Wireless Personal Communications
https://doi.org/10.1007/s11277-019-06872-3

Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing

Zahrah A. Almusaylim[1] · **NZ Jhanjhi**[2]

Abstract
One of the recent trends of networking and mobile technology is mobile cloud computing (MCC) that provides rich computational, storage resources and services in clouds to mobile users. MCC applications provide a variety of services to users and one of them is the location-based services (LBS) applications that are widely spread. By using mobile applications and LBS, mobile devices act as a thin client where the abundant data locations are collected and stored at the mobile cloud to provide corresponding services. Privacy of the user's location has been a renewed research interest and extensively studied in recent years. However, privacy is one of the most important challenges in MCC because the user's location on mobile devices is offloaded from mobile devices to cloud providers which can be utilized by third parties. Since protecting the privacy of the user is the key to maintain the trust on the mobile environment. LBS faces issues in protecting privacy such as, the privacy of user's current location, which may contain private information. In case, if the user's current location is compromised through unauthorized access, it possibly results in severe consequences. Therefore, protecting location privacy of the user while achieving precise location is still a challenge in MCC. This comprehensive research review will provide the challenge of protecting the privacy of user's location in MCC; analyze several related works regarding the issue. In addition, it suggests possible solutions related to the issue, in lighted few shortcomings which still needs attention with few related case studies.

Keywords Mobile computing · Cloud computing · Mobile cloud computing · LBS · Location-aware · Privacy · Encryptions

✉ Zahrah A. Almusaylim
zahra.almusaylim@hotmail.com

NZ Jhanjhi
noorzaman.jhanjhi@taylors.edu.my

[1] Department of Computer Science, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia

[2] School of Computing and IT (SoCIT), Taylor's University, Lakeside Campus, Subang Jaya, Malaysia

Published online: 17 October 2019

1 Introduction

The mobile computing (MC) in terms of mobile devices is considered as the current technological revolution in the world. Nowadays, people use mobile devices as the necessity of daily life. The users of mobile devices have much experience of how to use mobile applications that offer different services to help them to get their desires at their fingertips [1, 2]. One of the services provided by mobile computing is location-based services (LBS) which takes advantage of global positioning systems (GPS) sensor to provide the capability of searching for certain locations. Nevertheless, this service suffers from privacy concerns as the data location can be breached or disclosed if unauthorized users can track or misuse the collected or stored information in the service. Featured Research by GSMA Intelligence [3] showed that the milestone of the mobile industry was in year 2017. Where the number of users that are connected to the mobile services globally exceeded 5 Billion where the developing marketing took around 3.7 Billion. As such, by 2017, there were two out of three users had a subscription for mobile in the world. In 2025, the mobile devices industry will be in new leading milestone where there will be new internet users, unique subscribers, and 4th Generation/5th Generation (4G/5G) connections. Moreover, statistics were done by Statista [4] showed the worldwide total number of mobile users from 2013 to 2019. By 2014, the users of smartphone devices were about 38% of the total number of mobile users. Figure 1 is shown that the total number of users of mobile phone devices is forecast to increase from 4.43 Billion in 2015 to reach more than 5 Billion in 2019. In 2017, the worldwide number of users who used smartphone devices were expected to reach 4.77 Billion. And it was expected to reach about 50% in 2018 (4.93 Billion), where it is expected to exceed 5.07 Billion in 2019. In a time span of 5 years, this number is expected to grow by one billion worldwide. Due to the continuous improvement of software and hardware devices of the mobile devices, this leads to increase the number of mobile users. However, due to the challenges of mobile computing such as battery life, storage, bandwidth and etc., it is failing to meet the massive requirements of users and their full satisfaction [5–7]. Hence, organizations emerged the computing resources from room servers into

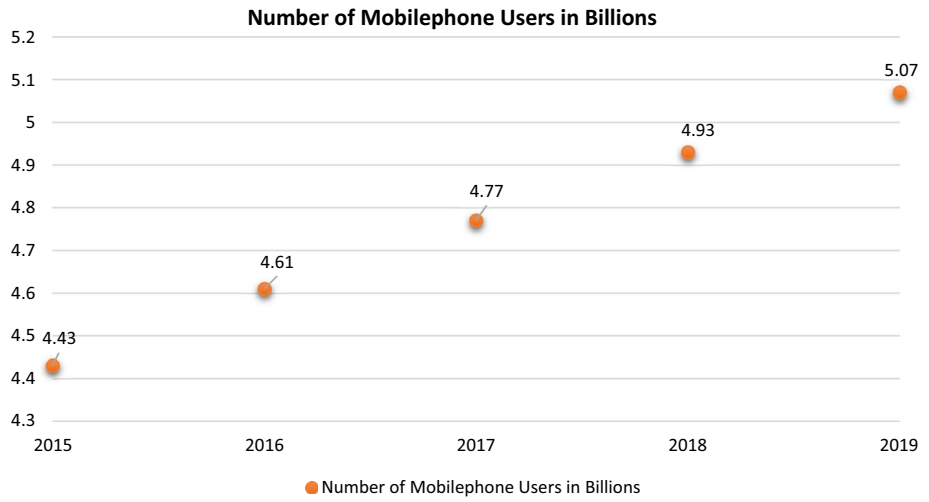

Fig. 1 Number of smartphone users [4]

mobile service providers. Then, they encouraged users to shift from using personal computers to data centers of mobile service providers [8].

Cloud computing (CC) is the current revolution technology with its growth in the IT field and it has become popular and accepted over the world. It takes the advantages of a collection of different concepts such as storage, connectivity, distributed computing, grid computing, virtualization, sharing, and processing power. Nowadays, cloud services have become the top priorities for customers as they offer unlimited storage and on-demand services which allow the customer to pay per use only [9–11]. The objective towards CC is to get the benefit of using distributed resources and solving the problem of the large-scale computation. These resources are shared among users and they can access them at any time from anywhere [12]. For example, users by utilizing CC can store and access their data remotely into the cloud. The cloud can offer on-demand high-quality services and applications from shareable pools of resources. Thus, users can relieve the burden on mobile devices into the cloud [10]. Report by Gartner in [13] said that estimation of the total number of cloud shift in IT from traditional services into cloud services is going to be around $111 Billion while in 2020. The cloud shift is going to affect more $1 Trillion in IT spending. The CC has three architectures that provide services which are: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). It has four deployment models that show how the resources in the cloud are shared which are: public cloud, private cloud, community cloud, and Hybrid cloud. Further details about them are elaborated in [11, 14–23].

The highly increased usage of data sensors such as GPS in the application of hungry resources mobile devices are costly because they restrict the devices providing the best services to the user. Consequently, offloading computation, data and other resources of mobile devices to remote thick resources servers is the main objective of CC [24]. Hence, the concept of mobile cloud computing (MCC) has been introduced to address the limitations of resources consumption of mobile devices in which the CC environment is integrated with MC [25]. The client/server architecture concept determines which one of them handles the tasks of computing the operations. If the tasks are computed in the client side and it is independent of the server side, then it is called a thick client/thin server. And if all the tasks of the client side are shifted and computed in the server side, then it is called a thin client/thick server where the client is dependent on the server. The concept of thin client/thick server is used in MCC in which the term MCC means that the running of different applications like for example running Gmail App for mobile from Google on a remote thick server. While the mobile devices can be a thin client which are connecting through the internet over remote thick server [26]. By this integration, it allows users to exploit and utilize resources in efficient and an on-demand manner with the goal of providing end users with better services and experience [27]. The applications of MCC have the ability to be executed on low or thin resource mobile devices. With MCC, mobile users can obtain their valuable data and real-time information at anytime from anywhere with the use of cloud services. The two deployment models of CC which are public cloud and private cloud are emerged in the MCC to provide mobile users with more efficient services. The MCC has a general architecture as it is shown in Fig. 2 which includes: (1) mobile devices have connection with mobile networks functional interfaces and control that are established via base stations, (2) the request and information of mobile user are forwarded to central processors of the mobile networks to provide mobile network services through connection to servers, (3) then through connection to the Internet, the request of the subscribers are delivered to the cloud and (4) finally, cloud controllers in the cloud process the request and send back the corresponding cloud services to the mobile users [28].

