A General Review on Location Based Services (LBS) Privacy Protection Using Centralized and Decentralized Approaches with Potential of Having a Hybrid Approach

Bessam A. Adem [1], Maen Alrashdan [2], Mohamed Abdulnabi [3], Ayman Jaradat[4], Mohammad Tubishat[5], Waheed Ali Ghanem[6] and Yusnita Yusof [7]
[1]tp037857@mail.apu.edu.my, [2]dr.maen@staffemail.apu.edu.my,
[3]mohamed.shabbir@staffemail.apu.edu.my, [4]A, [5]mtubishat@yahoo.com,
[6]waheedghanem@umt.edu.my, [7]yusnita@staffemail.apu.edu.my
[1,2,3,7]School of Computing and Technology, Asia Pacific University of Technology and Innovation, [4]Majmaah University, [5]Skyline University College, [6]Universiti Malaysia Terenganu

ABSTRACT

The online world is expanding with new features added frequently, new data generated exponentially, many users joining regularly and new services offered globally. Thus, sifting through such gigantic volumes of data to locate one's needs makes better sense if it is based on the user's current location. A person searching for list of amusement parks in Malaysia is not interested in those found halfway around the globe to be included in the search results. Similarly, online content that is meant to be available only to paid customers in Ethiopia should not be accessible by anyone elsewhere. Accordingly, online data processing and distribution has become vital and needs to be context-based. The core challenge in such an environment occurs when an adversary attempts to take advantage of users and/or service providers' vulnerabilities by either invading privacy of others or utilizing services they are not entitled to. In this paper, numerous concerns raised by LBS users and researchers are studied in great detail. Some of the major faults in LBS have been identified. The objectives of this research are to rigorously study and identify threats in LBS, propose enhanced framework and finally present the significance of the new approach. Previous studies focus on either centralized or decentralized LBS framework to protect users. This paper focuses on the combination of these two frameworks in order to benefit from the best aspects of each method. For this reason, an additional agent server to the general framework have been introduced in order to help eradicate the limited resources and vulnerability of smart devices thus creating safer location aware transactions among users and producers. The goal is to create a more secured environment for parties that will share location information without privacy breaches. Finally, the conclusion with summary of the findings, limitations and possible future enhancements.

Keywords: Location Based Services, Mobile Security, Privacy Protection, Location anonymization.

1. INTRODUCTION

In a world where many resources are readily available for online distribution, we shouldn't experience users attempting to get service form providers who cannot serve them because of location suitability. It is difficult to search and utilize a specific data that best caters to the users need in terms of their location. The solution is Location Based Services (LBS), which play a vital role in online transactions nowadays. In LBS technology, online users, mostly mobile users, are catered with online contents that best fit their respective geographical locations. This process will serve users efficiently with what they need based on their surroundings and save them the trouble of being bombarded with information that will not benefit them in any way. As it is implied in the above definition of LBS, the technology is mostly suitable for users that are in continuous motion. These users are commonly referred to as Mobile Users (MUs) as opposed to stationed users. Although, it is not to say that stationed devices or users will not benefit from LBS, it is widely applicable to those Mobile users who are constantly shifting locations and requesting different services that are suitable for them.

MUs can use software applications, commonly termed as mobile apps, on their devices to request numerous services that are offered by LBS providers. The LBS providers in return will serve the services based on the location of the MUs. This location can be provided by GPS, or a cellular network like GSM or even from the RFID + Bluetooth spots. Since the users are not stationed in a specific area, they must communicate to service providers and other MUs through a wireless communication channel, which are mainly designed and managed by Internet Service Providers (ISP). In addition to facilitating wireless networks, ISPs can provide mobile devices location based on the cellular network or other means. One vital thing about LBS is that whenever a user undergoes a certain transaction with any of the LBS providers, the integrity of the user will be at risk from different angles. For MUscto receive a certain service s/he has to generate private information about themselves, User Generated Content – UGC, and send it to the service providers through a wireless network. The private UGC, once it leaves the mobile device, is vulnerable either for third party attacks or misuse by LBS providers. Henceforth, keeping the safety of users while benefiting from the technology would concern everyone involved in the transaction. Many developments have been conducted and studied to overcome security and privacy concerns in LBS. However, there are always shortcomings in the developed system and more naturally, there are always new ways of attacking and misbehaving in the computer world.

The intensity of security and privacy challenges in Location Aware Services exacerbates due to the vast availability and usability throughout the world. In addition, with the advent of numerous useful applications integrated in the devices, users have grown to appreciate and prefer to use the devices on their daily routines and even in a more private transactions and data storage. Especially in the 21st century, where online services and mobile devices are being produced, distributed and utilized exponentially, it is apparent that the online world is in dire need for safer and robust LBS architecture.

One of the many ways to protect LBS users is by a technique called cloaking or anonymizing the private data, especially users' location. The technique involves hiding the actual locations of users and shuffling it with others in order to avoid being spotted while using a service from one of the providers. An ISP can take the role of creating a favourable environment for MUs and LBS providers to communicate. Alternatively, a third party security firm can provide a dedicated server called an anonymizers to provide the cloaking and/or anonymizing process.

Background

Encapsulation of private information can be done either by MUs themselves (called decentralized) or by dedicated anonymizers (called centralized) schemes. With each having their own advantages and disadvantages, this paper discusses the working structure and components of the latter.

The centralized framework has mainly three components: Anonymizer (trusted server), LBS Provider and MU as shown in figure 1(Gkoulalas-Divanis, Verykios, & Eleftheriou, 2009). There are many variations of the same architecture that uses a centralized dedicated server to encapsulate the location information of users. Figure 2 shows such variations but with basically similar skeleton of the centralized framework for LBS privacy (Mokbel & Chow, 2006). The MU will be using a secured connection to connect to the ISP wirelessly to request available online resources. An ISP (i.e. trusted body) will be hosting the dedicated server that will handle the anonymizing process. The LBS Provider serves the request of clients based on the information it receives from the anonymizer. Since the data it receives from ISP it is hidden and randomized, LBS provider use special algorithm to process queries and find appropriate resources to users without having to know their actual identity.

