Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 82-92 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Evolution of Privacy Preservation Models in Location-Based Services

A B Manju[1], Sumathy Subramanian[2,*]

[1]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore.*

[2]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.*

ARTICLE INFO

Article history:
Received: 17 February , 2020
Accepted: 10 April, 2020
Online: 03 May, 2020

Keywords:
Location-based services
Privacy preservation
Fog computing
challenges
benefits

ABSTRACT

Location-based services have become increasingly prevalent with the advancement in the positioning capabilities of smart devices and their emergence in social networking. In order to acquire a service, users must submit their identity, query interest and location details to service providers. Such information shared by users are accumulated continuously, stored and analyzed in order to extract the knowledge base from it. Generally, this extracted information is used by service providers to provide users with personalized services. The accumulated data have enormous market value which is found to be used for many lucrative purposes. This work presents a detailed study on the evolution of existing privacy preservation models need to preserve privacy, and the opportunities to integrate fog computing services into privacy architectures. The study proposes a fog integrated privacy preservation model exploring the benefits and open research issues in traditional models and recent integrated fog models. Future directions of fog incorporated privacy preservation models are presented.

1. Introduction

Though location-based services (LBS) originated in the early 1990s, they became significant only after 2000. Since then, massive improvements have been made in facilitating technologies (e.g. telecommunications services), expanding applications (e.g. from outdoor to indoor environments), delivering interfaces (e.g. Smartphone, smart devices) and increasing technological innovations that have made the ambient environment more user-friendly (e.g. an increasing number of devices connected to the Internet and access to 5G). Meteoric development of the functionality of mobile devices play a vital role in bringing comfort to people's everyday lives [1]. Low-cost positioning devices with acceptable power consumption have made location-based services accessible to the common man and, in addition to providing profitable business opportunities [2]. Although it comforts end-users with on-demand and recommendation based services, significant concerns about privacy [3] have become a dominant issue. In order to make use of location-based services (LBSs), service users must disclose their private data, such as their identity, location and query information, to third-party service providers who cannot be trusted. The exposed data is accessed through snapshot queries (single query) and continuous queries (continuous follow-up queries). When user data is collected over a period of time, a short user profile is created on the basis of the data accumulated. User profile data [4] is used profitably at the discretion of the service provider and moreover most location based-services are typically offered free of charge. When a service user is at a particular point on Earth, LBS providers infer users' interest on the basis of the user's time, location and query data. The point on earth is therefore considered to be significant data in the LBS, represented in latitude and longitude data. The amount of data accumulated by service providers infer the user's private data, which leads to user tracking, gathering user's daily activities, finding the user's home and office address, and children's school or college. Remarkable real-world case studies represent the unauthorized use of users' private data for monetary profits, cyber-stalking of victims, intrusion of thieves, and many such activities. Current location-based service policies need to be revised with stronger security standards to support hesitant location-based service users.

Developing cloud computing technology has facilitated many location service providers to outsource their data in order to use the cloud storage service efficiently [5]. Security issues occur as location data is outsourced to cloud service providers, because cloud providers may benefit from location data. The plain text is therefore encrypted before being outsourced to the cloud.

*Sumathy Subramanian, Email: ssumathy@vit.ac.in

Cryptographically signed data cannot be transferred directly to location service users. Users should therefore be assured of the key to the decryption of the data. Users must receive encrypted data from the cloud and keys from service providers. But, this track of users-cloud and, users-LSP (Location Service Provider), have privacy issues. The cloud service provider operates as a user and collect decryption keys (dual identity attacks [6]). Integrating cloud servers into location privacy models have increased complexities at user and LSP end. Simultaneously, fog computing systems have developed to provide distributed services at the edge of the networks [7]. Contemporary development in cloud computing technology has introduced fog computing, with features such as distributed architecture, location awareness, enhanced security, local storage, processing, increased latency, and connectivity support. The fog integrated design models for location-based services have become significant [8]. Generally, location based privacy schemes support peer-to-peer and trusted third party (TTP) models. Users need to undertake privacy and security policies in peer-to-peer models, as they do not implement intermediate servers, while in TTP-based models, intermediate servers manage privacy and security protocols. Recent work, such as K-anonymity [9] dummy based [10] and mix zone [11] models, have adapted TTP servers to ensure privacy and security. Adapting TTP servers have some drawbacks, such as an intruder hacking TTP to access confidential user data. This has prompted many design models to incorporate fog services and enhance protection and privacy in location-based services. Fog servers can replace conventional TTP servers by preventing TTP vulnerabilities such as single point failures and security issues. Although recent studies have introduced fog servers [12] as an intermediate server, the dynamics of fog servers have not been used exhaustively in privacy preservation models. This work explores privacy preservation in location-based services, as well as the feasibility and benefits of integrating fog servers as middleware instead of TTP servers.

The survey explores traditional privacy preservation models and recent fog integrated models to understand the benefits of integrating fog into privacy architectures. In addition, two different types of privacy preservation models are proposed, such as the integration of fog in the user-collaborative approach and the trusted third-party approach. Overall, the survey presents opportunities for future directions for the preservation of privacy in location-based services and benefits in integrating fog into the privacy preservation architecture.

The paper is structured as follows. Section 2 presents the evolution of privacy concern in location-based services, followed by need for privacy preservation in location-based services in section 3. Traditional privacy models for location-based services are detailed in section 4; section 5 uncovers the location privacypreservation attributes for location-based services. Motivation of integrating fog computing in privacy models is presented in Section 6, followed by Section 7 covering existing fog integrated privacy preservation models. Section 8 details the proposed fog incorporated approaches and Section 9 presents the conclusion of the work.

2. Evolution of privacy concern in location-based services

The scientists at MIT initiated the concept of GPS for the first time on October 4, 1957 and observed that the frequency of the radio signals from the Russian satellite increased as it approached closer and decreased as it moved away. They were able to track the position of the satellite and the speed of movement using the frequency of the signals. Using the distance from the satellite, the position of the receiver in the ground can be tracked. The theory has grown, creating a huge impact in the field of GPS systems. Currently (2019) there are 74 GPS satellites operating in space where 31 are operational, 9 are being assessed for failure replacement, 2 are being tested, 2 lost during launch and 30 have expired. At the early stage of development, location-based services were segmented into location-based tracking applications and position-based applications. In tracking applications, push services, such as local fast food commercials, are pushed into users ' smart devices, and in the positioning applications, the device location is used to update the timing of the mobile phone. The lightweight dynamic pseudonym approach [13] was developed as part of the service agreement and the active pseudonym is chosen by the user and submitted to the service provider. In order to provide the service, the service provider logs into the dynamic pseudonym. The pseudonym is dropped by the user at the end of the service. The service provider logs into a complex alias to provide the service. However, in agreement with the service provider, the pseudonyms are created by taking into account the service providers as a fully trusted party, whereas the trust agreement is not defined.