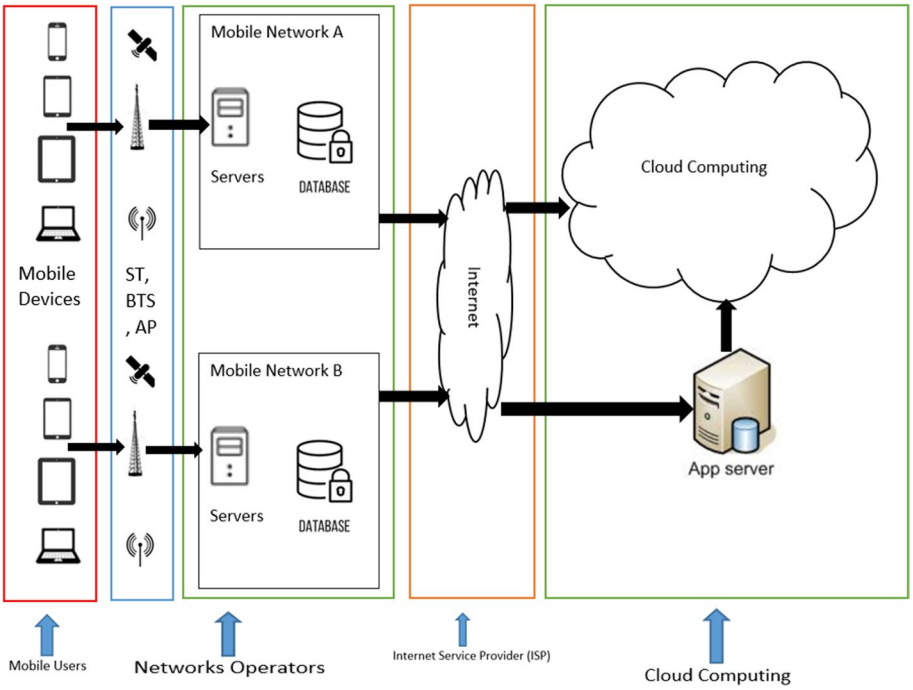

Fig. 2 MCC architecture [29, 30]

MCC faces many challenges and issues as they are highlighted by authors in [31] in six different perspectives including end users, operations, data management, context-awareness, application services, security and privacy as in Fig. 3 that shows a taxonomy of the current research issues in MCC. Privacy is one of the most important challenges because the user's private data in mobile devices is computed and offloaded from mobile devices to the cloud providers which have a distributed heterogeneous feature. One of the features of the advanced mobile devices is when a user can search for a certain location with the assistance of GPS sensor and Internet connectivity [32]. Recently, the increased popularity of LBS raises critical privacy concerns due to the massive amount of private location information which are outsourced to the cloud for processing and storage. The location information is considered private because it cloud be linked with other important information if for example they are shared on social networks. Then, processing the accurate location of users can infer significant information about them such as their home location, when they leave and arrive home, their interests, etc. [33].

This research provides a comprehensive review about protecting the privacy of the user in location-aware services of MCC and the most recent work to address this challenge. Also, this research suggests the possible solutions for it and identifies few issues that need to be pursued further. The paper is organized in a pattern such as introduction, literature review, discussion, and conclusion.

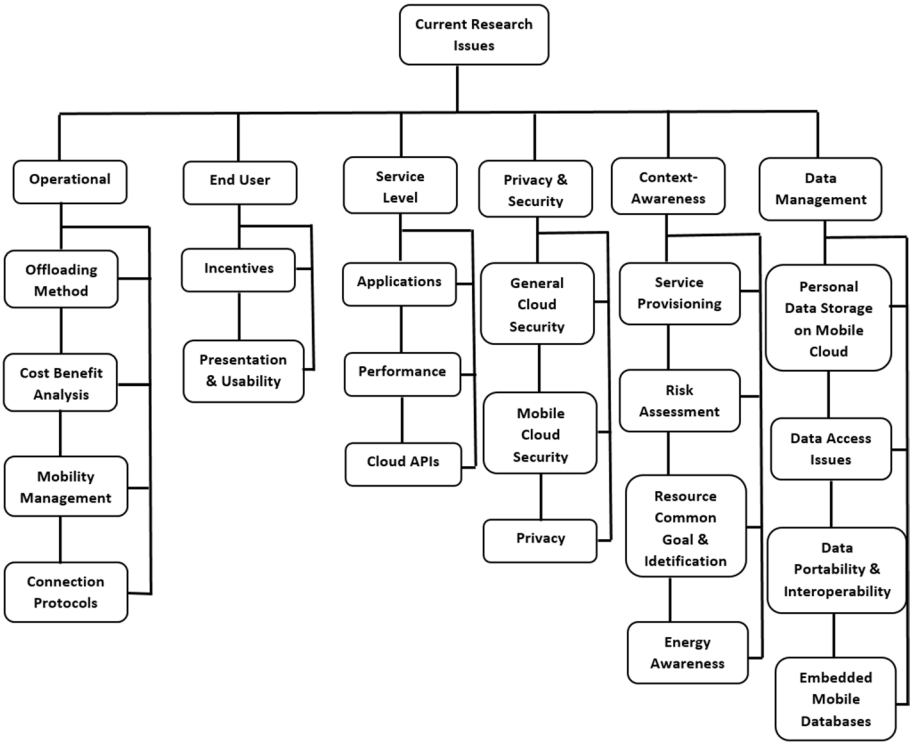

Fig. 3 A taxonomy of current research issues in MCC [31]

2 Literature Review

Many researchers in the literature have proposed several studies in the area of LBS in recent years. In this section, we review and discuss the challenges related to the user's location privacy in MCC based on recently conducted researches. Further, this section reviews the related work for protecting user's location privacy in MCC.

LBS can be defined as a set of mobile applications that harness the geographical location of the mobile device to provide services based on that location [34]. Via LBS, a user can query any location and get its services such as finding nearby locations, search for homes, stores or getting routing information of current traffic conditions [32, 35]. An example of LBS usage is when taking a picture with the smartphone's camera where the location is embedded in the picture. Moreover, the user can upload it to social media applications such as Facebook. So the location which is already embedded in the picture is shown on the map automatically by the system and it can be shared by the users' friends on Facebook [36]. The LBS can track the user's location, for example, the health status of the user could be inferred from the number of times that LBS is requested so it can detect the user's location that is close to hospital [37]. However, as the current mobile applications can execute, collect and store their data in the mobile cloud [38], therefore the location queried by the user is outsourced to the mobile cloud for processing and providing the corresponding result to the user [39]. MCC is curious to analyze and infer user's location to get more information that may be considered as private information to him.

Privacy of user's location refers to protect users from an unintended usage of data location [40]. Location privacy risks happen by the functionality of LBS that stores and collects historical location information in MCC in which query location may disclose private sensitive information of the user such as current location, identity or the query content. The LBS involves privacy leakage because the progress of the services depends on the movements of the user. These services require the users to provide them with who they are and what they want to know. While other services may expose the interests of the users and consumption records within their location through some applications. The personal private information such as habits and interests can be leaked or misused by adversaries, spam advertising or personal injury events such as robbery or tracking [41]. Hence, once the adversary captures the data service, the privacy of user's location can be compromised, which may lead to infer the individuals' sensitive information [42]. For example, if users' location information is collected by mobile social networks, then it may be provided to third parties for different purposes such as commercial or advertisement. This causes privacy leakage of user's location [43]. Consequently, using the location context in the LBS that contains personal information that is highly significant to the user can substantially breach the privacy of him and become the main reason for people abandoning LBS. Table 1 shows how different social media mobile applications can track the privacy of user's location.

The following subsection presents an overview of some approaches/techniques that are used for protecting the privacy of the user's location.

Table 1 User's location privacy tracking by different social media apps

Mobile application	Tracking user's location
Facebook	It can track user's location for multiple reasons such as letting others know where he is, checks- in certain places, tag it on posted pictures or uses the location to serve up ads
Google Apps	They collect data location with user permission and allow the services to make informed guesses on user's location and habits. They use implicit location information in which Google interprets search for a specific location as an evidence that the user is going to visit the location and then targets related ads based on this information. Also, they can track a user's offline location and behavior and sell the collected data to third parties
Instagram	It collects data location based on where the users post photos. When the user adds geotags to his photo, these data will be recorded and given an idea of where he spends his time which helps to post ads relevant to where he lives
Snapchat	The snap map feature of Snapchat lets users track other people's location in real time raising privacy concerns and advocates where the exact location of the user is going to appear on the map and this creates risks even without the user posts any snap like for example if the user is home alone or walks alone at night so this creates a risk when his contacts on Snapchat see from the map he is walking alone
Uber	It had a controversial feature that allowed the company to track the user's location even when he is not using the application or not sharing his location or during the pickup or after drop off. And they collected the user's location only for five minutes after the ride is completed. Later on, this feature has been removed to improve the user's privacy

2.1 K-Anonymity

The idea of K-anonymity is to group the users into k users groups and to hide the precise location of the real target user among other k users. It emphasizes that the target user is indistinguishable among $k-1$ users. Therefore, the probability of the target user to be identified is 1/k [44]. Through location anonymizer, an expanded query location of the user is sent to the server. The Cloaking Region (CR) of the expanded location can cover another user $(k-1)$ geographically instead of the precise location of the queried location. Consequently, the untrusted servers are unable to identify the precise location of the user among the other $k-1$ fake locations. However, to achieve k-anonymity model, a trusted third party (TTP) is required in which it will transform the original query location of the user into another region or will blur the exact location of the user into cloaked regions. Since the TTP has knowledge about the user's sensitive information, hence it can be easily a target of attacks. On the other hand, using the k-anonymity approach has some limitations such that using the location anonymizer can lead to a single point of failure. Since if the attacker has access to it, then the user privacy will be breached. Then it suffers from a performance of bottleneck because of using location anonymizer and the way of selecting fake locations to achieve k-anonymity is a challenge [45].

2.2 Transformation

The idea is to transform the query location in a secure way, so the cloud server of the LBS server would not able to distinguish the user's location. It is based on two techniques: (1) Non-Spatial in which cryptographic protocols are applied to provide strong privacy. But this approach needs high communication and computation costs and (2) Spatial Transformation in which the user's location is modified by the geometric transformation [46]. This approach has a trade-off between privacy and precision.