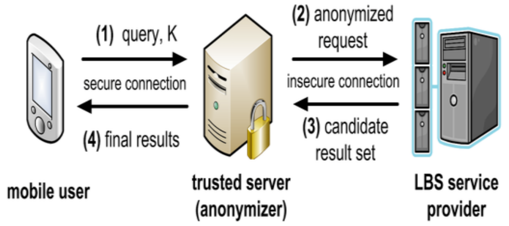

Figure 1: Centralized Framework for LBS privacy

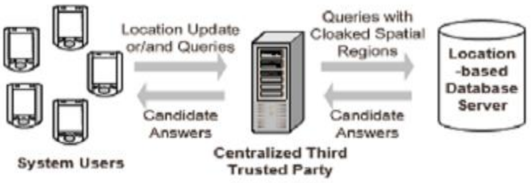

Figure 2: Casper Architecture – Variation of the centralized framework

According to Gkoulalas-Divanis, Verykios and Eleftheriou (2009) the anonymizing procedure takes several stages that starts from accepting service requests from mobile users. It then removes any private identifiers on the data and encrypts it before forwarding the request(s) to the service providers. An important role of the server, which is under ISP, is to cloak the actual location information to avoid the exposure of the exact location of users. There two major techniques of protecting users' personal data. The first one is known as Anonymity approach, which tends to shuffle users' data with other locally found users to disguise each one of them from the other. Anonymity approach can be achieved by simply merging users together to confuse attackers (historical anonymity), or creating a block of users and assigning users to random blocks (spatial anonymity), or by tracking regular route of users so as to find and block others trying to imitate (trajectory anonymity). The second type of technique actually hides the location data by either changing the actual figure of the location coordinates (obfuscation) or by disconnecting users from the regular trajectory and mixing their data with others for a short period before reconnecting them back to the service providers (unlinking). Saleh et al. (2020) mentioned the use of Web-based decision support systems by organizations to reduce the cost but not discussed the safety.

The centralized framework is chosen for this research over its counterpart, decentralized architecture, for a number of advantages that it has over it. As briefly mentioned above, the decentralized approach (also known as the distributed system) requires individual MUs to generate techniques to disguise their location as opposed to a dedicated central system. This approach generates few but critical disadvantages. First of all, there will be an added burden on each MU to create a pool of random location profiles that looks and works as if it is real. The added task requires MUs to have better and efficient processing capabilities. Moreover, since the server and service provider will be responding to each request as though they are real, it will create overwhelming load on all connected entities; not to mention the large bandwidth required to transfer all these to and from users. Hadidi et al. (2020) found the best selection of a system that improve the performance of organization.

Currently, the centralized framework suffers largely from location anonymization if and when adequate number of users are not found to satisfy the profile pool, out of which anonymity is created. In other words, if enough users are not present in proximity, mobile users are still vulnerable to be uniquely identified for lack of others to be shuffled with. In addition, at times, sufficient users could be present but not commuting to similar path. In such cases, it would still be difficult to cloak an MU who is on a unique route to his/her destination.

Problem Statement

Nowadays, location-aware services have become a very crucial part of our day-to-day online transactions. This fact is even more emphasized when dealing with vehicular devices that change locations in a continuous manner. The contents that are made available on the internet by users is growing exponentially both in variety and volume. Hence, it is to the utmost necessity to manage the type and amount of data a user gets based on the users' location. For best results and efficient data handling, only required information should reach a certain user that best fits his/her need, minimizing the time of search along the process. Location aware services also play an important role in terms of providing a better security that can change depending on the context of the area in which the device is located. Allocating data and a variety of services depending on a context makes it easier to find the data that users are most interested in and not to worry about superficial content that does not add a value to the intended online services.

Nonetheless, these services are not free from malicious attacks and misbehaving users. The servers that are providing the location-based services usually store profiles of users in order to make the best choice to what is appropriate to users. This creates a big gap in terms of users' privacy. An attack on the server could jeopardise users' sensitive information. In addition to this, misbehaving users can break into the mobile devices and act on behalf of legal users in order to gain the benefits that were intended to the legitimate user. The communication between servers and clients (mobile units) also has a greater risk in terms of security. A failure to authenticate users and secure the data transfer could lead to a breach in the service providers' data.

2. LITERATURE REVIEW

The internet has grown vastly both in diversity of services and coverage of geographical location since its inception in the early 1980s. It is an obvious reality that our current world is growing in a direction that we cannot escape many of the crucial services being handed to us by the ever-expanding internet. Moreover, with the advent of portable devices, the world's population has switched to utilizing the services in a vehicular mode where any service can be utilized in almost any location. Hence, disseminating the large internet data to individual users based on their location would create a more manageable and efficient flow. The **Google map** application, **Yelp** search engine and the **Foursquare** app, that claims to give meaningful customer experience based on location intelligence, are only a few examples of those who are taking advantage of location-based services (LBS) (Liu et al., 2016; Zhang et al., 2018). As computer networks grow along with many positioning systems, there is a natural growing demand for LBSs. Moreover, advancement of wireless networks to 4G and 5G that are equipped with identification of accurate location coupled with the high utilization of smart devices creates the opportunity to explore new means of personal navigation, entertainment, social networking, , personalized advertising, and many other location based services (LBSs) (L. Jin, Li, Palanisamy, & Joshi, 2018; Saravanan & Balasundaram, 2018; Zhang et al., 2018). However, LBS requires users to share their private information to gain access to the available services. Henceforth, users' privacy should be given the utmost priority to ensure information will not leak into perpetrators. Furthermore, the demand for LBS will eventually decline as users relent due to fear of exposing their privacy (Yang & Yan, 2019).