The need for trustworthy and intelligent middleware telematics (location-based telematics) is addressed by the authors in [14], who pioneered the idea of middleware servers to forward the user's request to telematics servers. But the principle of confidence for smart middleware is not obvious. The work proposed by [15] elaborates the privacy concerns of mobile users and the importance of designing an option that allows users to turn off the location of their devices. The authors survey a community of location-based service users in another distinct study [16] and conclude that "service users are not very concerned about their privacy when the services are helpful in emergencies. A comprehensive risk prediction analysis of LBS adoption is presented in [17]. This analysis reveals different ways in which consumers can adapt LBS, such as the revision of device policies towards consumers, the social contract between service providers and consumers, the integration of third parties for privacy services and privacy preferred services. The research in [18] states that most LBS providers are mobile communication providers, and hence privacy risks are higher than individual LBS providers. Mobile communication providers can easily track the mobile users' through cell tower information. The user cooperative method has been suggested in [19], where an agent is randomly chosen from the user group to forward group communications to service providers. However, collaborative user selection policies have not been established. The proposed work in [20] implements Casper server to respond to requests of, especially anonymous queries. The incorporation of Casper increases the complexity of the service providers' architecture in the LBS. Region-aware privacy protection technique is proposed in [21]. Two types of dummy selection strategies, such as circular area-based and grid area-based, have been developed. Compact processing is designed on the server-side for the processing cost reduction of dummy users. The practical feasibility of modifying the architecture of the server-side is challenging, as multiple users have different adoptions of privacy protection. The proposed hybrid approach

[22] allow users to switch between the peer-to-peer and collaborative approach based on the number of neighboring peers present. The aim of this work is to provide users with privacy in either case. An anonymous server is used in another query based privacy protection system [23] to forward queries from users to location service providers. The anonymous server shields the identity of the users, sending users request as anonymous request to achieve privacy. Nevertheless, the trust between the user and anonymous server has not been discussed in this study. The proposed work in [24] aims to protect the privacy of users without a trusted third party. Cloud server support is used to evaluate the user density present in each region in order to achieve user-side spatial cloaking. Distributed anonymous servers are deployed as a proxy between the LSP and users in order to forward the spatial cloaking area of group of users to LSP [25] .Yet it is burdensome to deploy and manage the distributed network of servers. The query privacy scheme proposed in [26] has a trusted agent to maintain network parameters such as key management and data management between a service provider and a cloud server. To access the device parameters, the user registers with service providers and requests the query from cloud service providers. The system must, however, maintain a completely trusted agent. Moreover adversaries target trusted agents. In [27] the dummy-based approach enhances the dummy features. The dummies are placed at the level as of the speed of the real users. The dummies and the real users are crossed to recover from the accidental reveal of a real user. There is no emphasis on the consistency of the number of dummies to choose. In [9], the collaborative scheme, user device memory is utilized to cache the query request. The trusted agents are eliminated, and the user's collaborative cache enhances the system by sharing the query among the collaborative users. The trust between the users are not elaborated. The dual protection model in [28], provide data privacy to service providers and query privacy to users'. The proposed model outsources the database of service providers to cloud servers by encrypting it. Users availing the service, register with service providers and obtain the secret key. The encrypted data from the cloud is decrypted at the users' side with keys. This model considers that cloud service providers do not collude with any other entities; however, possibilities are not focused. The system model proposed in [29] has a convertor and anonymizer in between user and the LBS provider. The convertor defines the user-defined grid to a uniform grid and is sent to the user. The encrypted request is forwarded to the anonymizer and the encrypted response from a service provider is forwarded from anonymizer to user. The anonymizer also maintains cache of the data for future queries. The maintenance of more than one middle agent increases maintenance complexities and have practical feasibility concerns. The R-constrained dummy based scheme proposed in [30], constructs virtual circles throughout the trajectory of the users for trajectory protection. The cost of processing the dummies is burdensome for the system. The semantic information of the location is utilized to generate fake queries [31]. In this approach, the queries are generated by the system based on the time and the location semantic information. However, the users' queries are not always related to the semantic location information of the users. To enhance the caching based design, a trusted agent in the middle is utilized to cache the efficient data that is frequently requested by the majority of users [8]. The trusted agent combines the K-spatial request from many users and eliminates the duplicates, to enhance the processing time at the server and to reduce the network traffic. The agent may collect sensitive users' information and use them profitably. The ongoing research evolution in location-based services is described widely in [32].

At the initial stages (2000-2004) users had less concentration on their privacy as they are helpful in emergency services. Moreover, awareness of nefarious activities was less. The awareness of users' information collection at the service providers' side was increasing (2002-2005), hence users' hesitation towards the usage of LBS was increasing. As a result, the service providers started revising their privacy policies in making them transparent to the service users' (2005). In the period (2000-2006), most of the location-based services are provided by mobile communication providers; hence providing privacy protection becomes complex. As mobile communication providers monitor the users' location based on cell tower information. In (2005-2006) simple pseudonym exchange models were proposed to hide the identity of the users. Random user collaboration approaches were initiated to eliminate agent in the middle. As the users' devices are not much capable of storing the queries for the future, the caching was not feasible. In (2007-2009), the random selection models were proposed to select the dummy users' and the behavioral pattern of the dummies was not much concentrated. In (2010-2012), many trusted third parties in the middle were proposed. They were deployed as a single agent or multiple agents as per the requirements. Various levels of user side caching have been proposed during (2012-2016), as the storage capabilities of smart devices have been enhanced. In addition, the number of location-based services increased dramatically, with third-party service providers starting to use cloud storage services. During (2016-2019), dummy-based strategies have been provided at the level of real user activity by improving dummies ' behaviors and concentrating on the locations where dummies are chosen. In addition, distributed computing, such as fog computing, was incorporated into privacy preservation models instead of trusted agents.

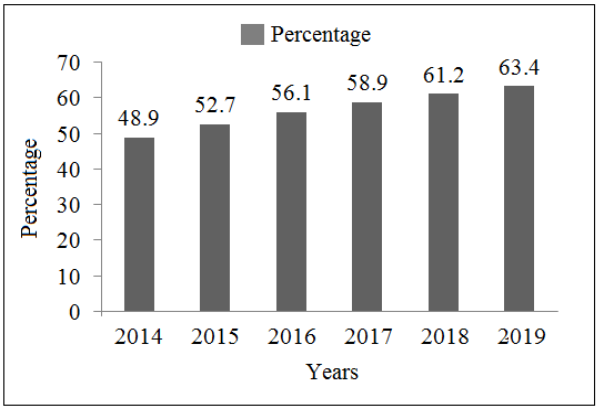

Figure 1: Percentage of mobile internet users from 2014 to2019 [34]

3. Need for privacy preservation in location-based services

According to Allied Market Research [33], location-based service market is expected to grow from 23.74 billion in 2018 to 157.34 billion in 2026. The enormous increase in the number of mobile Internet users has also triggered an increasing number of location-based applications. Figure 1 shows the rate of increase in the number of mobile phone internet users [34].

The need for privacy and awareness among service users is increasing as a result of the increasing number of online cybercrime cases. The trendy and dominant online social networking websites, such as Facebook and Twitter, provide registered customers with a free-of-cost subscription. These giant organizations have users from all over the world, where activities such as user's personal information, official follow-ups are deliberately uploaded to users. However, there are other unknown sources of information service providers can avail, such as locations from where the users' login, monitoring users' online activities to extract the users' interest for personalised advertisements and recommendations that have huge business profits. Service providers have no right to use the information of users for unauthorized purposes. There is no law controlling the information distributed from the service providers end to other third parties. The information includes privacy data that contain user's personal habits, regular timeline visits, business profits, banking details, and family member information. When this private information reaches the hands of targeted attackers, it can lead to unwanted stalking, theft, abuse of women, and kidnapping.