2.3 Dummy Location

In the dummy location, a set of fake locations that are randomly selected and the true locations are submitted to the server by mobile devices to provide protection for the user's true location. This approach does not need a Trusted Third Party (TTP) to transfer the original user's location. However, this approach suffers from heavy communication and computation costs due to choosing a large number of dummy locations by mobile devices.

2.4 Mix Zones

Mix zones are defined in which all users' locations are hidden within these zones. It is done by not allowing mobile devices to submit any location updates to the server. Hence, if the user enters any particular zone, his identity will be mixed with other users in the same zone by changing his name or pseudonyms [44]. However, this approach has a drawback in which it demands careful control of the number of users entered in the mix zones [47].

2.5 Private Information Retrieval (PIR)

PIR protocols allow users to submit their location queries to the server without detecting the request. The users can retrieve from the server without discovering which request is retrieved. These protocols are grouped into (1) computational, (2) secure hardware, and (3) information theoretic. However, there is a tradeoff between efficiency and privacy in this approach [48].

Protecting the privacy of user's location has been a concern for researchers. Some of the studies proposed to store the user's location in MCC in an encrypted manner so a secure sharing of location information can be achieved [41, 49–58]. Homomorphic encryption technique [59, 60] is widely used due to its simplicity and efficiency. Using homomorphic encryption, computation can be done on encrypted data without the need of decryption key. The study in [61] proposed a privacy-preserving localization scheme for protecting the privacy of user's location information in the cloud from attackers and untrusted servers. It is based on the homomorphic encryption technique which allows performing localization in an encrypted manner and the decryption of data is performed on the device. Hence, there is no leakage of the location information of the device because no unencrypted data is passed through the cloud server that cannot understand the computed results of the device's context. The system architecture is depicted in Fig. 4. The system works by allowing the mobile device to measure the signals of location and encrypt it. Then, only the encrypted version of the location is sent to unreliable cloud servers. After the cloud servers receive the encrypted location, they perform the process of localization. Finally, the result of that location information is sent back to the mobile device, so that it can be decrypted. This technique achieves a higher level of privacy with less complexity and there is no effect on the accuracy of the positioning results in the cloud. The authors in [46] proposed privacy-preserving architecture that provides secure mechanism over untrusted cloud server for LBS services anonymously. The users are prevented from the direct explosion of LBS

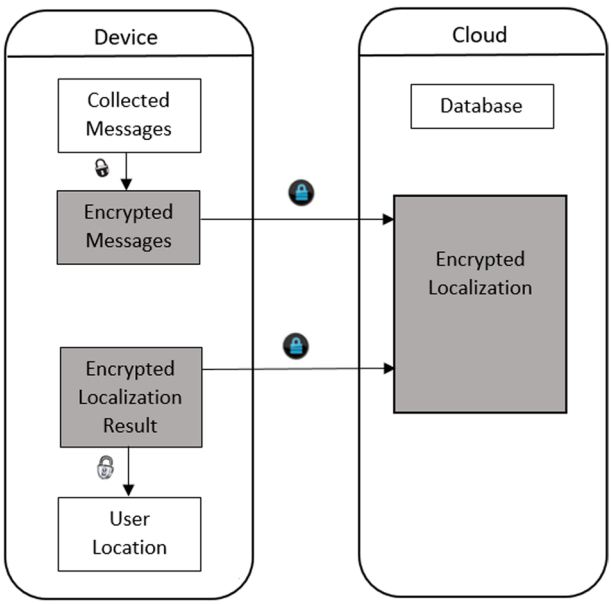

Fig. 4 The system architecture of privacy-preserving localization scheme [61]

providers when they query for a location. By using the hashes of the users' devices IMSI in the cloud server for authentication of malicious users, they are identifying them as a threat. The transformation is one of the studies that are proposed which transforms the query in a safe manner so that the server cannot identify the user's location. This approach uses two techniques: non-spatial that employs cryptographic protocols to provide privacy, and spatial that is based on changing user's location through geometric transformation. Zhu et al. [62] proposed efficient privacy-preserving LBS query where location information is preserved and kept secret from both LBS provider and cloud server. This is because the query location of the user and LBS data are computed in the cloud server without involving the LBS provider. The system consists of four components as Fig. 5 is showing which are: (1) Trusted Authority: for system initialization and sending system parameters to LBS provider and cloud server, (2) LBS Provider: for outsourcing data to the cloud server and providing system registration of users, (3) Cloud Server: for storing the encrypted data from LBS provider and providing users with query services and (4) The LBS User: who can query a location from LBS provider and obtain services based encrypted query from cloud server. The scheme employs improved homomorphic encryption with a special spatial range query algorithm constructed over Composite Order Group. Then, it protects the privacy of the user's location and provides good computation and communication costs.

Some researchers have been studied Attribute-Based Encryption (ABE) techniques [63] in which the location information is encrypted by the publishers. Also, the fine-grained access policies have been defined and the encrypted location information with access policies are outsourced to the mobile cloud. Only authorized users (queriers) can access the location information. Therefore, to provide access control mechanism Zhu et al. [38] introduced a fine-grained access control for LBS in the Cloud-Based SpatioTemporal Predicted-Based Encryption (ST-PBE) which is constructed on Key Policy Attribute-Based Encryption (KP-ABE) encryption [64]. It is implemented based on a secure cryptographic integer comparison supporting different types of spatiotemporal comparison based constraints in the LBS. The system architecture in Fig. 6 consists of three parts which are: (1) Mobile User who can have only authorized access to the data in LBS provider, (2) LBS Provider that can send location query to cloud provider for processing and can provide encrypted location information services to users according to their queries and (3) Certification

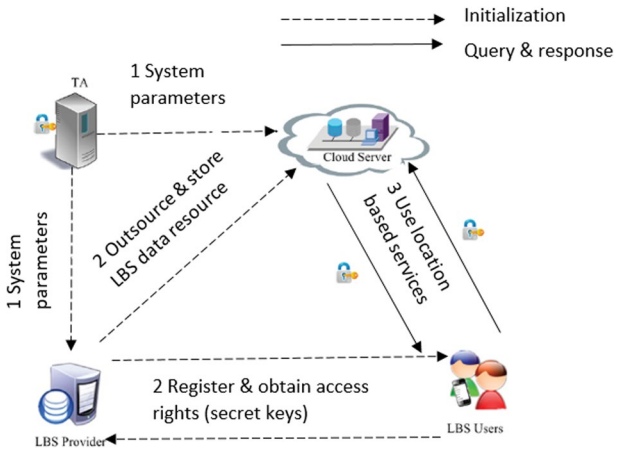

Fig. 5 System model of an efficient privacy–privacy location-based services query (EPQ) scheme [62]

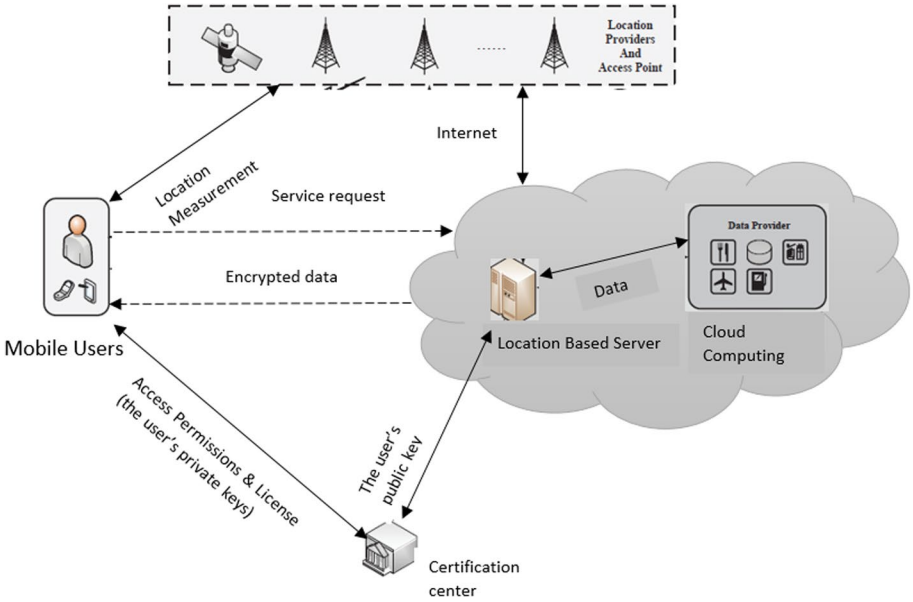

Fig. 6 System architecture of location-based fine-grained access control (LFAC) mechanism [38]

Center which is a Trusted Third Party (TTP) to issue certificate to users. The approach simplifies location authentication, access control as well as user privacy protection.

However, CP-ABE [65] is more appropriate than KP-ABE because it allows the owner of location information to specify access policies over the data location. Therefore, authors of [37] proposed a framework for fine-grained access control that protects the privacy of LBS in mobile devices. It is based on a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technique which is integrated with the techniques of proxy re-encryption and transformation key. In their system model in Fig. 7, the users query a location through the LBS provider that outsources the encrypted data according to access policies to the cloud server. Then, the users can obtain location information service from the cloud server with their access rights that are corresponding to the access policies. It provides minimum computation and communication costs over huge resources consumption. It allows the owner of the location to specify access policies control directly over the encrypted data by using these policies and their associated attributes with private keys and ciphertext. Also, only users that their identities attributes satisfy the access policies defined by the LBS provider can have access to the location information which achieves privacy-preserving requirements. The k-anonymity is introduced to verify that the user can be identified with 1/k probability only. The user's location is partitioned into groups in which each group has a k number of users at least.

