or guessed by a hacker, so it is difficult to retain the password or make the information unsecured. The open challenge is to secure the password. security trust location and client anonymity are still open issues. The hierarchical grouping of mobile social clients is valu-

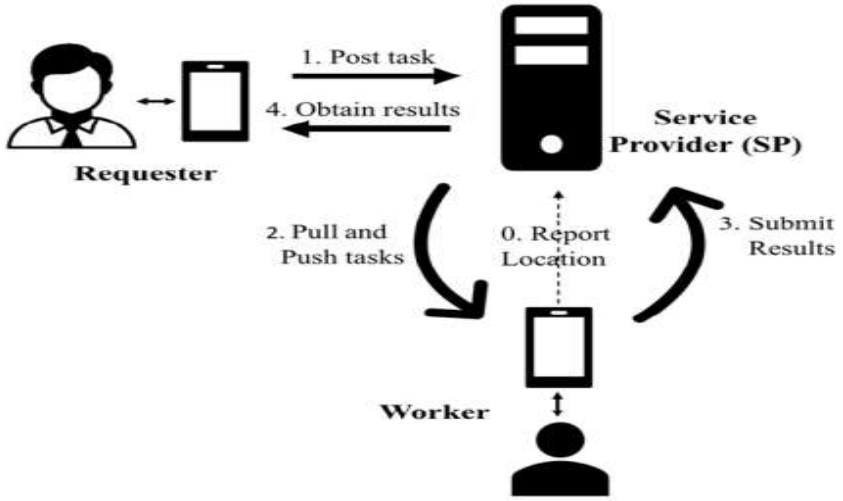

Figure 9. K-Anonymity based location privacy-preserving [17]

able with the k-anonymization method, but the problem of interpretation is not revealing imputation and not revealing the complete set of requirements [21]. A new method of securing a client's location based on the retrieval of personal information is compared to open path tracking of personal location. However, it used the total potential of these methods to challenge deeper inquiry into the cost of ciphering. However, the increased speed of research will reduce the costs of personal information retrieval operations. It also uses an efficient indexing method for structural inquiries in an upcoming research area cell phones generate and collect location information and disclosed/published it to third parties for processing. Analyzing the client's location information may reveal personal private information to research the collection of personal data [22, 28, 28, 29]. Table 1 shows the comparison of existing privacy-preserving mechanism and their limitations.

5 Conclusion

To develop aggregated knowledge, today's LBS depends on users' mobile devices and combines various new characteristics with the findings of location-related research. Researchers have become increasingly aware of the personal breach problem while using LBS services. The purpose of this survey is to present different accomplishments and upcoming works accomplished in the region of LBS privacy. Although several calculations are in place to protect personal information, there are still countless attacks that compromise personal location and as such, there are still multiple issues that remain to be addressed. By researching typical approaches, we collect their basic knowledge and advanced research. Finally, after analysis, we discuss different mechanisms and comparisons of different techniques that are used for services of location privacy-preserving. Also, discuss the different Attacks and open issues and challenges that are helpful for the Researcher in the field of protecting personal location as well as in future research.

Author Contributions

Muzammil Hussain : Conceptualization, Methodology, Software. **Fizza Abbas Alvi**: Supervision, Data curation, Writing- Original draft preparation, Visualization, Investigation.**Ubaidullah Rajput**: Software, Validation, Writing- Reviewing and Editing.

Table 1. Comparison Among Privacy Preserving based LBS Mechanism

Category	Computational Overhead	Communication-Overhead	Cost of utility	Privacy Level	Storage Overhead
Collaboration and caching-based	low	low	medium	high	low
Obfuscation-based	high	high	medium	high	medium
Cryptography-based	low	medium	high	medium	low
Privacy-preserving-policy-based	low	low	high	low	low
k-anonymity -based	Medium	High	Low	Low	Low
Private Information Retrieval (PIR) -based					
Clustering based	Medium	Medium	High	High	Low

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declared that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] M. B. Rajashekar and S. M. Sundaram, "A survey on user's location detail privacy-preserving models," SN Comput. Sci., vol. 1, no. 3, 2020.

[2] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," ACM Comput. Surv., vol. 54, no. 1, pp. 1–36, 2022.

[3] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," J. Netw. Comput. Appl., vol. 101, pp. 55–82, 2018.

[4] S. Ji, P. Mittal, and R. Beyah, "Graph data anonymization, DE-anonymization attacks, and DE-anonymizability quantification: A survey," IEEE Commun. Surv. Tutor., vol. 19, no. 2, pp. 1305–1326, Secondquarter 2017.