Increasing numbers of cyber-crime cases enable privacy breeches from small organizations to large service providers. In 2011, iPhone's hidden location synchronization was uncovered, and user locations were sent to Apple without user's knowledge. Similarly,angry bird game collects the age, gender, and location of the user [35]. The main concern of users is that the private information is trapped in the hands of adversaries that result in vulnerabilities.

• Privacy threats

Location service users are exposed to threats in many ways, such as tracking service users (tracking threats), mapping online identity to real-world identity (identification threats) and uncovering online behavioral patterns (user profiling threats).

• Tracking threat

Service users need to use location-based services in many situations to know the location information. Timing information related to the service request is the significant data that links the day-to-day activities of users in accordance with time [36]. When these private data are analyzed, the adversary may be able to track the location of the user throughout the day [37]. With accurate data analytics, past, present and future locations of users are easily exposed to attackers.

• Identification threat

The online identification used by users can be linked to the real-world identity of users with the help of quasi-identification attributes such as geographical tags in uploaded photos, home and office addresses from personal websites [38]. Adversaries may be able to identify the real identity of the user and map the data of the user.

• User threat profiling

The location information associated with the time exposed by the user reveals the user's private information [39]. When the online activities of users are documented for a period of time, the data analyzed reveals user profiles containing health conditions, religious beliefs, marital status, political interest, business details, and the home branch of the bank [40].

4. Traditional system models of privacy preservation for location-based services

The generic framework of location-based service is the Peer-to-Peer and trusted third party model.

4.1. Peer-to-Peer model

The basic structure of the peer-to-peer model is illustrated in Figure 2, which consists of three entities, such as location-based service users, location providers and location-based service providers. With the help of GPS technology, the user acquires the current location from the location provider via his smart device. The current location of the user is then sent to location-based service provider along with the user identity and query interest to avail the service. The location-based service provider responds with the location of the user based on the query request.

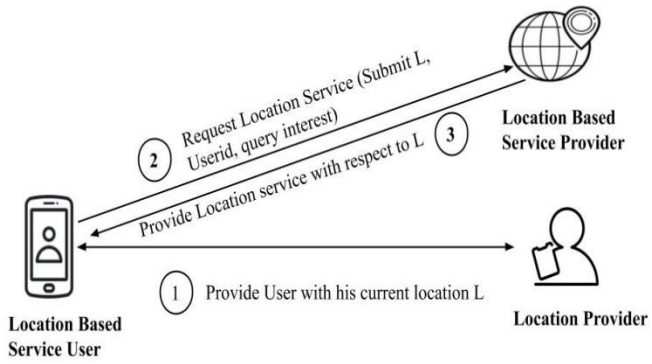

Figure 2: Peer-to-Peer Architecture

In the peer-to-peer model, data is communicated between the service user and the service provider directly. The privacy of users are defined by a user-trusted collaboration model [9] or with the help of online friends circles such as social networking friends [41]. In general, users' do not send the unprocessed data to the service providers, hence in [42], the users get collaborated locally with n-hop distance and the data grouped is sent to the service providers. The advancement of social networking sites has increased social friendships and their bonding. Trust between social friends is used to hide private data sent to the (Location Service Provider) LSP. Location obfuscation models have been implemented as dummy-based approaches [27] and location perturbation approaches [43]. In obfuscation models, users independently outsource their data as anonymous data such as enlarging their position in an area and adding dummy users. The main drawback of the model is the service user, who becomes solely responsible for the outsourcing of the data. However, these models do not require additional systems to support. In feelings-location privacy [3], the authors have presented the depersonalization of location-based on user-desired location The k-locations chosen for the protection of privacy are based on the priority of the user and also on the popularity of the region. In this approach, finding k-locations is a complicated process, as all locations chosen must be equally popular as users' location.

The dummy-based approach formulated in [31] considered the correlation between the location subject and the query type to

generate more robust dummies. Dummies are created in locations where the semantic subject information and the query type are the most appropriate. Finding dummy locations to match semantic information is complex as it depends on the spatial distribution of a region. The authors of the user-centric location privacy architecture [44] proposed the user-desired level of privacy in which the service user decides which data to be sent and which should not. Although service automation has enhanced the process, finding dummy locations with service similarities in all geographic regions is still complex. The asymmetric encryption technique involved in [45] preserves the sharing of private locations with social friends. The location can only be known to friends by decrypting the location information. Encryption and decryption increase the number of messages being exchanged between friends. The dummy-based approach proposed in [27] creates dummies with a replica of the actual user. Dummies are limited to travel and are managed to keep similar to the actual user. User membership benefits could save the cost of dummy user processing in location-based services. However, in the current research, the conditions for the number of dummies to be created have not yet been defined.

4.2. Trusted third party-based architecture

The architecture of the trusted third party server is shown in Figure 3. Unlike the peer-to-peer model, third-party servers have been integrated between the location-based service user and the location-based service provider. The user obtains the current location from the location provider, and then sends the user's identity, current location, and query interest to the trusted third party server. A trusted third-party server also receives a request from other service users. The user-identity is hidden and the query is sent to a location-based service user as an anonymous query using a third party server. Service response from location-based service providers is sent to trusted third party servers, and third party servers finally segregate user response and forward it to service users.

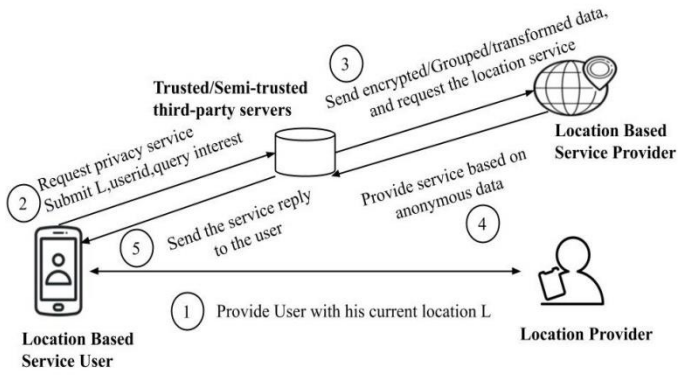

Figure 3: Trusted third party based architecture

The TTP servers are responsible for the data submitted by users. The cost of incorporating TTP servers is an additional burden for service users. Attackers may target TTP servers to access private data. Trust maintenance between the service user and the TTP server defines the robustness of the system. TTP servers are implemented as fully trusted [46] or, in some cases, as semi-trusted [6], to overcome privacy threats. The location transformation approach [47] replaces a fully trusted third-party server with a semi-trusted server and a function generator as an intermediary. Semi-trusted servers and function generators work independently. The function generator transforms the location coordinates, and without the knowledge of the transformation parameter, the semi-trusted server does not have a chance to learn the true location. This approach has an additional burden on the execution of a function generator and a semi-trusted server, making the model expensive. The trusted third party intermediary servers involvement in [48] forms a user group under the intermediary server. The authors argue that there is no need to exchange pseudonyms (in order to hide the real identity of the users) as they do not enhance security; instead, the members of the group are qualified on the basis of positive, negative and no change in membership to continue with the group on the basis of their activities. However, trusted third-party servers are expensive and maintaining a group becomes more complex.