To provide dynamic location, a LBS for attribute-based fine-grained access control for mobile cloud constructed based on ABE in [66] is introduced. It provides minimum computation and communication costs over huge resources consumption by integrating ABE with proxy re-encryption techniques to offload computation to the cloud. The system architecture contains three entities which are: (1) Anonymizer that defines and broadcasts the cloaking area in a predefined time interval, (2) Location Service Provider that provides each user with contextual attributes time access, unforgeable exact location, etc. Users send

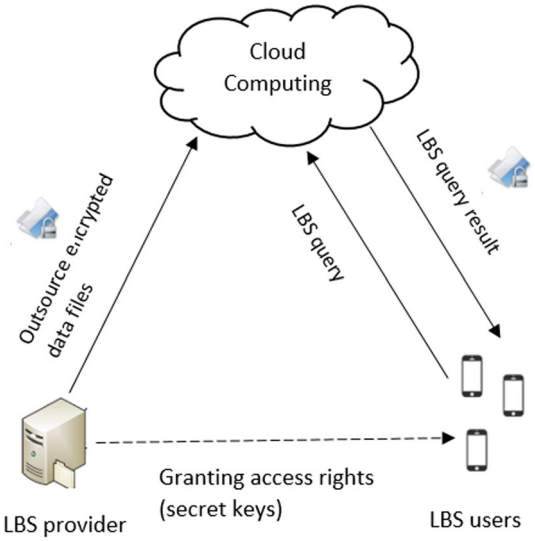

Fig. 7 Framework architecture of fine-grained privacy preserving location-based service (FINE) [37]

their encrypted query including th contextual information to anonymizer. Upon receiving k requests for a cloaking area, Anonymizing Spatial Region (ASR) is generated by the anonymizer that contains at least k users and performs k-anonymity cloaking and (3) Cloud Service Provider that receives a cluster of ASRs which defines for them a real-time access time. Then, the data is partially decrypted based on that time and other access policies for decryption computation cost to be outsourced. Reponses of k-queries are generated and sent back to anonymizer to filter them and to send them to users. Finally, only authorized users can decrypt the location information. The scheme provides an efficient dynamic location of mobile devices as context information does not change the private key of the device. Multi-authority attributes based access control is provided which protects users' authority and identity against unauthorized access. Anony Control is adopted [67] in the scheme to provide location anonymity by utilizing the coarse location as an attribute in the ABE to achieve k-anonymity and filter the results returned for more accuracy. Moreover, location privacy is supported by utilizing comparison based encryption based on CP-ABE that hides the exact location of devices from the server. Xie et al. [68] applied the RSA (for Rivest, Shamir, and Adleman) algorithm [69] based CP-ABE encryption technique to achieve fine-grained access control over encrypted location information. Their system model in Fig. 8 contains four components which are: (1) mobile cloud service provider that supports location-based query service, (2) a crowd of publishers that can share their data locations that are encrypted with mobile cloud, (3) many queriers that send request to mobile cloud service provider for location-based query service, and (4) trusted Authority that issues the key parameters. A location distance computed and a comparison over encrypted location are supported. Moreover, at the querier side, the computation cost is low and only authorized queriers can get the results.

The authors in [70] presented GeoSecure approach that is based on delta compression to compress the data location and maintain confidentiality as well as privacy. The data location is preserved and its confidentiality cannot be revealed or compromised. The first location coordinates are collected from mobile devices and the differentials are outsourced to the cloud service provider. Then, the cloud service provider (CSP) computes the distance

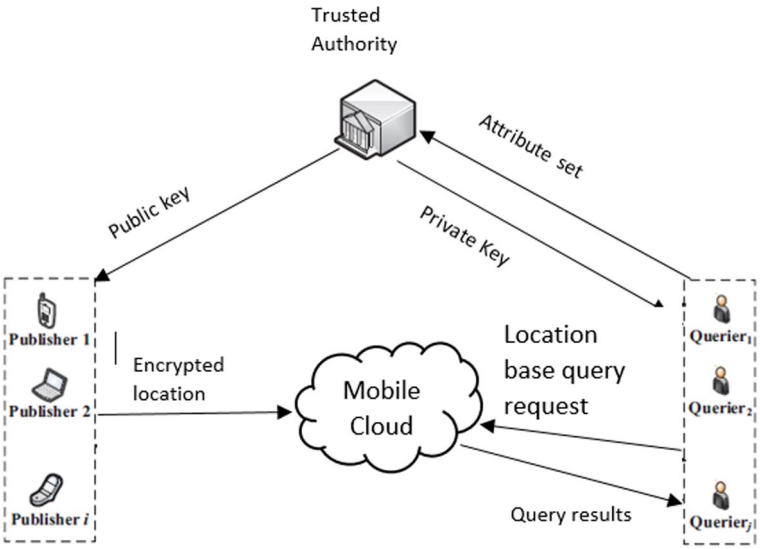

Fig. 8 System model of mobile cloud service system (MCSS) [68]

of differentials and utilizes it to determine different parameters. Using these parameters, users can obtain different location-based services such as distance traveled with different transportation modes. Baseri et al. [71] proposed an attribute-based access control with multi-authority (MA-ABE) scheme. It provides the user's anonymity and protects the user's identity against malicious authorities with the coexistence of authorities support. The mobile user's dynamic location is used as contextual information about him with his access policies and is authorized with the dynamic locations to satisfy the access policies. A proxy re-encryption is integrated with the scheme to (1) allow the secret information from authorities to be transformed and to protect the identity of the users from disclosure to the cloud server and (2) Allow the computation to be outsourced into the cloud server with limited computation costs. To outsource the LBS to the cloud in privacy-preserving manner, authors in [72] presented a solution for that. The scheme allows a search to be performed in the cloud while protecting the user's privacy queries and identity. Also, it keeps the data location confident from the cloud provider. Moreover, it allows users to query multi-location with continuous access control in an efficient way. And it provides a trade-off control between precision and privacy per query basis. Their system model in Fig. 9 consists of three components which are: (1) Location-based service provider that collects and encrypts data location, and before outsources them to the cloud service provider, it constructs an index for them, (2) client that registers itself with the location-based service provider to get the certificate and obtain the desired services, (3) cloud service provider that processes the encrypted query with the index and sends back the result to client. Authors in [73] proposed a privacy-preserving and an efficient LBS query based cloud scheme. Hybrid encryption is adopted in this scheme to protect the data location and the requests of users against the cloud server. The hybrid encryption encrypts the data location and queries that are outsourced to the cloud server. The cloud server provides accurate services for the queries by performing efficient and privacy-preserving search over the encrypted data location. Moreover, the scheme can allow flexible user enrollment and revocation mechanisms which are suitable for multiuser settings.

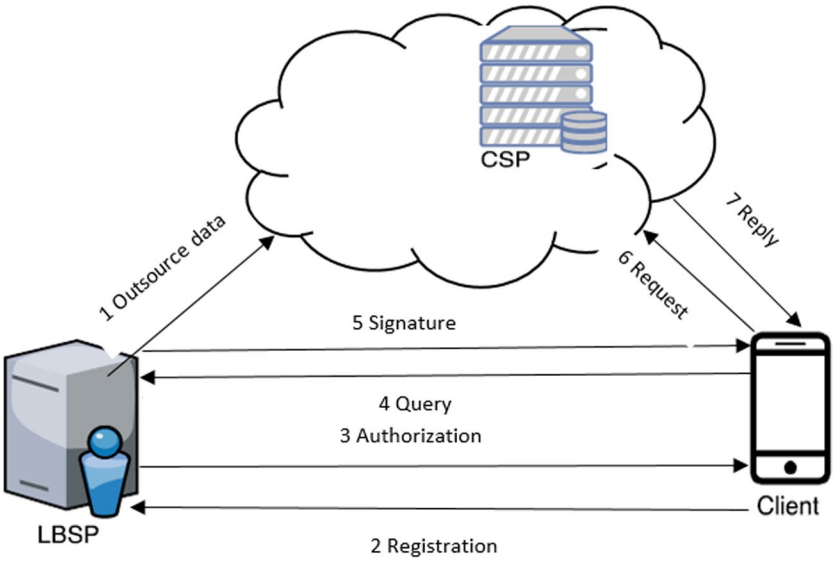

Fig. 9 System model of privacy preserving outsourced LBS system [72]

The literature review about improving the privacy of user's location in mobile cloud shows that developing effective and efficient frameworks for it is a challenge. This is because due to the amount of data location collected that needs to manage and allow only authorized users to access it to avoid privacy location violation. A detailed tabular critical comparison is provided in Table 2 below in terms of six criteria which are: encryption type, fine-grained access control, dynamic location support, multi-location query, anonymity, confidentiality, and future work in order to achieve protection of privacy for user's location in MCC. Therefore, based on the literature review, the contribution of the paper is as follow,

1. Introducing the concept mobile cloud computing (MCC) with protecting the Privacy of user's in location-based services (LBS).
2. Addressing the important points (for example, challenge of user's privacy [74], efficient computation of data outsourcing, etc.) in MCC for users.
3. Showing few techniques protecting user's privacy in one's location such as, K-anonymity, transformation, dummy location, mix zones and PIR.
4. Considering a design for a unified scheme to improve the challenge of privacy, of user's location in the future.
5. Identifying few open issues that need to be pursued further.