[5] J. Cortes, G. E. Dullerud, S. Han, J. L. Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in 2016 IEEE 55th Conference on Decision and Control (CDC), 2016, pp. 4252–4272.

[6] K. G. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," IEEE Wirel. Commun., vol. 19, no. 1, pp. 30–39, 2012.

[7] F. Li, S. Wan, B. Niu, H. Li, and Y. He, "Time obfuscation-based privacy-preserving scheme for Location-Based Services," in 2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2016, pp. 465–470.

[8] W. Enck et al., "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," ACM Trans. Comput. Syst., vol. 32, no. 2, pp. 1–29, 2014.

[9] C. Rechberger and R. Walch, "Privacy-preserving machine learning using cryptography," in Security and Artificial Intelligence, Cham: Springer International Publishing, 2022, pp. 109–129.

[10] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch, and N. Sadeh, "Caché: Caching location-enhanced content to improve user privacy," in Proceedings of the 9th international conference on Mobile systems, applications, and services - MobiSys '11, 2011.

[11] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd: LocationPrivacy through collaboration," IEEE Trans. Dependable Secure Comput., vol. 11, no. 3, pp. 266–279, 2014.

[12] A. Bashanfar, E. Al-Zahrani, M. Alutebei, W. Aljagthami, and S. Alshehri, "A survey on location privacy-preserving mechanisms in mobile crowdsourcing," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 7, 2019.

[13] B. Liu, L. Chen, X. Zhu, Y. Zhang, C. Zhang, and W. Qiu, Protecting location privacy in spatial crowdsourcing using encrypted data. 2017.

[14] B. Zhu, S. Zhu, X. Liu, Y. Zhong, and H. Wu, "A novel location privacy preserving scheme for spatial crowdsourcing," in 2016 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2016, pp. 34–37.

[15] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," Sensors (Basel), vol. 18, no. 11, p. 3894, 2018.

[16] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," IEEE Commun. Mag., vol. 53, no. 8, pp. 75–81, 2015.

[17] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," Comput. Netw., vol. 135, pp. 32–43, 2018.

[18] K. Mouratidis and M. L. Yiu, "Shortest path computation with no information leakage," arXiv [cs.DB], 2012.

[19] A. Alamer, J. Ni, X. Lin, and X. Shen, "Location privacy-aware task recommendation for spatial crowdsourcing," in 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), 2017, pp. 1–6.

[20] J. Li et al., "Drive2friends: Inferring social relationships from individual vehicle mobility data," IEEE Internet Things J., vol. 7, no. 6, pp. 5116–5127, 2020.

[21] L. Zheng, H. Yue, Z. Li, X. Pan, M. Wu, and F. Yang, "K-anonymity location privacy algorithm based on clustering," IEEE Access, vol. 6, pp. 28328–28338, 2018.

[22] P. Jagwani and S. Kaushik, "Privacy in location based services: Protection strategies, attack models and open challenges," in Information Science and Applications 2017, Singapore: Springer Singapore, 2017, pp. 12–21.

[23] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," IEEE Trans. Veh. Technol., vol. 64, no. 12, pp. 5631–5641, 2015.

[24] Y. Shen, L. Huang, L. Li, X. Lu, S. Wang, and W. Yang, "Towards preserving worker location privacy in spatial crowdsourcing," in 2015 IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–6.

[25] R. Al-ani, B. Zhou, Q. Shi, and A. Sagheer, "A survey on secure safety applications in VANET," in 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2018, pp. 1485–1490.

[26] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," Sensors (Basel), vol. 20, no. 12, p. 3519, 2020.

[27] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 6, pp. 3765–3775, 2021.

[28] X. Wang, Y. Xing, Y. Wei, Q. Zheng, and G. Xing, "Public opinion information dissemination in mobile social networks – taking Sina Weibo as an example," Inf. Discov. Deliv., vol. 48, no. 4, pp. 213–224, 2020.

[29] M. K. Tefera, X. Yang, and Q. T. Sun, "A survey of system architectures, privacy preservation, and main research challenges on location-based services," KSII Trans. Internet Inf. Syst., vol. 13, no. 6, pp. 3199–3218, 2019.

[30] H. Liu, H. Guo, K. Yang, and H. Li, "A novel privacy-preserving location-based service framework with distributed spatial data mining," IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1104–1117, 2018.

[31] R. Lu, X. Lin, X. Liang, and X. Shen, "PALM: Privacy-enhanced and location-based messaging," IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1662–1676, 2011.

[32] D. Zhang, H. Zhu, and R. Chen, "Private spatial data publishing with data-oblivious algorithm," Future Generation Computer Systems, vol. 75, pp. 311–318, 2017.