The k-anonymity approach [49] involves the location perturbation server in the middle. The intermediate server maintains the private data of the k-users and sends the group request to the LBS to protect the identity, location and query of the k-users. However, trust issues arise from the trusted location perturbation server implementation. Incorporating more than one TTP server has also been experimented to prevent TTP from learning private data of users [50].

5. Attributes of location privacy

Figure 4 shows the attributes of location privacy. The service user identity can be an email ID, phone number, unique login ID and device ID. There are many LBS applications that require verification of email ID or phone number before acquiring the service. Few LBS applications do not ask for any user identities, such as finding "My location" in Google. However, the service is used based on the continuous monitoring of the type of service obtained with a many context-based link information about the user obtained at service providers end. The user's identity is protected by the use of pseudonyms acquired from TTP servers. The real identity of the user is replaced by a pseudonym (fake ID). Whenever different pseudonyms are used, the adversaries find it hard to track the user. However, when TTP servers work with LSPs, real users can be easily tracked. As a result, user collaboration approaches have evolved [51]. In collaborative user approaches, users exchange their user ID in a temporary collaboration that eliminates TTP servers.

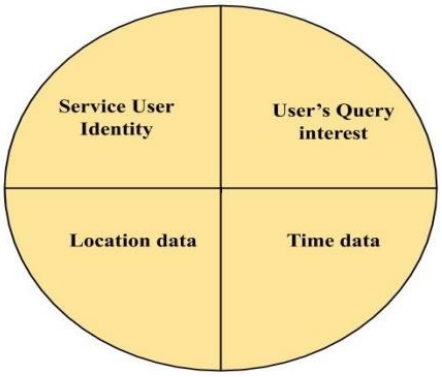

Figure 4: Attributes of location privacy

The location data of the user is the primary information used as the basic attribute that is required for the LBS service. Based on the location data, service users home location, the office address and the school address of the children can be obtained.The security attribute "location" is obtained from service users based on their service usages. When users obtain location-based services on a continous basis, user trajectory data can be easily mapped with location updates. The location of the user is protected by

- Add noisy locations to the real location of the user [52]
- Location transformation approaches:real location of the user is transformed to other neighboring locations [53]
- Group-based service procurements: Exchange the location of the users with group members [54]

The time data, acquired by the adversaries is linked with other attributes to coordinate the users' activities depending on the time of the day. The exact time of the service request is delayed by the user to hide the timing of the service request from the user. Time transformation will help third party intruders to record the delay in the user's request for service instead of actual time.

Information on the users ' **query** reveal their personal interest, which becomes the key information for personalized online advertisements. To hide users ' query interest, there are models such as crypto-algorithms that encrypt the query at the users' end and decrypt it in the service providers end. There are different types of models that add noise data to the exact query information. The addition of noise data to the exact query must not delay the quality of the service provided to the user. In this regard, the user collaboration approaches have helped by adding a collaborative user query, and the intermediate server approach has helped users to hide their identity by adding other users from the same region.

The PIR (Private Information Retrieval) technique was used to reduce computational latency [55]. The specific query of the user is anonymized with the help of expanding the size of the region from the location of the user. The query response for all the locations in the region is stored in the local database . Users retrieve an accurate query response from the local database. The requirement and trust of the local database is not defined. Protecting the privacy in continuous queries creates more complexity [56]. Fake queries are added to the actual queries in order to anonymize the query of the user. Fake queries inserted into the actual queries must be contextually linked to the location of the user in order to avoid attackers toremove the fake queries. In [56], a query pool is built for each location, which provides queries from the historical query request provided by different users. However, the processing of large queries for single users creates additional burden for service providers.

In general, the privacy preservation models degrade the precision of information submitted to the service providers and target to acquire the services accurately without compromising the service quality.

5.1. Location Privacy

Location privacy threat is the leakage or misuse of service users' location information by the service providers or other adversaries [57]. The most popularly used protection scheme is the dummy-based models. Semantic location-related information is used to generate realistic dummies [31]. However, the number of dummies to be generated is not defined. Dummy locations are generated within a circular area where the actual location is centered [30]. However, there is a high risk of exposure to the centered real location. Most dummy-based models are designed to generate realistic dummies, and similarly, the attribute-conscious scheme [58] uses location attributes to generate dummies in the context of location query probabilities. Vehicular location privacy protection based on the vehicles in their proximity is implemented in [51], but the dynamic collaboration has the risk of management of the dynamic group. Another vehicular privacy protection model [59] enhanced the dynamic group formation technique by introducing local hotspots and global hotspots. The positive activities of the group members act as a credit to join the group each time. The collaborative approach in [40] suggests that TTP servers to be replaced by service users device resources, and user collaborative groups need a central controller. The multidimensional privacy protection model [60] with both location and query protection is targeted and based on the model, the semi-anonymous server is incorporated to direct the request to a service provider. The accuracy of the results of the query may be degraded in this model.

5.2. Query Privacy

Query privacy protection prevents adversaries from accessing accurate query information. Basically, query protection schemes fall into two broad categories, such as query obfuscation techniques [61] and dummy query insertion techniques [62]. Query protection scheme "Dummy-Q" [56] eliminates TTP servers by using mobile resources to store the query pool system in order to optimally store the queries used by the quad tree system. Cloud servers [63] prevent location and query directly from being submitted to service providers. The user submits the enlarged region where the service is needed, and the encrypted data related to the region is sent to the cloud server where the cloud server assists the user in the requested service. In [64], the TTP server is used to collaborate with users and to send a collaborative query request to the service provider where the TTP servers trust is not defined. The work proposed in [5] presents on how cloud servers can effectively replace TTP servers, and how users can gain greater privacy on the basis of homomorphic encryption.

5.3. User Identity Privacy

The online user identity associated with online user activities defines user behavior patterns and serves as the perfect information for personalized recommendations and advertisements. Identity protection models of users are comparatively less focused than the location and query protection, as the achievement of location privacy and query privacy completely undermine the identity of the user. In general, the pseudonyms replace the identity of the user. Dynamic pseudonyms are used to protect the identity of users. Pseudonyms are used to hide the identity of service users [65]. The game-theoretic approach has been implemented in [66] in order to protect the identity and location of the service user's privacy.

5.4. Privacy metrics

Wide range of privacy metrics are used to measure the protection achieved. Privacy in location-based service is achieved by using a fake identity, encrypted or anonymized query and

location instead of actual name, queryand location. The purpose of the privacy measure is to evaluate any breach attempted by an attacker. The most common privacy metrics used are

- Entropy (H)

The most widely used metric inspired by the Shannon Information Theory is entropy [67]. Entropy is a logarithmic measure of the number of states with a significant probability, explicitly and the states with a substantial probability of being occupied. Entropy is used by modifying it according to their considered parameters. In general entropy is defined in Eq.(1)

$$H=-\sum_{i=1}^{K} P_i \log P_i \quad (1)$$

Where 'P_i' is defined in Eq.(2)

$$P_i=Q_i \,/(\sum_{i=1}^{K} Q_i) \quad (2)$$

Maximum entropy is achieved when all K locations have the same query probability Q, as shown in Eq.(3)

$$H_{max}=\log_2 K \quad (3)$$

The higher the value of entropy, greater the privacy achieved.