3 Discussion

In MCC, the location services have raised privacy concerns in mobile devices for their users. Knowing the user's location can deliver many services such as advertisement services in which they need to collect, store, process the data location that could be used in a way that violates the user privacy [5, 75]. The major outcome of our research review is

Table 2 Comparative of privacy protection of user in location-aware services of MCC

Scheme/functionality	Encryption type	Fine-grained access control	Dynamic location support	Multi-location query	Anonymity	Confidentiality	Future work
Privacy-preserving localization algorithm [61]	Homomorphic encryption	X	X	X	X	X	_
PPCCP [46]	AES encryption	X	X	X	✓	X	Cloud based environment Implementation Users can have more control over privacy
EPQ [62]	Homomorphic encryption with a special spatial range query algorithm	X	X	X	X	✓	Collusion attack consideration Low trust level in the cloud server
LFAC [38]	(SP- PBE) and (KP- ABE)	✓	X	X	X	X	_
FINE [37]	CP- ABE	✓	X	X	✓	✓	Reduce the cost on the cloud server. Low trust level in the cloud server.
MA attribute based access control [66]	ABE	✓	✓	X	✓	✓	Evaluate the performance of the work
MCSS [68]	(RSA) and CP- ABE	✓	X	X	X	X	_
GeoSecure [70]	Delta Encryption	✓	X	X	X	✓	Detect traffic congestion.
MA attribute based access control [71]	MA- ABE	✓	✓	X	✓	✓	_
Privacy preserving outsourced LBS system [72]	Function- hiding inner product encryption	✓	X	✓	X	✓	Support the search of k- nearest neighbor
Privacy-preserving multiuser LBS query scheme [73]	Hybrid encryption	X	✓	X	X	✓	Detect collusion attack in the cloud

comprehensive enough to grasp the challenge and the current studies for protecting the privacy of user's location in MCC with some shortcomings that need further studies. The study in [61] protects privacy of user's location only during the transmission and from the cloud server side, but it does not protect it from the user side. Also, the computation cost at the user side is high. In [46], the computation cost for finding nearest point of interest locations for each k users is big and requires more time. Comparing with other studies, the study in [62] does not take into consideration the various attacks and the level of trust in the cloud server. However, all the above studies do not provide mechanisms for access control policies. Because the framework in [38] is constructed based on KP-ABE technique and the use of associated attributes, then the owner of location information is unable to directly specify access policies of user's location. Also, the computation of the encryption technique used requires huge resource consumption. Also, both in [37] and [37], there will be a leakage of user's location information while searching for data patterns due to the trapdoors that are generated from locations. So they are always steady for the same location. Hence, the malicious user can count the number of trapdoors and identify their locations. Then, he can declare the fake location of the device and get unauthorized access to the information. Also, they do not support dynamic location of mobile devices. In [66] location distance computation is not supported. Due to the interaction between the queries that they access social networks via smartphones and publishers in [68], the publishers should always stay online and this is unacceptable because of the limited power of smartphones. The study in [70] does not provide detection for congestion traffic. The research in [72] does not support dynamic location and in [73] does not provide a solution for collusion attack in cloud-based and it does not support fine-grained access control. The solutions have several common features such as providing encryption scheme, supporting anonymity, supporting confidentiality, providing dynamic location query, providing multiple location queries and supporting fine-grained access control.

Based on critical review as of Table 2, we can observe that the best technique is the one that provides high protection for the user's location and provides efficient performance in terms of computation overhead and communication overhead. The researchers in [61] compared the computational complexity between the homomorphic and RSA methods. They observed that generally, the method of homomorphic encryption requires fewer operations (computation overhead) on end devices than the RSA method. The complexity of consumption decryption time of the algorithm is less sensitive to the number of Access Points (APs). The number of operations on devices are dominated by the sum of M and D (M is the number of APs and D is the dimension of the coordinates) in which the operations for addition is N, multiplication is M and mod function is M + D. On the other hand, the algorithm which they proposed requires zero operations on the cloud because the encryption procedure is ignored by the cloud in which the operations for addition is 0, multiplication is 0 and Mod function is 0. The privacy level improvement is obtained by the expense of extra decryption computation overhead. Nevertheless, though homomorphic encryption method on mobile device results in more consumption of energy, still it is very small on devices with high-level resources and capacities. The computation overhead and communication overhead are not evaluated in the study of [46]. The authors in [62] compared the computational complexity between the Spatial Range Query over Cipher-Text (SRQC) algorithm in an Efficient Privacy–Privacy Location-Based Services Query (EPQ) and Fine-Grained Privacy Preserving Location-Based Service (FINE) scheme. They observed that the computation cost overhead of the cloud server which is about 1-second increases slowly with the increase of the search region and range. Also, the computation cost overhead of LBS provider increases linearly with the increase of a number of resources. And the total computation cost overhead on the user's smartphone is less

than 200 ms and it is needed once communication only. The computation complexity of their scheme for user, cloud server and service provider respectively are shown in the following equations.

$$4 * C_e \tag{1}$$

$$2N * C_p * 4N * C_m \tag{2}$$

$$2N * C_p + 2N * C_m + 6N * C_e \tag{3}$$

While the computation complexity of the FINE scheme for User, Cloud Server, and Service Provider are shown in the following equations.

$$l * C_p + (2 + l) * C_m + 2l * C_e \tag{4}$$

$$2N\Delta x\Delta y * C_p + 5N\Delta x\Delta y * C_m + (4N\Delta x\Delta y + 2l) * C_e \tag{5}$$

$$2N * C_p + 3N * C_m + N(8N + 6) * C_e \tag{6}$$

It is obvious that their scheme achieved privacy preserving LBS with less computation complexity on the LBS provider, user, and cloud server. It solved the issue of the time-consumption effectively on LBS user and cloud server. The researchers of [38] presented the computational cost overhead of the basic cryptographic operations with experiment included 23 LBS requests, some location queries and some policies that are chosen randomly over a set of 7 attributes. They observed that the additional operations may take much more time. Consequently, the decryption overhead in service authentication is smaller than the overhead on the LBS data transmission because the expressions of the coordinates in LBS transmission are larger. However, the system performance is affected by different attributes and constraints but this effect is not very significant.

The researchers in [37] evaluated the performance of their proposed framework in terms of computation cost overhead and communication cost overhead including exponentiation and multiplication. The computation cost overhead at the user side including User Grant (UG) is 0 and Location Based Service (LBS) is $O(l)$. The bandwidth cost overhead at the user side including User Grant (UG) is $O(1)$ and Location Based Service (LBS) is $O(l)$. The computation cost overhead at the LBS provider side including System Initialization (SI) is O(1), Service Data Creation (SDC) is O(N), User Grant (UG) is O(N) and User Revocation (UR) is O(1). The bandwidth cost overhead at the LBS provider side including System Initialization (SI) is 0, Service Data Creation (SDC) is O(N), User Grant (UG) is O(N) and User Revocation (UR) is $O(1')$. The computation cost overhead at the cloud server side including Service Data Creation (SDC) is 0, User Grant (UG) is 0, User Revocation (UR) is 0 and Location Based Services (LBS) is O(N). The bandwidth cost overhead at the cloud server side including Service Data Creation (SDC) is O(N), User Grant (UG) is O(N), User Revocation (UR) is $O(1')$ and Location Based Services (LBS) is O(l). They observed that the computation cost overhead and communication cost overheads at the user side is low but they are high at the cloud server side.