2.1 Location based services (LBS)

Location-Based Services are those techniques used to gather up-to-date data from certain regions and supply it to users based on their interest. Interests could range from traffic status to restaurant details and many other points of interest (H. Jin & Papadimitratos, 2019). Due to the advent of Geo-Positioning capabilities integrated in smart devices, novel services have emerged. These services are named Location-Based-Services or LBS that will use the geographical location of devices to provide numerous services suitable for users based on their locations. **Strava** and **Google Maps** are few of many examples that utilise this feature in mobile devices (Li, Salinas, & Li, 2013; Parmar & Rao, 2020b). Hence, these applications are labelled as MLBS which stands for Mobile Location-Based Services. MLBS could range from social networking where users can find nearby friends to a more serious and stringent transaction like crime investigation whereby a person's innocence could be identified based on his/her proximity to the crime scene. It can also be used in medical centres in which physicians would gain access to patients' profile only if they are found near the location of the patient(s). Most recently, MLBS has found a way into the gaming world rewarding player's points when they visit certain locations. Furthermore, MLBS can be used by business owners to distinguish and reward frequent customers by counting the number of times they visit their shops and/or branches. Alrahhal et al. (2020) explain that due to the advent of LBS human beings have started enjoying their lives that has been simplified because of it. One of such achievements is the implementation of LBS in Internet-of-Things (IoT) where many day-to-day devices like smart cars, smart wearables and other house/office devices are integrated into a network to facilitate easier and comfortable life. LBS can also be used in health sectors to monitor patients' status based on his/her whereabouts.

LBS can also be integrated into an area known as "m-business" which is business transactions that are conducted online using mobile devices. LBS plays vital role in improving the quality-of-service (Aloui, Kazar, Bourekkache, & Omary, 2020). An enhanced location-aware analytics system, called ELAN, developed by Liu et al (2016) claims to provide better services than the traditional map. The new system can provide users with useful inputs like locating most important activities in a given region for regular users, potential competitive businesses for those who want to start a new one, or even suggest government officials locations suitable for public facilities. In the latter case, ELAN scans through a given geographical location to find what public facilities are available for the general public and what are missing.

Security Risks and Attacks in LBS

Even if mobile users are enjoying useful LBS services that does not mean they are keen in sharing their private data with the rest of the world including the LBS providers. Consequently, MU's privacy gains utmost attention while working with all sorts of LBS applications. Many techniques have been developed to hide this highly regarded data (identity of users) so as to preserve their privacy. Nonetheless, hiding (cloaking) the users' identity may not always be sufficient. Adversaries can use the location information as a pseudo-identity of users to get their exact location and whereabouts. There are numerous methods introduced to as a response to the above concern. Preserving location information through merging the actual user with other generated dummies is one of the prevalent mechanisms (Parmar & Rao, 2020a).

According to Parmar and Rao (2020b), there are few types of attacks that can occur in LBS environment that uses a pseudo-location (dummy location) to anonymize mobile users (MU). One of these attacks is known as Map-matching in which the dummy locations can easily be eliminated by the attacker for not fulfilling a legitimate location criterion. For instance, the location could be unrealistic areas like water bodies or mountainous. Another type of attack, known as Centre-of-ASR (Anonymized Spatial Region), can occur if the original location of the user is used as the centre point of a region while dummy locations are populated around it randomly. In this case, even if there are many locations information scattered in a given area, it is possible to find only the central point to get to the actual position of the user. Similarly, Location-homogeneity attack can take place if the dummy locations are not scattered as far away as possible from the genuine mobile user. Since, many of the location data will be concentrated in a small area, it is rather easy to identify the actual mobile user. Moreover, anonymizing location information through pseudo data has challenges on both mobile users and anonymizing servers. If the dummy locations are generated by the user itself, it will create huge load of processing on the mobile device to generate, send and filter the data to and from LBS providers. On the other hand, LBS could be requested just once or continuously depending on the type of service. Unfortunately, many of the privacy frameworks are suitable either for one-time requests, or continuous requests and may not work well for both request types.

Kita et al. (2018) mention four types of attacks that can occur in a centralized privacy framework. The first of these attacks is known as "Location similarity attack" which occurs if all available locations are cramped into small area. In such cases, adversaries can easily narrow down their attack target. "Center-of-AS attack" is already being explained above (Parmar and Rao, 2020b) in section 2.3. "Brute force attack" occurs when an algorithm uses common distinguishable feature in creating dummy locations. If an attacker recognizes the common features among location units, it can easily be discarded, and the real user can be identified. The last and major type of attack is known as "Inference attack". This kind of attack happens when locations units are somehow connected to one another making it possible to navigate through all units trying to find the real location inferred by the dummies.

Yang and Yan (2019) explain the two main mechanism used to protect users' privacy in LBS: centralized and decentralized scheme. In the centralized scheme, a central server is responsible for all the information encapsulation required by all mobile users. This technique takes the burden of anonymizing users and filtering while communicating with service providers from mobile users. However, in case of a data breach, it risks losing private data of multiple users from just a single point. On the other hand, in decentralized scheme, mobile units take it upon themselves to create the additional information to hide their privacy. Although, it resolves the issue of single leakage point of the centralized scheme, it creates huge storage and processing demand on individual mobile users. On a related topic, Kita et al. (2018) further explains that an entity that works as anonymizer ought to be trusted because they have access to the actual location data of users. Central servers also run the risk of exposing entire set of users' data in the advent of data breach. Decentralizing the anonymizing process is used to overcome the inherent weakness of centralized model. In the latter mechanism, mobile users collect multiple location information by themselves and communicate directly to LBS provider without the need for anonymizer. However, this enables adversaries to easily imitate real users if they have little information about them.

Li, Salinas and Li (2013) highlighted that the core security threat on MLBS is users' privacy. Since the entire data of users would be stored in one location, a compromise to the data store would put the privacy of users at substantial risk. An attacker who has gained access to this data would know who was where at what time. On the other side, even users can cheat on their GPS location and mislead service providers into rewarding them privilege they do not deserve. The most common attacks are as follow: -

- Impersonation attack: - refers to a scenario whereby user steals others' identity to acquire unauthorized token/privilege.
- Multi token request attack: - refers to a case where mobile devices attempt to acquire many tokens to gain more benefits and bonuses.
- Duplicate token redemption attack: - refers to the attempt to redeem the same token more than once.
- Token-Tampering Attack: - defined as an attempt to tamper the contents of a token to stipulate higher value than the originally assigned.
- Colluding Attack: - is a case in which users try to obtain a token through agents who are in a designated location(s) who are willing and cooperating to play their roles.
further

Furthermore, the following are advanced forms of inference attacks as described by (Alrahhal, Alrahhal, Jamous, & Jambi, 2020).