- Single location exposure risk (SE)

The probability of exposing the actual location of the service user from the group of locations chosen for anonymity is single location exposure risk [30]. The exposure probability of single location from the group of location points $D_i$is shown in Eq.(4)

$$\frac{1}{D_i} \quad (4)$$

The probability of exposing the actual location of the user from the group of locations termed as 'set n'is defined in Eq.(5)

$$SE=\frac{1}{n}\sum_{i=1}^{n}\frac{1}{|D_i|} \quad (5)$$

The lesser the value of SE, the greater the privacy.

- Trajectory Exposure Risk (TE)

Number of dummy trajectories m, in which s defines the number of trajectories that overlap, and (m-s) trajectories that do not overlap [30]. The trajectory exposure risk is determined as in Eq.(6)

$$TE=\frac{1}{(m-s)+T_s} \quad (6)$$

where $T_s$is the total overlapping trajectories present in the group of trajectories formed by the user. TE value is aimed ata minimum to achieve higher privacy.

- Distance deviation (dd)

The mean value of offset distance between the location position of real trajectory and the dummy trajectory [30] is defined in Eq.(7)

$$dd=\frac{1}{n}\sum_{t=1}^{n}\left(\left(\frac{1}{m}\sum_{j=1}^{m} L_{dist}(RL^t, DL_j^t)\right)\right) \quad (7)$$

where m is the number of dummy trajectories, t is time instance and (RL^t, DL^t) is the distance between each location position in the real and dummy trajectory. Minimum distance deviation defines maximum privacy.

- Distance deviation degree (D_{degree})

The distance deviation degree is the mean value of distance deviation(dd) and radius (|R|) of the circular area defined for dummy locations generation [30]. When n is the number of dummy locations the D_{degree}isdefined as in Eq. (8)

$$D_{degree}= \left(\left(\frac{1}{n}\sum_{i=1}^{n} dd_i\right) / |R|\right) \times 100 \quad (8)$$

Lesser the D_{degree} value, maximum privacy is achieved.

- Temporal similarity between real and the dummy trajectory (Sim_t)

The temporal difference between the real and the dummy trajectory should be minimum in order to increase privacy [30]. The temporal similarity is defined in Eq.(9)

$$Sim_t = \frac{||(t'-t)||}{\Theta} \quad (9)$$

where t' is the query request time of real trajectory and t is the query request time of dummy trajectory. 'Ɵ'is maximum time threshold defined by the user and || ''|| is the normalization. The higher the value of Sim_t,the maximum privacy is achieved.

- Spatial similarity between the real and the dummy trajectory (Sim_S)

The spatial similarity between the real and the dummy trajectory is measured using Eq.(10)

$$Sim_S = \frac{||<x,y>,<x',y'>||}{\delta} \quad (10)$$

in which <x,y> is the spatial position of real location and <x',y'> is the spatial position of the dummy location. $\delta$is the maximum spatial threshold set by the users [30]. The higher value of Sim_S achieves higher privacy value.

- Anonymous area requirement (A_{Area})

The anonymous area requirement is 100% when the anonymous area determined satisfies the anonymous area defined by the user [12]. If (A_{min}==A), then A_{Area} is 100%,where A_{min} is the minimum area defined by the user and A is the anonymous area determined. The higher the value of A_{Area}, the maximum the privacy. However, it increases the processing cost as well.

- Position protection (PP)

The position protection [12]is defined in Eq.(11)

$$PP=((x',y')^p - (x,y))\,(x',y')^p \quad (11)$$

in which $(x',y')^p$ is the number of all dummy positions and (x,y) is the actual position.The maximum value of PP leads to maximum privacy.

- Trajectory protection (TP)

The trajectory protection [12] is determined based on the number of valid trajectories. When S_T represents the total valid trajectories, the trajectory protection is determined using Eq.(12)

$$TP= (S_T-1)\ S_T \quad (12)$$

The maximum the value of TP, the maximum is the privacy achieved.

6. Research motivation of integrating fog computing in privacy models

The analysis of the privacy protection models presents the existing downsides in the current protection models. For example, in the context of peer-to-peer architecture, users are solely responsible for forwarding the request to service providers. Users need to take care of protection techniques such as data encryption, user collaboration, local storage, and user mobility. When users are in emergency situations such as the abduction of attackers, road accidents, trapped in the forest, and other such activities, they will not be able to take complex steps to use the location services and could increase their risk of being trapped in the hands of strangers.

Considering TTP as a solution for peer-to-peer approaches, they are also of concern to users. TTP servers are designed to forward user service requests in a privacy-friendly manner, but the risk of single-point failure attacks [68] is unsolvable. The risk of trusting anonymous servers is always a matter of concern. Instead of defining TTP servers as fully trusted, research focused on semi-trusting servers. The semi-trusted servers [6] were implemented to store encryption keys, encrypted data of the users' collaboration details and other details related to the users. The problem with semi-trusted servers is that they might get collaborated with third party-service providers to map the users' private data.

Traditional location-based services are provided to customers through centralized cloud-based approaches. Cloud computing policies have been satisfying customers as they evolved, but the huge increase in data movements from and to cloud computing has degraded the quality of the service it provides to customers. Centralized cloud computing has therefore evolved to serve customers in a promising way, without compromising the quality of services in a decentralized manner. The promising solution for decentralized computing is termed as fog computing by Cisco [69]. Fog computing serves customers at the edge of the network (at their local ends) and the data is being processed with the help of networking resources [68]. Further, if necessary, the data will be sent to the cloud for processing. The promising fog computing solution has the following advantages: proximity to end-users, geographical distribution, optimum resource utilization, low latency, reduced network traffic, improved service quality and a superior computing environment for users. By acquiring the benefits of fog in research, fog computing can fit into privacy-preserving LBS models instead of traditional TTP servers.

7. Existing fog integrated privacy preservation models

The characteristics of fog computing, such as improved security, decentralized control, improved latency, local computing, stimulate many researchers to incorporate fog. The fog computing technique is used in many recent works as local computing. The benefits of fog computing are used by the incorporation of fog nodes [70]. IoT devices are used to implement the location privacy protection algorithms by incorporating surveillance cameras in the location of users, and to forward the user request to service providers [71]. Fog-based privacy preservation technique [72], implemented fog servers to store encrypted data, and users are provided with decryption keys from the location service provider. Keys are generated based on the region of division; therefore, vehicles entering the region will only be able to access the region key. In [73], TTP servers are replaced by fog servers to eliminate single point failure attacks and to store cache data.

8. Proposed Fog incorporated approaches

Based on previous deliberations, it is clear that there is a strong need for privacy preservation techniques that makes existing privacy policies more user-friendly. In addition, the integration of fog servers will bring enormous benefits to service users, service providers and global green computing benefits [74]. Resources between the source (end users) and the destination (cloud servers) are referred to as fog resources.