The authors in [66] analyzed the computation cost overhead and communication cost overhead of their proposed scheme which is concerned with multiplication (M), exponentiation (E) and pairing (P). Nevertheless, their objective is to minimize the overheads of computation and communication cost at mobile users side. The computation cost at the user side for Setup is 0, Key Gen. (Dynamic) is 0, Encryption is 0, Acc. Req and Cloaking and Decryption respectively are shown in the following equation.

$$(6 + 2t)T_E \tag{7}$$

$$T_E + T_{ENC(ak)} \tag{8}$$

The communication cost at the user side for Setup is 0, Key Gen. (Dynamic) is 0, Encryption is 0, Acc. Req and Cloaking and Decryption respectively are shown the following equations.

$$(6 + 2t)^l G_{n'} \tag{9}$$

$$l_{G_{n'}} + l_{ENC(ak)} \tag{10}$$

The computation cost at the Data Owner (DO) side for Setup is 0, Key Gen. (Dynamic) is 0, Acc. Req and Cloaking is 0, Decryption is 0 and Encryption is shown the following Equation.

$$O(t)T_P \tag{11}$$

The communication cost at the DO side for Setup is 0, Key Gen. (Dynamic) is 0, Acc. Req and Cloaking is 0, Decryption is 0 and Encryption is shown in the following Equation.

$$l_{ENC(ak)} + (3 + 2t)_{l_{G_{n'}}} \tag{12}$$

The computation cost at the Location Service Provider (LSP) for Encryption is 0, Acc. Req and Cloaking is 0, Decryption is 0, Setup and Key Gen. (Dynamic) respectively are shown in the following equations.

$$(2K - 2)\left(T_M + T_E\right) \tag{13}$$

$$(K + 4)T_M + (17 + 2m)T_E \tag{14}$$

The communication cost at the LSP for Encryption is 0, Acc. Req and Cloaking are 0, Decryption is 0, Setup and Key Gen. (Dynamic) are shown the following equations.

$$(2K - 2)l_{G_{n'}} \tag{15}$$

$$(2K + 7)l_{G_{n'}} \tag{16}$$

They observed that the computation cost overhead and communication cost overhead are lower at the user side and hence their proposed scheme is convenient for smartphone devices. The researchers in [68] compared the computation cost overhead measured in (ms) of their scheme with the computation cost overhead of the PLQP scheme in [36]. The average computation cost overhead at querier (user side) for distance compute is 0.5944 in their proposed scheme while it is 1.9645 in PLQP. The average computation cost overhead at querier (user side) for distance compare is 0.6579 in their proposed scheme while it is 1.6195 in PLQP. The average computation cost overhead on the publisher for distance compute is 0 in their proposed scheme while it is 0.8524in PLQP. The average computation cost overhead on the publisher for distance compare is 0 in their proposed scheme while it is 0.6926 in PLQP. The average computation cost overhead on Mobile Cloud Service Provider (MCSP) for distance compute is 0.5130 in their proposed scheme while it is not mentioned in PLQP. The average computation cost overhead at MCSP for distance compute is 0.5172 in their proposed scheme while it is not mentioned in PLQP. It is obvious that their scheme has lower computation than PLQP at the querier side. Also, it is obvious that their scheme has lower computation cost than PLQP for both the location distance and compare as the MCSP contributes in the distance compute and compare instead of the publisher, while the PLQP does not use it for computation because it uses the publisher to interact

with the querier. Hence, their proposed scheme has zero computation cost at the publisher side. Overall, the computation cost overhead of each query in their scheme is lower than in the PLQP which makes it suitable to be put in practice. The authors in [70] did not provide an evaluation performance for the computation and communication overhead. The researchers in [71] evaluated the computation cost overhead and communication cost overhead of their work and compared them with the computation cost overhead and communication cost overhead in [37, 38] with a goal to reduce the computation cost overhead at the user side. The analysis was based on the static overhead caused by attribute of authorities to provide multi-authorities and dynamic overhead caused by location service provider (LSP) to provide location services. The static computation cost overhead of their proposed work is performed only once at registration time and every attribute authority is included only once at registration time. Therefore, it does not affect the efficiency of the scheme. The dynamic data access computation cost overhead of their proposed work at User (U) side for Key Gen is 0, Acc. Req is $5T_{E_G}$ and Dec is $T_{E_{G_T}}$. The dynamic data access communication cost overhead of their proposed work at U for Key Gen is $5l_G$, Acc. Req and Dec respectively are shown in the following equations.

$$\left(6 + 2|A_u|\right)l_G \tag{17}$$

$$l_{ENC} + l_{G_T} \tag{18}$$

The dynamic data access computation cost overhead of their proposed work at Location Service Provider (LSP) side for Acc. Req is 0, Dec is 0 and KeyGen is shown in the following equation.

$$(5 + 2m)T_{E_G} \tag{19}$$

The dynamic data access communication cost overhead of their proposed work at Location Service Provider (LSP) side for Key Gen is $6l_G$, Acc. Req is 0 and Dec is 0. The dynamic uploading computation cost overhead of their proposed work at Data Owner (DO) side for Encryption is shown in the following equation.

$$(1 + 2m + 2|t|)T_{E_G} + T_{E_{G_T}} \tag{20}$$

The dynamic uploading communication cost overhead of their proposed work at Data Owner (DO) side for Encryption is shown in the following equation.

$$l_{ENC} + (2 + 2|t|)l_G + l_{G_T} \tag{21}$$

It is observed that their scheme eliminated paring operations in the decryption that are a costly process with limited computation at the user side. Since the work in [38] does not support most of the functionalities support by the researchers' scheme, they only compared the computation performance with work in [37]. Although it is shown that the computation cost overhead in both key generation and decryption process are reduced to a negligible value at user side, work in [37] has a high level of computation cost overhead in both key generation and decryption process at location service provider (LSP) side. The authors in [72] evaluated the computation cost performance of their proposed solution by measuring the index of traversing to reach a location at a particular level. The computation overhead of the Query Generation is $O(n^2)$. While the search procedure which is divided into traverse tree, checking the condition of a node and retrieving the encrypted information has computation overhead of $O(\log N.n)$. It is observed that the time overhead of the Bloom Filter utilized by the blind signature for the search efficiency is negligible. Additionally, there is no communication overhead at the user side. The authors in [73] evaluated the

computation performance of their proposed scheme at LBS user side, LBS provider side and cloud server side. The computation cost overhead for LBS data encryption is raised linearly for different sizes of categories set with fixed a number of data location while the number of different data location has a slight impact on the computation cost overhead with a fixed size of category set. Hence, it is obvious that encrypting the categories in each category set has the most time consumption while encrypting the data location has roughly small time consumption for the scheme. The total computation cost overhead for producing a query request at LBS user side is efficient and almost 161 ms. The computation cost overhead of search on cloud server is effected slightly by the number of categories and data location while it is obvious that the response time is raised linearly with the increased number of query users which is efficient and about 6.82 s. However, the evaluation of communication overhead is not considered in this study. From the detailed comparison, we can observe that the most efficient scheme in terms of performance computation cost overhead and communication cost overhead and in terms of functionalities in the literature is privacy preserving location-based access control (PPLBAC) that is proposed by the researchers in [71]. The performance of PPLABC as compared is better than FINE [37] and LFAC [38] and the performance computation of ABE technique used for FINE is better than homomorphic technique that is already discussed in the previous sub section.

As a case study, we consider a user that uses Uber taxi car service, when he requests a ride by entering the destination address and setting his default pick-up according to the current GPS location of the user. From the moment that the user is picked-up until where he is dropped off to his destination, the app is able to track the user's location. It can track the user during the ride, and for five minutes after the user reaches his destination, and by doing this, it can give much more information to the service about the user. It could find out the users' daily routes, which way he goes after a fare and his habits just by following him around in the background. The app can collect the precise location data from its users at all the time when it is running in the foreground or the background which mean that even if it is not being used for the ride. However, if the Uber service is compromised due to any reason, then the users' data location that are unencrypted or not protected with anonymity can be compromised and easily accessed by the adversaries which mean breaching the user's privacy. Moreover, the app can save the historical records of the locations that the user requests them for a ride so it can retrieve them when it is requested again through the shortcut icon. And according to the study done by [76], it concluded that the short period of time between each or frequent requests location from mobile application lead to higher risks of privacy. Therefore, when Uber app updates or retrieves the user's location or destination location, this leads to increase the risk of user's location leakage due to the high rate of the request. Another case study is a user that uses a snap map location feature on the Snapchat application. This feature allows the user to track other users on a snap map and it can be used to view the snaps of others, as well as other features snaps like breaking news, sporting events and so on. It allows updates the user's location to appear automatically on other friends' snap map when he chooses to share his location. Then, the user can be seen on a virtual map with their precise location as shown in Fig. 10. Therefore, through this feature, the users can share their daily life activities like a user can see if his friend is riding a car and on what road he is driving. The dispute of the snap map comes from its accuracy in which zooming in on Snapchat users it shows where their home is exactly. Also, if a user has an unknown friend on Snapchat and he does not know him, he can track him wherever he is going. And anyone of the users' friends can see his location, even someone pretending to know him so this behavior can breach the user's privacy and this feature can be a harmful one.