- Homogeneity attack: - deducing the status of a user by the location without getting to know their exact location. For instance, if a user is located in an area where hospitals are located, adversaries can infer that user has a matter relating to health.
- Query Sampling attack: - this type of attack targets users who are found in an unproportionally distributed areas. If a user is isolated and distant from the rest of the cluster, it creates favourable scenario for attackers to distinguish them.
- Semantic Location attack: - occurs when adversaries tries to deduce the status of users by relating to the time they spent in a particular area.

Applications that provide security features for smartphone vary greatly depending on the operating system and manufacturer/developer. Some applications are deployed to protect the general environment of devices while others are meant to protect a specific application or data on the device. Although, it makes it inflexible for users, some security features even lock an entire hardware to protect it against intruders and/or malwares. The fact that Android OS allows applications to utilize system resources based on permission level creates loophole for ill-intended users (Amerasinghe & Walpola, 2015).

Amerasinghe and Walpola (2015) stressed on the idea that mobile devices have become an essential part of our current lives. These smart mobile devices tend to store large amount of sensitive and private data both intentionally by the users and by the applications that are running on them. This phenomenon attracts potential intruders from many angles. One should consider a different protection protocol for such devices considering their unique nature and sensitivity of data stored and processed on them. One such method would be setting the security to different levels based on the location (context) of the device. For example, device can be set in a low risk state with minimum authorization requirement if and when it is found in a trusted zone. If the device gets out of the trusted zone/region, it would be set to high alert and authentication level.

Saravanan and Balasundaram (2018) believe that the following are types of location-based attacks that could result in privacy breaches: -

- Location linking attack occurs when users send one-time LBS request with their exact location. The location information can be used to infer and identify the actual user using many online databases.
- Query sampling attack occurs when the location data is in fact cloaked but adversaries use the LBS query contents to identify which query is sent from which region to finally discover the actual sender.
- Centre point or boundary attack occurs when users are placed at the centre or edge of cloaked region. Since many cloaking algorithms tend to place the actual user at a specific location, it will take adversaries little effort to locate such users even if the location is anonymized or cloaked.
- Location dependent attack is a scenario that could occur while users are transmitting their location data continuously. In which case, attackers can infer users previous and current location relying on the boundaries of the cloaked region. Since, every cloaked region has its boundaries, for users sharing location data and moving in a certain speed, adversaries can deduce where they came from or where they are stationed.

Threats on location-based service areas refer to attacks that take place to obtain raw location data of mobile users from transmitting devices to deduce the actual identity of users. Once the location (or private data) of users are compromised, it can be used spamming unwanted ads, track users, understand users' political or religious affiliations, or even health status. Jin et al. (2018) identify Location Injection Attack as one of the biggest privacy threats in LBS environment with anonymized regions. The attack is basically executed by LBS provider or part of it that already has prior knowledge of the region and the victim as well. The attacker will pretend to be a legal participant of the LBS environment and compromise the privacy of other real users. This kind of attack could occur in three different forms as described below:

- Stalking attack occurs when an attacker obtains series of users' accurate location upon which can track him/her to identify the exact location at a given time in the cloaked region.
- Fixed location attack is a type in which an adversary stays in sensitive fixed location and collects private data of whomsoever visits that place.
- Fixed trajectory attack is another type of location injection attack in which adversaries are only interested in certain users who are taking specific route in the region.

Attempted Solutions for LBS Privacy Concerns

Alrahhal et al., (2020) claim that there are three basic models of protecting privacy of LBS users. As depicted in figure 3, they are: completely server-based approach, completely user-based approach or a collaboration of the two. In the first case, having a central server provides the LBS with high processing and large storage capabilities. However, storing large amount of user data can either create potential attraction point for adversaries or enable them to manipulate the data themselves. On the other hand, a complete user side approach helps to safeguard their own privacy by themselves. They will decide what type of environment to expose their sensitive data and where to hide it. However, the limited battery life, storage media and processing capacities are the main hindrance to these devices and this approach. The last approach tends to merge the two approaches and provide a better service by taking the best of both worlds. In principle, both server and user will take part in protecting the intended personal data. The user protects their own data but with some help from the server. The third approach, named collaborative approach, could also have a third party that is elected from among the users who can act as a leader. The main purpose of leaders is to gather most frequently used queries from users and establish a quick access for other users who want similar requests.

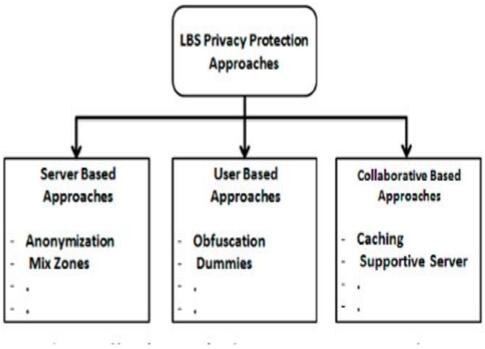

Figure 3: Classification of Location-based privacy protection (Alrahhal et al., 2020)

In Alrahhal's et al., (2020) work involves around the collaborative approach of LBS privacy protection. They tend to resolve the problem if an elected leader acts mischievously and breaks users entrusted private data. To begin with, leaders are introduced into LBS environment to avoid contacting untrusted LBS server by every user for every query. Instead, users will contact the leaders and leaders will fetch the required data from servers. If a certain query is not found in the cache (previously queried tasks), then users will send the new request (with their actual location data) to the leader. In return, the leader will query the LBS server for the required information leaving the untrusted LBS server with no private data of users. The general system of their approach is depicted in figure 4. However, if and when trusted leader becomes an attacker himself, there should be another way to overcome such scenarios. The proposed mechanism is to deliberately send already known queries to users in the same region to cross-examine it with results from leaders. In such cases, if, in fact, a leader is misbehaving, its trust level would decrease and will lose the role of leadership; in which case will be replaced by another.