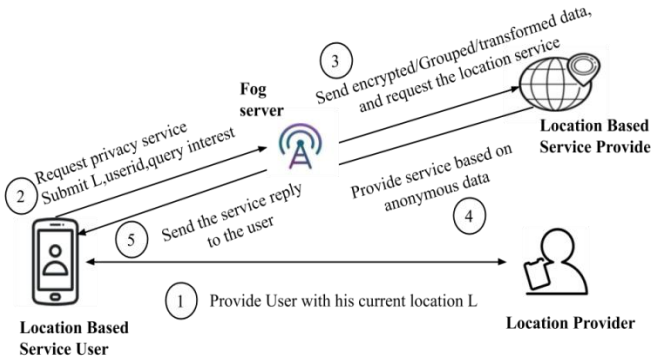

Figure 5: Trusted third party as fog server

8.1. Fog Server as TTP

The architecture of fog server as intermediate server is shown in Figure 5. The user obtains the current location from the location provider and then sends the user's identity, current location, and query interest to the fog server. A fog server also receives a request from other service users. The user-identity is hidden and the query is sent to a location-based service user as an anonymous query using a fog server. Service response from the location-based service provider is sent to fog server, and fog server finally segregates user response and forwards it to service users.Fog servers are intermediate servers set up by fog service providers at the edge of the network with the help of edge resources. The fog servers are proposed to establish at the locations where the fog services are required the most (based on the number of tasks forwarded to the cloud from that location). The fog servers established in such locations can act as the TTP servers for privacy protection models. The local map information can be stored in fog servers for easy updates and retrievals.

The research gaps identified are

- Frequency of the cache data update

Fog servers are deployed with available idle resources from end-users [75] and therefore have fewer resources than the cloud. Cache memory in fog is used for faster access to location-based data stored in fog [73]. Cache memory must be updated on the

basis of the newest data accessed by users. It is therefore necessary to focus on updating the cache memory frequency based on the availability of the cache memory and to use the cache efficiently.

- Optimal utilization of fog resources

The fog resources are deployed at each location based on the requirements and the focus of utilizing the resources optimally plays a major role in fog services. Fog resource optimization focused on recent works [76] [77]emphasizes the importance of optimized resource utilization in fog services.

- Security issues in fog storage

Fog computing services are expected to face many security issues other than those inherited from cloud [78] Cloud servers are deployed and maintained by a single party, while fog servers take on a variety of deployment options, such as end-users, cloud providers, and internet providers [79]. Trust issues while using e-commerce services, insiders attack fog providers, secure data storage and authentication issues prevail in fog services [80].

8.2. User collaborative approach

The architecture of user collaborative fog incorporation is shown in Figure 6. Intially, the users from a proximity colloborate into a group and a group representative is chosen among them.Then each user obtains the current location from the location provider, then sends the user's identity, current location, and query interest to the fog server as a group request. A fog server also receives a request from other service users groups. The user-identity is hidden and the query is sent to a location-based service user as an anonymous query using a fog server. Service response from location-based service provider is sent to fog server, and fog server finally segregates user response and forwards it to service users. Further, the group representative segragates the users request and sends it to each user. In this approach two level anonymization is achieved, one at user level and the other at fog server level.

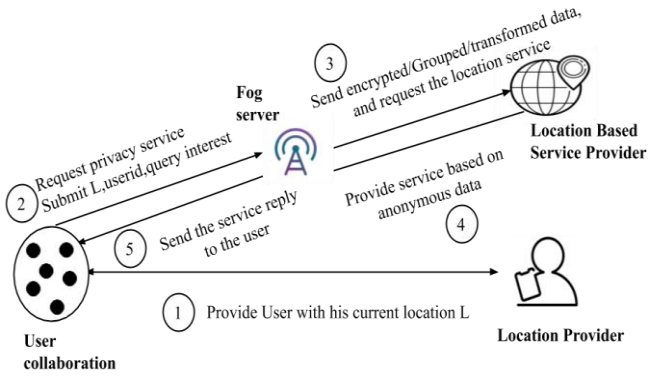

Figure 6: User collaborative approach incorporating fog

User collaborative techniques reduce the risk of third party dependence; however, they increase the burden on the user side. Peer-to-peer computing [81] is gaining popularity due to the increasing number of smart devices and their computational capabilities. Users are reluctant to establish peer-to-peer computation as there is a need to establish trust between peers. The key challenge is to establish cooperation between devices owned by different individuals [82]. Influenced by online social networking sites, individual social relations are on the rise every day [83]. Consider, for example, a device user from home interacts with a friend in the office or a family member in the neighborhood. These interactions will set up a device-to-device relationship to work together for peer computational task. Relationships are established in the framework of mutual cooperation. However, for the benefit of others,no device voluntarily establishes communication. In such situations, the previous history of device assistance helps the devices to help eachother. Incentive mechanisms will bring satisfactory benefits for users of devices in order to build a fair relationship between devices.

The ultimate aim of collaborative computing is to establish a user group that is physically or socially connected. These group members exchange their privacy attributes, such as their identity, location and query in order to acquire privacy-friendly location-based services.

The research gaps identified are

- Defining trust between users

Trust between users during collaboration is critical in collaborative approaches. In collaboration with a group, no single user must leave the system until all the users in the group are prompted to benefit equally. Trust models are developed based on user history, and online or offline user relationships.

- Central authority to manage the user group

The group's central representative leads the group in a positive direction in the models of user collaboration. The selection of a central group representative is an open issue in collaborative strategies.

- Automated dynamic group formation

The pervasive nature of mobile devices always forms a dynamic group, as proximity users are not always the same. The policy focusing on the benefit of the group members must push LBS users to join the secure LBS group.

- Incentives for the collaborative members

Collaborative user work is being developed to eliminate third-party servers [77]. Voluntary involvement of users in collaboration is difficult because users become greedy and are unable to use their resources for the benefit of others. Incentive mechanisms for such collaborative models are needed to encourage users to participate in collaboration, where a user acting as a representative will receive incentives from all other users [84]. The implementation of an effective reward system will ensure productive cooperation between users.

9. Conclusion

The location-based services are increasingly gaining significance along with the increasing utilization of mobile devices. The survey presents an overview of the evolution of the privacy preservation models of location-based services. The work describes the current research attainment of fog-integrated models of privacy preservation for location-based services. The research benefits and issues are described in detail and the opportunities to integrate the fog into the current user-collaboration approach and trusted third party approach are proposed. The research outcomes

provide a better understanding of the current research scenarios of privacy preservation techniques and future directions in integrating advanced computing paradigms such as fog computing in the privacy preservation approaches. The survey provides directions for many fog integrated robust privacy approaches in order to gain market adoptions soon.

References

[1] J. Raper, G. Gartner, H. Karimi, and C. Rizos, "A critical evaluation of location based services and their potential," *J. Locat. Based Serv.*, vol. 1, no. 1, pp. 5–45, 2007.

[2] Ryan Goodrich, "Location-Based Services: Examples and Uses," *Https://Www.Businessnewsdaily.Com*, 2013. [Online]. Available: https://www.businessnewsdaily.com/5386-location-based-services.html. [Accessed: 06-Dec-2019].

[3] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2009, pp. 348–357.

[4] W. Luo, Y. Lu, D. Zhao, and H. Jiang, "On Location and Trace Privacy of the Moving Object Using the Negative Survey," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 1, no. 2, pp. 125–134, 2017.

[5] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An efficient privacy-preserving location-based services query scheme in outsourced cloud," in *IEEE Transactions on Vehicular Technology*, 2016, vol. 65, no. 9, pp. 7729–7739.