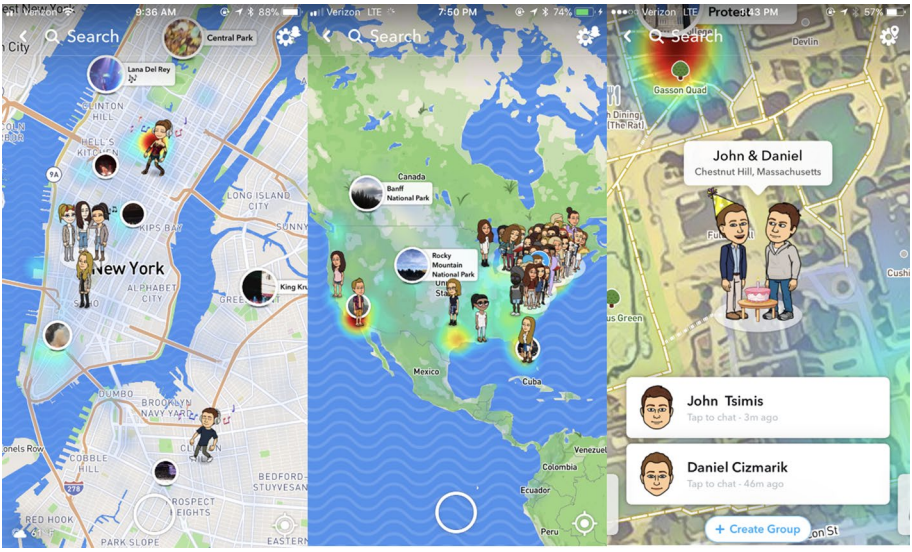

Fig. 10 Snap map feature of snapchat application [77]

Conclusively, by comparing all the approaches and the related work, there are several possible suggested solutions that should be taken into consideration while designing a unified scheme to improve the challenge of the privacy of user's location in the future. It includes that the privacy of user's location should be protected during transmission from both sides of the mobile users and cloud servers, it should allow the mobile users to have control over what location information to share with others, it should support multi-location query, it should support location compression to minimize the computation cost and it supports user revocation which is when the user leaves the system then his location information, attributes, and access rights should be revoked from the system directly. Moreover, from the above literature review, we can conclude there are some drawbacks that still found which are as follows: (1) The heavy computation and communication cost at cloud server side, (2) The need for reliable and highly precise location, (3) They do not provide long term consistency location protection, (4) They did not consider the trust level of honest but curious cloud to malicious that should be lower, (5) They do not support multi-authority feature to provide coexistence of users' authorities in which each authority issues part of the secret key instead of issuing it to a single authority and 6) They do not consider multi-location query feature that allows the user to scan location by an index only once time for multiple locations instead of scan it multiple times for a single location. Therefore, these shortcomings have considerable significance to be studied and addressed in order to protect the user's location.

4 Conclusion

One of the recent trends of networking and mobile technology is Mobile Cloud Computing that emerges both MC and CC which have been increased dramatically and provided optimal services to the users. MCC has inherited the characteristics of MC as well as CC,

and it has become a hot research area nowadays. However, MCC faces many challenges and one of them is the privacy of the user's location. Location privacy challenge raises by the functionality of LBS that stores and collects historical location information in MCC in which query location may disclose private information of the user's current location and the sensitive information about user's identity or the query content. The personal private information such as habits and interests can be leaked or misused by spam advertising, adversaries or personal harm events such as robbery or tracking. This research presents: (1) A comprehensive review for readers about the challenge of protecting the privacy of the user in location-aware services of MCC. (2) Presents and analyzes different approaches and set of research projects that are proposed recently for this challenge with their characteristics, advantages, and disadvantages. (3) A case study of Uber taxi car service, as well as Snap Map, and how the user's location is being tracked or leaked. (4) Suggesting some possible solutions with a unified scheme to improve the challenge of the privacy the user's location in future with efficient performance overhead and (5) Identifying few of the shortcomings that need to be pursued further related to protecting the privacy of the user's location. This research provides direction to other researchers to focus more on state of privacy issues to protect the user's location information on the mobile cloud while providing better services and experience to the users. As future work, we are extending our work to implement the suggested solution with including of multi-location query, multi-authority, location compression and user revocation.

References

1. Othman, M. (2017). Mobile computing and communications: An introduction. *Malaysian Journal of Computer Science, 12*(02), 71–78.
2. Bouazzouni, M. A., Conchon, E., & Peyrard, F. (2018). Trusted mobile computing: An overview of existing solutions. *Journal of Future Generation Computer Systems, 80,* 596–612.
3. Sivakumaran, M. Iacopino, P. (2018). The mobile economy 2018. Retrieved April 21, 2018, from https://www.gsmaintelligence.com/research/2018/02/the-mobile-economy-2018/660/.
4. Statista. (2015). Mobile phone users worldwide 2013–2019. Retrieved April 21, 2018, from https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.
5. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications, 84,* 38–54.
6. Paranjothi, A., Khan, M. S., & Nijim, M. (2017). Survey on three components of mobile cloud computing: Offloading, distribution, and privacy. *Journal of Computer and Communications, 05*(06), 1–31.
7. Sharma, M., & Kumari, R. (2018). Survey on mobile cloud computing: Applications, techniques, and issues. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 03*(01), 933–940.
8. Weng, W. H., & Lin, W. T. (2015). A mobile computing technology foresight study with scenario planning approach. *International Journal of Electronic Commerce Studies, 06*(02), 223–232.
9. Moghaddam, F. F., Ahmadi, M., Sarvari, S., Eslami, M., & Golkar, A. (2015). Cloud Computing Challenges and Opportunities: A survey. In *IEEE 1st international conference on telematics and future generation networks* (*TAFGEN*), 2015 (pp. 34–38).
10. Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: A critical review. *International Journal of Computer Network and Information Security, 06*(03), 20–29.
11. Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications, 60,* 113–129.
12. Ahmed, A. A., & Wendy, K. (2017). Mutual authentication for mobile cloud computing: Review and suggestion. In *IEEE conference on application, information and network security (AINS), 2017* (pp. 75–80).
13. Stamford, Conn. (2016). Gartner says by 2020 "cloud shift" will affect more than $1 trillion in IT spending. Retrieved April 22, 2018, from http://www.gartner.com/newsroom/id/3384720.

14. Sadiku, M. N., Musa, S. M., & Momoh, O. D. (2014). Cloud computing: Opportunities and challenges. *IEEE Potentials, 33*(01), 34–36.
15. Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). Cloud computing features, issues, and challenges: A big picture. In *IEEE international conference on computational intelligence and networks (CINE)*, 2015 (pp. 116–123).
16. Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials, 15*(02), 843–859.
17. Wang, S., Liu, Z., Sun, Q., Zou, H., & Yang, F. (2014). Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing. *Journal of Intelligent Manufacturing, 25*(02), 283–291.
18. Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Computing Surveys (CSUR), 47*(01), 1–47.
19. Shawish, A., & Salama, M. (2014). Cloud computing: paradigms and technologies. In: F. Xhafa, N. Bessis (Eds.), *Inter-cooperative collective intelligence: Techniques and applications* (pp. 39–67). Heidelberg: Springer.
20. Alam, M. I., Pandey, M., & Rautaray, S. S. (2015). A comprehensive survey on cloud computing. *International Journal of Information Technology and Computer Science, 2,* 68–79.
21. Durao, F., Carvalho, J. F. S., Fonseka, A., & Garcia, V. C. (2014). A systematic review on cloud computing. *The Journal of Supercomputing, 68*(03), 1321–1346.
22. Nandgaonkar, S. V., & Raut, A. B. (2014). A comprehensive study on cloud computing. *International Journal of Computer Science and Mobile Computing, 03*(04), 733–738.
23. Branch, R., Tjeerdsma, H., Wilson, C., Hurley, R., & McConnell, S. (2014). Cloud computing and big data: A review of current service models and hardware perspectives. *Journal of Software Engineering and Applications., 07*(08), 686–693.
24. Chen, M. H., Dong, M., & Liang, B. (2018). Resource sharing of a computing access point for multi-user mobile cloud offloading with delay constraints. *IEEE Transactions on Mobile Computing, 17*(12), 2868–2881.
25. Chen, M. H., Liang, B., & Dong, M. (2017). Joint offloading and resource allocation for computation and communication in mobile cloud with computing access point. In *IEEE conference on INFOCOM 2017-computer communications, IEEE* (pp. 1–9).
26. Li, R., Shen, C., He, H., Xu, Z., & Xu, C. Z. (2017). A lightweight secure data sharing scheme for mobile cloud computing. *IEEE Transactions on Cloud Computing, 06*(02), 344–357.
27. Rahimi, M. R., Ren, J., Liu, C. H., Vasilakos, A. V., & Venkatasubramanian, N. (2014). Mobile cloud computing: A survey, state of art and future directions. *Journal of Mobile Networks and Applications., 19*(02), 133–143.
28. Kumar, G., Jain, E., Goel, S., & Panchal, V. K. (2014). Mobile cloud computing architecture, application model, and challenging issues. In *IEEE international conference on computational intelligence and communication networks (CICN)*, 2014 (pp. 613–617).
29. Yan, Z., Li, X., & Kantola, R. (2017). Heterogeneous data access control based on trust and reputation in mobile cloud computing. In *Advances in mobile cloud computing and big data in the 5G era* (pp. 65–113). Cham: Springer.
30. Wu, X. (2018). Context-aware cloud service selection model for mobile cloud computing environments. *Hindawi Journal of Wireless Communications and Mobile Computing*, 1–14.
31. Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Journal of Future Generation Computer Systems, 29*(01), 84–106.
32. Marcelino, L., & Silva, C. (2018). Location privacy concerns in mobile applications. In *Developments and advances in intelligent systems and applications* (pp. 241–249). Cham: Springer.
33. Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., & Palamidessi, C. (2013). Geo-indistinguishability: Differential privacy for location-based systems. In *ACM proceedings of the 2013 ACM SIGSAC conference on computer & communications security* (pp. 901–914).
34. Singhal, M., & Shukla, A. (2012). Implementation of location based services in android using GPS and web services. *IJCSI International Journal of Computer Science Issues, 09*(01), 237–242.
35. Shankar, P., Huang, Y. W., Castro, P., Nath, B., & Iftode, L. (2012). Crowds replace experts: Building better location-based services using mobile social network interactions. In *IEEE international conference on pervasive computing and communications (PerCom)*, 2012 (pp. 20–29).
36. Li, X. Y., & Jung, T. (2013). Search me if you can: Privacy-preserving location query service. In *IEEE proceedings of INFOCOM*, 2013 (pp. 2760–2768).
37. Shao, J., Lu, R., & Lin, X. (2014, April). Fine: A fine-grained privacy-preserving location-based service framework for mobile devices. In *IEEE proceedings of INFOCOM*, 2014 (pp. 244–252).