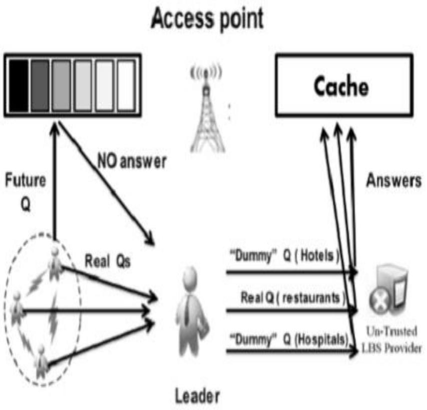

Figure 4: Proposed Model by Alrahhal et al., (2020)

Parmar and Rao (2020b) argue that implementing the following techniques could result in improved privacy and anonymity in LBS:

- Meticulously verifying all generated dummies are genuine-like before sending them over to the LBS will avoid the Map-matching attack.
- In a spatial region (cloaking region), if mobile users can be assigned a different location besides the centre, the Center-of-ASR attack can easily be avoided.
- Furthermore, to ease-off processing load from mobile users, a trusted third-party anonymizer can be utilized instead.

Parmar and Rao (2020a) specify techniques to enhance the anonymization process of centralized approach to LBS privacy in the following three main points:

- Avoiding resource-poor mobile devices and move towards cloudlets
- Avoiding creating dummy location on invalid places
- Avoiding putting real users at the centre of cloak region and opting of edges.

Yang and Yan (2019) explain an improved version of the centralized framework for LBS privacy protection as depicted in the figure 5. The model is composed of three main components: clients (Mobile users), Third Party Servers, and LBS provider. A client initiates a service request which is then transferred to a trusted anonymizing server. The trusted server then creates a set of numerous locations units to disguise the actual user from other parties. To accomplish successful transaction between LBS provider and MU without compromising sensitive information, they have taken three major steps. A) divide the cloaking map equally and create a set of anonymous location units in the given area that are widely dispersed and away from the main user, B) not sending actual data from the user's query to the LBS provider instead sending query of a random location unit from the map that has high similarity of Point-Of-Interest (POI) as the real user and C) if higher security measure is required by certain users, Private Information Retrieval (PIR) technology, which is encryption based, can be used to transact between the LBS server and the TTP (Trusted Third Party) server. The PIR will provide extra layer of protection to the transaction in addition to the anonymized location provided by the TTP.

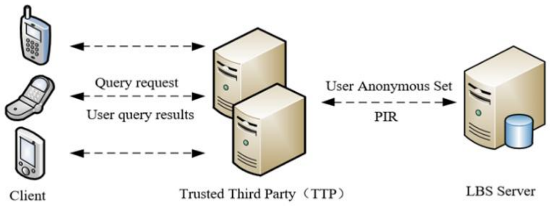

Figure 5: Centralized Hierarchical Communication Model

Novel model designed by Kita et al. (2018) attempts to create stable privacy mechanism that overcomes issues related to fully trusting anonymizers. The model, called Semi-Honest Anonymizer, utilizes location anonymity together with session anonymity. It first divides the given geographical area, that is based on available service providers, equally into N number of locations. Then upon request from service users, the anonymizer sends out the available map locations to users. Users select one of the anonymous locations as their corresponding point (presumed target location) for all future transactions with LBS providers. The anonymizer will send out requests to service providers based on requests from MUs. After collecting the results from LBS providers, the server will send it back to users with a signature from service providers. The entire process does not disclose the exact location of users at any given time.

Unlike other approaches, the semi-honest model considers the anonymizer, the network routers and LBS providers are considered as potential adversaries. Service providers can deduce the exact location of users to gain benefits for themselves, whereas, routers are not adversaries per se rather a potential point for others to eavesdrop and collect data. On the other hand, anonymizers may not always act against users, but they hold all the sensitive data and as such could be infiltrated by other perpetrators or tend to misuse the data themselves. To secure threat form LBS providers, the model makes sure that all the available list of locations in a given area are equally and widely spread throughout the area. This guarantees all the available random locations have the potential to be considered as the target user and cannot be easily distinguished by service providers. This technique of hiding users' location is applied even to the anonymizer to make sure private information is not leaked even from the central server. The anonymizer is not required to get the exact location of users to create the dummy anonymous locations. A Mobile User would just request for a set of randomized locations and the server would respond to the request. In addition to location anonymity, every session of users' transaction should remain anonymous to deter adversaries from inferring users' data based on their previous queries. Session anonymity is achieved by mainly through both the anonymizer and the networking routers. While the server deletes transactions records after short period and uses session-based encryption during communication, the router sends out packets without source and destination addresses (Kita, Kurihara, Koizumi, & Hasegawa, 2018).

Kita et al. (2018) argue that the algorithm they have deployed satisfies the location anonymity to the best possible scenario due to adherence to four principles. The first principle states that all locations units generated by the anonymizer must refer to an actual feasible locations and not unrealistic places like rivers and so on. The second principle is that all generated locations must have similar popularity in terms of being used as a location. If a location unit has a higher or lower popularity among the list of others, it can easily be distinguished and picked by adversaries. The third principle states that all available locations should be disjointed from one another to avoid a potential to backtrack a specific location. The last principle has to do with evenly scattering the dummy location all over the service map to avoid congestion which enables attackers to zoom in a particular area for attack. Following all the above principles guarantees that a user can select any one of the given location units without being vulnerable to possible attacks.

LocaWard is a system developed to award certain points ("tokens" hereafter) to Mobile Users based on their respective locations. Its architecture has five main modules: Mobile Users (MU), Trusted Third Party (TTP), Token Collectors (TC), Token Distributors (TD), and Central Controller (CC). TTP are required to issue unique identity and certificate to every MU participating in the system. MUs are any one of the service users in the system that interact with multiple parties. They collect Tokens from TDs and redeem the respective values with TCs. A TD is any commercial (or otherwise) entity that distributes redeemable tokens to participating MUs. In addition to distribution, TD work with CC to verify tokens upon redemption. TCs entities that are responsible for rewarding MUs upon submission of valid tokens collected from TD. A CC works as a data store for genuine token codes that are used for authentication process. The LocaWard is developed on the premise that all genuine MUs with legit tokens will be rewarded without complications and chances of users redeeming manipulated tokens is almost zero. Apart from that the private data of users is considered to be safe because TDs can only have limited information on MUs which does not include actual identities and token details. Whereas, TC can only have access to values of tokens and nothing more including location information or user details. When MU collects tokens at the TD it communicates with a pseudonym (temporary ID that changes for every transaction) instead of its real ID to cloak itself from sharing unwanted data. The TD authenticates the MU based on algorithm set in the system and delivers the location-based token. The authentication identifies any misbehaving real users who try to take more rewards or fake users who try to take tokens by pretending to be real user, type of LBS attack known as impersonation and/or colluding attack as mentioned in section 2.3. The TC performs similar authentication procedures to verify users while the privacy of users is not exposed (Li et al., 2013).