[6] J. Chen, K. He, Q. Yuan, M. Chen, R. Du, and Y. Xiang, "Blind Filtering at Third Parties: An Efficient Privacy-Preserving Framework for Location-Based Services," *IEEE Trans. Mob. Comput.*, vol. 17, no. 11, pp. 2524–2535, 2018.

[7] "Cisco Fog Data Services," 2015. [Online]. Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/fog-data-services/index.html. [Accessed: 17-Apr-2019].

[8] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial-anonymity driven privacy enhancement scheme in continuous location-based services," *Futur. Gener. Comput. Syst.*, vol. 94, pp. 40–50, 2019.

[9] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Inf. Sci. (Ny).*, vol. 387, pp. 165–179, 2017.

[10] D. Wu, Y. Zhang, and Y. Liu, "Dummy location selection scheme for k-anonymity in location based services," in *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, 2017, pp. 441–448.

[11] Q. A. Arain *et al.*, "Clustering Based Energy Efficient and Communication Protocol for Multiple Mix-Zones Over Road Networks," *Wirel. Pers. Commun.*, vol. 95, no. 2, pp. 411–428, Jul. 2017.

[12] G. Li, Y. Yin, J. Wu, S. Zhao, and D. Lin, "Trajectory Privacy Protection Method Based on Location Service in Fog Computing," in *Procedia Computer Science*, 2019, vol. 147, pp. 463–467.

[13] T. Rodden, A. Friday, H. Muller, and A. Dix, "A lightweight approach to managing privacy in location-based services," in *2 nd International workshop on mobile commerce*, 2002, no. Equator-02-058, pp. 15–24.

[14] C. Bisdikian *et al.*, "Intelligent pervasive middleware for context-based and localized telematics services," in *Proceedings of the ACM International Workshop on Mobile Commerce*, 2002, pp. 15–24.

[15] A. Dey and L. Barkuus, "Location-Based Services for Mobile Telephony : a Study of Users ' Privacy Concerns," in *IFIP Conference on Human-Computer Interaction*, 2013, pp. 702–712.

[16] L. Barkhuus, "Privacy in Location-Based Services, Concern vs. Coolness," 2004.

[17] H. Xu, H. H. Teo, and B. C. Y. Tan, "Predicting the adoption of location-based services: The role of trust and perceived privacy risk," in *Association for Information Systems - 26th International Conference on Information Systems, ICIS 2005: Forever New Frontiers*, 2005, pp. 897–910.

[18] V. Johnson, R. Torres, B. Phillips, and A. Rahnamaee, "Continued Usage of Location-Based Services: Privacy Risk Impact on Motivation and Adoption," *Inf. Q.*, vol. 1, no. 1, pp. 1–17, 2014.

[19] C. Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems*, 2006, pp. 171–178.

[20] C. Y. Chow, M. F. Mokbel, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," *ACM Trans. Database Syst.*, vol. 34, no. 4, pp. 763–774, 2009.

[21] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for location-based services," *2014 IEEE Int. Conf. Commun. ICC 2014*, pp. 957–962, 2014.

[22] C. Zhang and Y. Huang, "Cloaking locations for anonymous location based services: A hybrid approach," *Geoinformatica*, vol. 13, no. 2, pp. 159–182, 2009.

[23] F. Liu, K. A. Hua, and Y. Cai, "Query l-diversity in Location-Based Services," in *Tenth International Conference on Mobile Data Management: Systems, Services and Middleware , IEEE.*, 2009, pp. 436–442.

[24] S. Wang and X. Sean Wang, "In-device spatial cloaking for mobile user privacy assisted by the cloud," in *Proceedings - IEEE International Conference on Mobile Data Management*, 2010, pp. 381–386.

[25] Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, "L2P2: Location-aware location privacy protection for location-based services," in *Proceedings - IEEE INFOCOM*, 2012, pp. 1996–2004.

[26] H. Zhu, F. Liu, and H. Li, "Efficient and Privacy-Preserving Polygons Spatial Query Framework for Location-Based Services," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 536–545, 2017.

[27] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-Based User Location Anonymization under Real-World Constraints," *IEEE Access*, vol. 4, pp. 673–687, 2016.

[28] M. Zeng, K. Zhang, J. Chen, and H. Qian, "P3GQ: A practical privacy-preserving generic location-based services query scheme," *Pervasive Mob. Comput.*, vol. 51, pp. 56–72, 2018.

[29] S. Zhang, K. K. R. Choo, Q. Liu, and G. Wang, "Enhancing privacy through uniform grid and caching in location-based services," in *Future Generation Computer Systems*, 2018, vol. 86, pp. 881–892.

[30] J. Zhang, X. Wang, Y. Yuan, and L. Ni, "RcDT: Privacy Preservation Based on R-Constrained Dummy Trajectory in Mobile Social Networks," *IEEE Access*, vol. 7, pp. 90476–90486, 2019.

[31] G. Sun *et al.*, "Location privacy preservation for mobile users in location-based services," in *IEEE Access*, 2019, vol. 7, pp. 87425–87438.

[32] H. Huang, G. Gartner, J. M. Krisp, M. Raubal, and N. Van de Weghe, "Location based services: ongoing evolution and research agenda," *J. Locat. Based Serv.*, vol. 12, no. 2, pp. 63–93, 2018.

[33] "Location-Based Services Market Predicted to Hit $157.34 billion by 2026." [Online]. Available: https://www.alliedmarketresearch.com/press-release/location-based-services-market.html. [Accessed: 06-Dec-2019].

[34] "Global mobile phone internet user penetration 2019 | Statista," 2018. [Online]. Available: https://www.statista.com/statistics/284202/mobile-phone-internet-user-penetration-worldwide/. [Accessed: 06-Dec-2019].

[35] J. Bell, "Angry Birds and ' leaky ' phone apps targeted by NSA and GCHQ for user data," *The Gaurdian*, 2014. [Online]. Available: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data. [Accessed: 05-Dec-2019].

[36] O. Jan, A. J. Horowitz, and Z. R. Peng, "Using global positioning system data to understand variations in path choice," *Transp. Res. Rec.*, no. 1725, pp. 37–44, 2000.

[37] A. Y. Xue, R. Zhang, Y. Zheng, X. Xie, J. Huang, and Z. Xu, "Destination prediction by sub-trajectory synthesis and privacy protection against such prediction," *Proc. - Int. Conf. Data Eng.*, pp. 254–265, 2013.

[38] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2005, vol. 3674 LNCS, pp. 185–199.

[39] K. Fawaz, H. Feng, and K. G. Shin, "Anatomization and Protection of Mobile Apps Location Privacy Threats," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 753–768.

[40] R. Gupta and U. P. Rao, "Achieving location privacy through CAST in location based services," *J. Commun. Networks*, vol. 19, no. 3, pp. 239–249, 2017.

[41] M. Han *et al.*, "Cognitive Approach for Location Privacy Protection," *IEEE Access*, vol. 6, pp. 13466–13477, 2018.

[42] W. Sheng, H. Jiafeng, Z. Hui, W. Hanyi, and L. Fenghua, "A collaboration-based scheme for location-based services with incentive mechanism," *Chinese J. Electron.*, vol. 27, no. 2, pp. 310–317, 2018.

[43] T. Dimitriou and N. Al Ibrahim, "'I wasn't there'—Deniable, privacy-aware scheme for decentralized Location-based Services," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 253–265, 2018.