38. Zhu, Y., Ma, D., Huang, D., & Hu, C. (2013). Enabling secure location-based services in mobile cloud computing. In *ACM proceedings of the second ACM SIGCOMM workshop on mobile cloud computing*, (pp. 27–32).
39. Tang, F., Li, J., You, I., & Guo, M. (2016). Long-term location privacy protection for location-based services in mobile cloud computing. *Journal of Soft Computing, 20*(05), 1735–1747.
40. He, T., Ciftcioglu, E. N., Wang, S., & Chan, K. S. (2017). Location privacy in mobile edge clouds: A chaff-based approach. *IEEE Journal on Selected Areas in Communications, 35*(11), 2625–2636.
41. Wang, S., Hu, Q., Sun, Y., & Huang, J. (2018). Privacy preservation in location-based services. *IEEE Communications Magazine, 56*(03), 134–140.
42. Wang, T., Zeng, J., Bhuiyan, M. Z. A., Tian, H., Cai, Y., Chen, Y., et al. (2017). Trajectory privacy preservation based on a fog structure for Cloud location services. *IEEE Access, 05,* 7692–7701.
43. Sun, G., Xie, Y., Liao, D., Yu, H., & Chang, V. (2017). User-defined privacy location-sharing system in mobile online social networks. *Journal of Network and Computer Applications, 86,* 34–45.
44. Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2014). A classification of location privacy attacks and approaches. *Pers Personal and Ubiquitous Computing, 18*(01), 163–175.
45. Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2014). Achieving k-Anonymity in Privacy-Aware Location-Based Services. In *IEEE Proceedings of INFOCOM*, 2014 (pp. 754–762).
46. Abbas, F., Hussain, R., Son, J., & Oh, H. (2013). Privacy preserving cloud-based computing platform (PPCCP) for using location based services. IEEE Computer Society. In *Proceedings of the 2013 IEEE/ACM 6th international conference on utility and cloud computing*, 2013 (pp. 60–66).
47. Paulet, R., Kaosar, M. G., Yi, X., & Bertino, E. (2014). Privacy-preserving and content-protecting location based queries. *IEEE Transactions on Knowledge and Data Engineering, 26*(05), 1200–1210.
48. Jagwani, P., & Kaushik, S. (2017). Privacy in location based services: Protection strategies, attack models and open challenges. In *International conference on information science and applications*, 2017 (pp. 12–21). Berlin: Springer.
49. Puttaswamy, K. P., & Zhao, B. Y. (2010). Preserving privacy in location-based mobile social applications. In *ACM proceedings of the eleventh workshop on mobile computing systems & applications*, 2010 (pp. 1–6).
50. Chen, Y. J., & Wang, L. C. (2011). A security framework of group location-based mobile applications in cloud computing. In *IEEE 40th international conference on parallel processing workshops (ICPPW)*, 2011 (pp. 184–190).
51. Jagwani, P., & Kaushik, S. (2012). Defending location privacy using zero knowledge proof concept in location based services. In *IEEE 13th international conference on mobile data management (MDM), 2012* (pp. 368–371).
52. Li, W., Jiao, W., & Li, G. (2012, October). A location privacy preserving algorithm for mobile LBS. In *IEEE 2nd international conference on cloud computing and intelligent systems (CCIS), 2012, 0*2, (pp. 548–552).
53. Yao, L., Wu, G., Wang, J., Xia, F., Lin, C., & Wang, G. (2012). A clustering K-anonymity scheme for location privacy preservation. *IEICE Transactions on Information and Systems, 95*(01), 134–142.
54. Sun, Y., Chen, M., Hu, L., Qian, Y., & Hassan, M. M. (2017). ASA: Against statistical attacks for privacy-aware users in location based service. *Journal of Future Generation Computer Systems, 70,* 48–58.
55. Xiao, X., Chen, C., Sangaiah, A. K., Hu, G., Ye, R., & Jiang, Y. (2017). CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks. Elsevier *Journal of Future Generation Computer Systems*.
56. Peng, T., Liu, Q., & Wang, G. (2017). Enhanced location privacy preserving scheme in location-based services. *IEEE Systems Journal, 11*(01), 219–230.
57. Rohilla, A., Khurana, M., & Singh, L. (2017). Location privacy using homomorphic encryption over cloud. *Proquest International Journal of Computer Network and Information Security, 09*(08), 32–40.
58. Wu, H., Wang, L., & Jiang, T. (2018). Secure and efficient k-nearest neighbor query for location-based services in outsourced environments. *Science Journal of China Information Sciences*, *61*(03), 1–3.
59. Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation, 04*(11), 169–180.
60. Gentry, C. (2009). *A fully homomorphic encryption scheme*. Ph.D. Thesis Stanford University.
61. Fang, S. H., Lai, W. C., & Lee, C. M. (2012). Privacy considerations for cloud-based positioning. In *IEEE 2012 12th international conference on ITS telecommunications (ITST)*, 2012 (pp. 527–531).
62. Zhu, H., Lu, R., Huang, C., Chen, L., & Li, H. (2016). An efficient privacy-preserving location-based services query scheme in outsourced cloud. *IEEE Transactions on Vehicular Technology, 65*(09), 7729–7739.
63. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In *Advances in cryptology- eurocrypt*, Volume 3494 of LNCS, (pp. 457–473). Berlin: Springer.
64. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *ACM proceedings of the 13th ACM conference on computer and communications security*, 2006 (pp. 89–98).

65. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *IEEE symposium on security and privacy*, 2007 (pp. 321–334).
66. Baseri, Y., Hafid, A., & Cherkaoui, S. (2016). K-anonymous location-based fine-grained access control for mobile cloud. In *13th IEEE annual consumer communications & networking conference (CCNC)*, 2016 (pp. 720–725).
67. Jung, T., Li, X. Y., Wan, Z., & Wan, M. (2015). Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. *IEEE Transactions on Information Forensics and Security, 10*(01), 190–199.
68. Xie, Q., & Wang, L. (2016). Efficient privacy-preserving processing scheme for location-based queries in mobile cloud. In *IEEE international conference on data science in cyberspace (DSC)*, 2016 (pp. 424–429).
69. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM., 21*(02), 120–126.
70. Patil, V., Parikh, S., Singh, P., & Atrey, P. K. (2017). GeoSecure: Towards secure outsourcing of GPS data over cloud. In *IEEE conference on communications and network security (CNS)*, 2017 (pp. 495–501).
71. Baseri, Y., Hafid, A., & Cherkaoui, S. (2018). Privacy preserving fine-grained location-based access control for mobile cloud. *Journal of Computers & Security, 73,* 249–265.
72. Zhu, X., Ayday, E., & Vitenberg, R. (2018). A privacy-preserving framework for outsourcing location-based services to the cloud. *Research report* http://urn. nb.no/URN: NBN: no-35645.
73. Ou, L., Yin, H., Qin, Z., Xiao, S., Yang, G., & Hu, Y. (2018). An efficient and privacy-preserving multi-user cloud-based lbs query scheme. In *Security and communication networks*, (pp. 1–11).
74. Almusaylim, Z. A., & Zaman, N. (2018). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Journal of Wireless Networks*, 1–12.
75. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In *IEEE In 2018 4th International Conference on Computer and Information Sciences (ICCOINS)* (pp. 1–5).
76. Iu, D., Gao, X., & Wang, H. (2017). Location privacy breach: Apps are watching you in background. In *IEEE 37th international conference on distributed computing systems (ICDCS), 2017* (pp. 2423–2429).
77. Kiess, K. (2017). Mappenstance: Snap map is more than just a map. Retrieved May 23, 2018, from https://blog.richmond.edu/livesofmaps/2017/11/03/snap-map-is-more-than-just-a-map/.

Zahrah A. Almusaylim She an assistant scientific researcher at King AbdulAziz for Science and Technology (KACST), Saudi Arabia. She earned her BSc in Computer Science in 2014 from College of King Faisal University, Saudi Arabia. She is currently pursuing her master in Computer Science at King Faisal University since 2015 up to date. Her area of interests include: Internet of Things, Cloud Computing, IoT Privacy and Security, Wireless Sensor Network, Security of RPL networks, Cloud Computing Security, Network Security, Mobile Computing, Context-Aware Computing, Machine Learning, Web and Mobile Applications Programming.

Dr. NZ Jhanjhi has 18 years of teaching and administrative experience internationally, authored several research papers in indexed and impact factor research journals and conferences, edited 11 international reputed Computer Science area books, focused on research students. He has successfully completed more than 18 international research grants. He is Associate Editor of IEEE Access, Guest editor of several journals, Regional Editor, and Editorial board member, PC member, reviewer for several reputed international journals and conferences around the globe. His areas of interest include Cybersecurity, IoT, WSN, Internet of Things IoT, Mobile Application Programming, Ad hoc Networks, Cloud Computing, Big Data, Mobile Computing, and Software Engineering.