MUs privacy can be infiltrated not only through online attacks but also physical device theft. In fact, the loss of such devices would result in much greater damage to users than online intrusions. Henceforth, Yazji et al. (2014) proposed a solution to identify if a device is stolen from the lawful owner so as to secure the location data and other private information. The system developed tends to build user profiles based on location data collected from routes taken during routine life activities of users (Yazji, Scheuermann, Dick, Trajcevski, & Jin, 2014). Under normal circumstance, people use regular routes to go about their daily lives so normal user profiles are easier to construct. After the construction of the normal user profile, the main task of the system is to detect possible anomalies on the path to identify potential theft scenario. If a mobile device goes out of its regular path above certain threshold, that is considered as an anomaly and the system will report malicious activity taking place. The authors have used location information and trajectory to build user profiles. As mentioned above, any future activities will be compared to the stored profile to verify if a strange and suspicious path was taken. The system is built on client-server architecture to reduce processing and storage load from mobile devices. In doing so, it can run efficiently and quickly while saving users from the trouble of worrying about having sophisticated smart devices. It will also minimize the response time in case of emergency. Overall, cloud-based server collects user data (location data, network activities, file system access), builds the benchmark for user profiles and finally detects anomalies on future movements. The system also performs some sort of data mining to attain perfect prototype for user profiles that helps identify irregularities and anomalies as accurate as possible. The data is stored following different algorithms to allow compact data storage and less processing time for user devices. The experiments taken by the authors have shown a promising above 94% attack detection.

Liu et al. (2016) believe that the location-aware system they have developed can efficiently identify the most favourable and beneficial locations for mobile users based on the user-generated contents (UGC) collected from users. Hence, the system, called ELAN – Efficient Location-Aware Analytics System, relies mainly on location data collected from users. The data includes geographical locations, textual descriptions of places, reviews and point of interests (POI). ELAN has four main modules namely, Data cleaning and integration, Offline index, Online analytics and user interface. Data integration collects millions of location related data from users and stores it in organized format. Offline index categorizes the collected data in a tree format together with a score value for every location unit. The score of every location data will help search for the most important POI in a given region. The Online analytics uses special algorithm to scan through the stored locations data and find required results based on keywords from users. The User interface provides users with important keywords to choose from user selected map. The general architecture of ELAN is depicted in figure 6 (Yang & Yan, 2019).

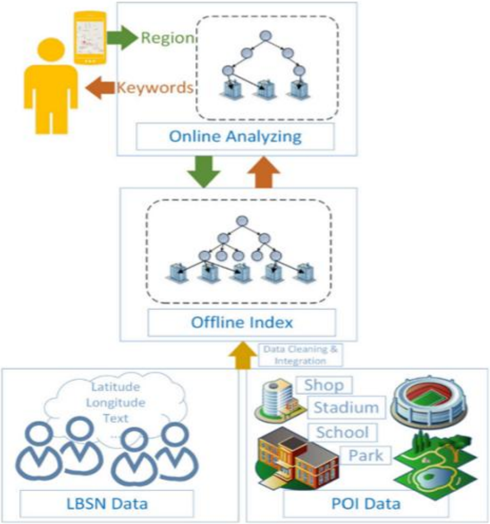

Figure 6: Centralized Hierarchical Communication Model

Amerasinghe and Walpola (2015) proposed a system that detects malicious activities on mobiles devices. Since, Mobile Devices have limited processing capacities, they have opted to create a client-server environment in which heavy processing is handled by the servers rather than Mobile Units. The servers and clients have distinct responsibilities in the model. Clients are responsible for implementing the security policies and auditing security features of running applications/processes. After the security application starts running on the mobile device, it will closely monitor the geographical changes and adapts to suitable security level suitable for the environment. The client application gathers location data from GPS and/or WiFi connections. Once location change is detected it changes the security level based on the policies set for that particular location. If such policy does not exist, a default security level will be assigned. In addition to this, client application will also keep records of all transactions of running processes for future analysis and security improvements. On the other hand, the server side is responsible for tracking the movements of mobile units together with running applications and recording them accordingly. Once the activities of mobile units are recorded, they will be graded based their traces compared with known malware activities/traces. The results are collectively made available as applications ratings for clients' proper decision making. Clients have the choice to either block or allow certain permissions for applications.

Aloui et al. (2020) argue that the following three parts must be protected to safeguard privacy of users while using LBS on mobile business (m-business); the location of MU, identity of the query and content of the query. In the past, online intruders have used these kinds of data to invade users' privacy to understand their political or religious affiliations, home or work addresses, financial situations, health conditions, daily activities or tracking their whereabouts (L. Jin et al., 2018; Zhang et al., 2018). LBS providers collect, process and store large amount personal information from users. Hence, misuse of this information could lead to huge data breach and privacy exposure. The proposed system focusses on trusted-third party (TTP), also called anonymizer that handles transactions between LBS providers and users/clients. The setup is on client-server architecture where clients send queries through the server and the sever contacts LBS providers after cloaking users' location information. They have used novel algorithm called MCC (Mobile Clique Cloak) to handle continuous queries that require sending continuous location data. In addition, they claim that the dummy locations generated by their system is more realistic than other algorithms because it follows mobility client metric i.e., the dummies will have similar velocity and path of real users. In addition to mobility client, the proposed system uses two more metrics known as k-anonymity and cloak granularity. Other models which use k-anonymity metric wait for k-1 clients or expand the cloaking region. Whereas, this model thrives on creating realistic dummies that are hard to distinguish from actual users. If dummies are generated randomly, adversaries can easily identify them. That is why generated dummies should look as real as possible and diversified throughout the region. The proposed MCC works in such a way that it continuously searches an undirected graph until it could find k-1 other users that are close to the requester and with similar movements. The proposed system is shown in figure 7. The cloaking engine hides exact location of clients by mixing it amongst other k-1 users and sends the request to service providers (LPs or LBS providers). Result refiner collects the results produced by LPs and filters it in a manner that would benefit the client based on his/her location. The Cloaked repository stores some of the results from previous cloaking and uses them for future region cloaking. Finally, the profile storage is used to store users' privacy requirements such as preferred locations.