[44] R. Dewri and R. Thurimella, "Exploiting service similarity for privacy in location-based search queries," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 374–383, 2014.

[45] R. Schlegel, C. Y. Chow, Q. Huang, and D. S. Wong, "Privacy-Preserving

Location Sharing Services for Social Networks," *IEEE Trans. Serv. Comput.*, vol. 10, no. 5, pp. 811–825, 2017.
[46] S. Wang, Q. Hu, Y. Sun, and J. Huang, "Privacy Preservation in Location-Based Services," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 134–140, 2018.
[47] T. Peng, Q. Liu, and G. Wang, "Enhanced Location Privacy Preserving Scheme in Location-Based Services," *IEEE Syst. J.*, vol. 11, no. 1, pp. 219–230, 2017.
[48] X. Pan, J. Xu, and X. Meng, "Protecting location privacy against location-dependent attacks in mobile services," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 8, pp. 1506–1519, 2012.
[49] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mob. Comput.*, vol. 7, no. 1, pp. 1–18, 2008.
[50] S. Zhang, G. Wang, M. Z. A. Bhuiyan, and Q. Liu, "A Dual Privacy Preserving Scheme in Continuous Location-Based Services," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4191–4200, 2018.
[51] J. Cui, J. Wen, S. Han, and H. Zhong, "Efficient Privacy-Preserving Scheme for Real-Time Location Data in Vehicular Ad-Hoc Network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3491–3498, 2018.
[52] H. Lu, C. S. Jensen, and M. L. Yiu, "PAD: Privacy-area aware, dummy-based location privacy in mobile services," *MobiDE 2008 - Proc. 7th ACM Int. Work. Data Eng. Wirel. Mob. Access*, pp. 16–23, 2008.
[53] T. Peng, Q. Liu, and G. Wang, "Privacy preserving for location-based services using location transformation," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8300 LNCS, 2013, pp. 14–28.
[54] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Comput. Commun.*, vol. 31, no. 6, pp. 1181–1191, 2008.
[55] F. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner, "Achieving efficient query privacy for location based services," 2010.
[56] A. Pingley, N. Zhang, X. Fu, H. A. Choi, S. Subramaniam, and W. Zhao, "Protection of query privacy for continuous location based services," in *Proceedings - IEEE INFOCOM*, 2011, pp. 1710–1718.
[57] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proceedings - IEEE INFOCOM*, 2014, pp. 754–762.
[58] Y. Li, W., Li, C., & Geng, "APS: Attribute-aware privacy-preserving scheme in location-based services," *Informtion Sci.*, 2019.
[59] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, "Location and trajectory privacy preservation in 5G-Enabled vehicle social network services," *Journal of Network and Computer Applications*, vol. 110. pp. 108–118, 2018.
[60] T. Peng, Q. Liu, G. Wang, Y. Xiang, and S. Chen, "Multidimensional privacy preservation in location-based services," *Futur. Gener. Comput. Syst.*, vol. 93, pp. 312–326, 2019.
[61] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *Proceedings - IEEE INFOCOM*, 2014, pp. 244–252.
[62] H. Niu, B., Zhu, X., Lei, X., Zhang, W., & Li, "Eps: Encounter-based privacy-preserving scheme for location-based services," in *IEEE global communication conference*, 2013.
[63] Z. Liu, L. Wu, J. Ke, W. Qu, W. Wang, and H. Wang, "Accountable Outsourcing Location-Based Services With Privacy Preservation," *IEEE Access*, vol. 7, pp. 117258–117273, 2019.
[64] P. Zhao, J. Li, F. Zeng, F. Xiao, C. Wang, and H. Jiang, "ILLIA: Enabling k-Anonymity-Based Privacy Preserving Against Location Injection Attacks in Continuous LBS Queries," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1033–1042, 2018.
[65] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 93–105, 2016.
[66] Y. Qu, S. Yu, L. Gao, W. Zhou, and S. Peng, "A hybrid privacy protection scheme in cyber-physical social networks," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 773–784, 2018.
[67] Jianhua Lin, "Divergence Measures Based on the Shannon Entropy," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 145–151, 1991.
[68] M. Aazam and E. N. Huh, "Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2015, vol. 2015-April, pp. 687–694.
[69] Cisco, "Cisco Fog Computing Solutions : Unleash the Power of the Internet of Things," *White Pap.*, pp. 1–6, 2015.
[70] Y. He, J. Ni, B. Niu, F. Li, and X. (Sherman) Shen, "Privbus: A privacy-enhanced crowdsourced bus service via fog computing," *J. Parallel Distrib. Comput.*, vol. 135, pp. 156–168, 2020.
[71] Y. Tian, M. M. Kaleemullah, M. A. Rodhaan, B. Song, A. Al-Dhelaan, and T. Ma, "A privacy preserving location service for cloud-of-things system," *J. Parallel Distrib. Comput.*, vol. 123, pp. 215–222, 2019.
[72] S. Liu, A. Liu, Z. Yan, and W. Feng, "Efficient LBS queries with mutual privacy preservation in IoV," *Veh. Commun.*, vol. 16, pp. 62–71, 2019.
[73] T. Wang *et al.*, "Trajectory Privacy Preservation Based on a Fog Structure for Cloud Location Services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.
[74] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: A green computing paradigm to support IoT applications," *IET Networks*, vol. 5, no. 2, pp. 23–29, 2016.
[75] Y. Sun and N. Zhang, "A resource-sharing model based on a repeated game in fog computing," *Saudi J. Biol. Sci.*, vol. 24, no. 3, pp. 687–694, 2017.
[76] V. Mushunuri, A. Kattepur, H. K. Rath, and A. Simha, *Resource optimization in fog enabled IoT deployments*. 2017.
[77] O. Skarlat, M. Nardelli, S. Schulte, M. Borkowski, and P. Leitner, "Optimized IoT service placement in the fog," *Serv. Oriented Comput. Appl.*, vol. 11, no. 4, pp. 427–443, Dec. 2017.
[78] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," in *Mobile Networks and Applications*, 2019, pp. 1–10.
[79] O. Skarlat, S. Schulte, M. Borkowski, and P. Leitner, "Resource provisioning for IoT services in the fog," in *Proceedings - 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications, SOCA 2016*, 2016, pp. 32–39.
[80] F. Alghamdi, S. Mahfoudh, and A. Barnawi, "A Novel Fog Computing Based Architecture to Improve the Performance in Content Delivery Networks," *Wirel. Commun. Mob. Comput.*, pp. 1–13, Jan. 2019.
[81] D. S. Milojicic *et al.*, "Peer-to-Peer Computing," 2003.
[82] S. Ye, F. Makedon, and J. Ford, "Collaborative automated trust negotiation in peer-to-peer systems," *Proc. - 4th Int. Conf. Peer-to-Peer Comput. P2P2004*, pp. 108–115, 2004.
[83] M. Nitti, G. A. Stelea, V. Popescu, and M. Fadda, "When social networks meet D2D communications: A survey," *Sensors (Switzerland)*, vol. 19, no. 2, 2019.
[84] X. Li, M. Miao, H. Liu, J. Ma, and K. C. Li, "An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism," *Soft Comput.*, vol. 21, no. 14, pp. 3907–3917, Jul. 2017.