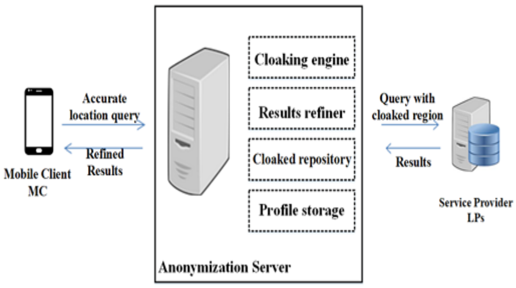

Figure 7: Proposed system by Aloui et al. (2020)

According to Jin and Papadimitratos (2019), during LBS transactions, users' personal information is easily communicated to and from LBS servers. Although, the servers may not be threats to users, they collect extensive data to extract specific interests of users that could help them for targeted marketing or advertising. To tackle such challenges, central server is introduced that anonymizes the identity of users before communicating with LBS providers/servers. However, similar issue may arise with anonymizers. Since they hold all the personal data of LBS users, they will have the potential to misuse or being breached by adversaries. The alternative method to this is known as decentralized approach. In this case, the central server is eliminated users are required to protect their privacy by themselves collaborating with one another. In collaborative method, users have the option of either anonymizing their own location or share a result obtained from LBS provider amongst themselves to minimize the interaction with providers.

Jin and Papadimitratos (2019) have proposed an enhanced decentralized method to overcome the aforementioned privacy threats. The general structure of their proposed system is as depicted in figure 8. The mobile units in the architecture are either smartphones or vehicles with on-board units (OBU). These units interconnect with each other in P2P manner either over wireless ad-hoc or cellular networks. The main source of information is from within mobile units. A mobile unit contacts a third party (LBS service provider) only when satisfactory response is not attained from other peers. All participating units and service providers will have a registered identity in the Public Key Infrastructure (PKI) system that will allow them to communicate securely. In this scenario, LBS providers have the capacity to track users for personal gain. Even certain peers in the system may try to collect persona data from the group to leverage their status to dig into privacy of others. Hence, the authors have set the following requirements to resolve such adversary model/scenario.

- Authentication and Integrity – messages sent over the system should be verified whether or not modified by other than the sender.
- Accountability – a sender unit cannot deny itself being the sender of message(s). All sender should be tied to what they have sent. For misbehaving users, worst case scenario, the permanent identity of users will be revealed and be evicted from the system.
- Anonymity/Pseudonymity and Unlinkability – anonymity of users should remain intact unless need arises to penalize misbehaving users. The permanent identity of users should not be used while transacting with peers or LBS providers.
- Confidentiality and Reduced Exposure – personal data in requests and responses should only be accessible by authorized entities and kept to minimum exposure to peers and service providers.
- Resilience – units/users should be resilient in identifying garbage data sent by peers for sole purpose of disturbance.
- Sybil-resistance – a legitimate unit should be visible and accessible only once (one instance) in the system. It should, under no circumstance, should be present at different place in the system with the same identity.

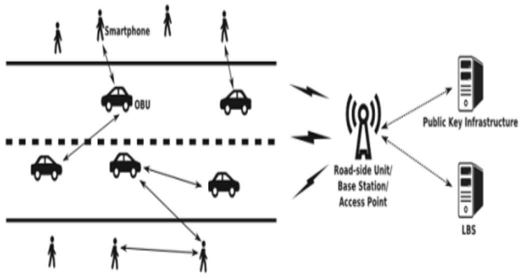

Figure 8: Decentralized System Architecture of Jin and Papadimitratos (2019)

Hashem et al. (2018) declare that conducting efficient LBS transactions is highly dependent on deploying optimized mechanism of locating POIs (Point of Interests) (Hashem, Hasan, Salim, & Mahin, 2018). Unlike other methodologies, their proposed system puts into consideration both distance of POIs and personal ratings when selecting specific POI. In other words, the algorithm tends to locate a resource in the LBS region that is the closest possible with good reviews from other users in a group. Groups are basically made up of users, who have adequate knowledge about POIs in a given area. Every member of a group has the potential to rate POI(s) based on his/her own preference and experience. Only users with up-to-date knowledge of the surrounding are eligible to become members of groups that would eventually have to respond to LBS requests. This will eliminate overcrowding the LBS environment with too many members and helps to verify accuracy of produced results. LBS requestors can add personal rating on the ratings provided by group members to show their personal preferences and show their confidence on certain members over others. Hence, the main goal of the authors' technique is to collect as much information about POIs as possible from group members until the requestor's need is fulfilled. Moreover, users can add multiple variants of POIs to further clarify and accurate identify results that best suits them.

Following the methodology of crowdsourcing LBS requests as Hashem et al. (2018), avoids sharing of private data to service providers to gain similar benefits. Implementing crowdsourcing technique has its own drawbacks such as unreliable members that could either give false information or do not provide rating for the POIs they know. In summary, the proposed system strives to deliver either of the following results without compromising users' privacy: POI that is the nearest to the requestor with satisfactory level of ratings or POI that has the highest ratings with satisfactory/acceptable distance from the requestor. There are three principles that are implemented in the system to guarantee the results mentioned above.

1. Distance and ratings: - the distances between all available POIs and requestor will be measured in linear fashion and stored in a list for processing/selection. When it comes to ratings, all group members will provide certain ratings of POIs according to their knowledge. In addition to that, users will also rate the POIs based on the sources they trust the most.
2. POI variants: - users can refine the search by putting variants of POI such certain brands or specific names they prefer. Adding variants will also ensure that all possible results included in the result set that may not be preferred by other group member. For instance, when searching for restaurants, group members might only include results they prefer not necessary those that fulfil the criteria. So, by adding specification and details to the search, all possible outcomes will be included even if they are favoured by others.
3. Confidence: - this feature addresses the possible inaccuracy of results collected through crowdsourcing. To start with, only users with knowledge of many POIs will be nominated to become group members. This will weed out users that would supply false information into the group. Secondly, if a requestor gets results that are shared by only one (or very few) group member, this will automatically be given a low score of confidence compared to those results shared by many members.

According to Hashem et al. (2018), there are two ways to select members of groups. The first one is to search of users who share many POIs in a given region which is called knowledge-based selection. The other one generic-based and it creates groups with random users. With multiple interaction with users, those members who are closer to requestors' needs are given higher weight and be selected for the final group formation.

Another approach proposed to protect privacy of LBS users is graph-based model cloaking algorithm. In this model, each unit of information collected from location-based queries from several mobile users is characterized by a node (vertex) on the graph. Users in the same region who are in the proximity are connected by edges. The algorithm then makes sure that there are k-1 number of users in the cloaked region (CR) to satisfy the k-anonymity ruling so as all requests can be communicated in anonymized manner. The CR also should be of reasonable size (adequate number of users in manageable area). At the beginning of the process, all user groups are considered in the system. However, throughout proceeding iterations, users that require cloaking/anonymizing are selected and put into subgroups to create the final Cloaked Region (CR) without compromising the Quality-of-Service. The algorithm relies on graph and grid-based approach to handling queries to and from LBS providers. In doing so, it believes to have maximized the uncertainty level of users' exact locations by both intruders and service providers (Saravanan & Balasundaram, 2018).

Cloaking an area is mainly done by anonymizing server, AS, that collects actual data from mobile users and merges it with others to hide the true identity of users. The main issue with this approach is that all mobile users, MU, and AS are trustworthy. However, this may not always be the case. An attacker can act as a legit user and AS would not have the means to distinguish it from other users. In such cases, attackers would gain access to the LBS environment acting as real users to infiltrate MUs' privacy; enabling them to execute what is commonly termed as injection attack. Furthermore, some approaches deploy fake-user detection techniques, but it comes with its own drawbacks. Detection mechanism often generate false positives and false negatives. There is also no unified description of "fake user" so even legal users can be denied access or fake users can be granted one. An approach to resolve this issue is to use trust-based k-anonymity to differentiate fake users from real ones as opposed to the regular k-anonymity that only anonymizes users' data and not differentiate. Trust-based anonymity (k-trustee) does not validate users nor does it detect fake users, rather it mitigates the occurrence of an attack by adding cost (computational and time) on the transaction of LBS services. Trust has to be built among users and locations in the region for successful LBS transaction. Once a user misbehaves s/he loses their trust level and no longer eligible to perform any interaction with other users. They will have to create a new id and have to work harder starting from the bottom just to be thrown out again upon misconduct. This will cost attackers lots of resources. A MU is said to trust another MU if the former is not following the latter (be in proximity) for specified number of times in the cloaked region. If the two are found to be in short gap of one another for specified time, that user is considered as a talker who is capable of executing stalking attack (type of injection attack). Trusts are built locally (local trust) with neighbouring users or (global trust) with other users in the entire cloaked region, CR. Injection attack could be performed by either following users around (stalker) or staying in a particular sensitive place (stationary) as a bait. "Stalker" can create a fake user or use other real mobile users to stalk and collect information. "Stationary" are those who are employed by attackers to wait in one place and record data of all visitors. *Stalker* can be identified by counting the number of times that a user has appeared together with another user in CR in certain period of time. *Stationary* can be identified by counting the number of users visiting a particular area in which a stationed user is located. **Local trust** refers to those users who do not fall under the category of either "stalker" or "stationary". However, since an adversary who is not trusted with certain mobile users can move to another location and build trust with other users, the idea of global trust comes to play. **Global Trust** refers the status of users throughout the CR; if a user is known not to be trusted globally, they will lose the credibility to ever be used again elsewhere in the CR. In conclusion, user-1 is said to be trusted by user-2 if and only if user-2 is locally and globally trusted. Also, a CR is said to be trustworthy for user-1 if and only if there are at least k number of trustees (k-trustee) in that region for user-1. As such, even if a user may start as a trustee, once issues arise, that user will be demoted. Hence, an attacker will have to keep generating fake users (or employ real users) over and over again to do its business which will be too costly (non-beneficial). On the other hand, an authentic user, even if not trusted by others, can still request for services on the LBS and will not be denied due to false negative. This phenomenon is because LBS providers are not linked with computing the trust level of users. Using the K-trustee approach as opposed to K-anonymity has proven to mitigate location injection attacks (L. Jin et al., 2018).

When users interact with LBS providers, their personal data will be stored in the receiving end of such transactions. A system has been developed that claims it resolves the mentioned issue (Jency, 2017). The process introduces an anonymizer that handles the traffic between users and service providers. The system basically has modules: a) Pre-processing module collects users profile together with their preferred region, b) Query processing module analyses requests from users and displays them according to the location they have selected, c) Anonymizer module is the part where the server collects results from service providers and responds to users based on their queries and location, finally, d) Location processing module stores numerous location information in a given area together with the objects found in them for easier retrieval and display.

Zhang et al. (2018) state that there are many mechanisms that have been deployed to protect privacy of LBS users and mitigate imminent attacks. Privacy protection can be done either using central trusted party to do regional cloaking or by mobile users themselves. In both cases, it would not fully guarantee privacy protection due to the lack taking the contextual data of LBS environment into consideration. Contextual data could be density of Point-of-interests, map information and users' privacy requirement. In response to the above concerns, the authors have proposed context-aware scheme system that does not use third party servers. The system also implements an efficient data compression algorithm considering the limited resources available within mobile devices. Furthermore, the LBS area will be mapped based on the density of available POIs helping users not to be uniquely identified for requesting certain places. The POI distribution is done in such a way that many POIs will not be congested in small geographical location. If a cell has more POIs than the threshold, it will be further divided into multiple cells. The proposed system has two main components as depicted in figure 9; LBS user and LBS provider. Users are connected to the system using cellular connection, WiFi or similar technologies that are capable of LBS transactions. They perturb or shuffle their own location in predefined algorithm before communicating the LBS providers. Service providers are considered adversaries and as such will try to deduce exact location of users through the approximate location that they already possess through LBS transactions. The proposed system guarantees users would not have collision attack because of the fact that every user will use his/her own given position on the map without interacting with other users and all processes are executed on individual devices without any help from third party while querying the LBS providers. The authors also claim that this approach is inference attack resilient due to the fact that LBS providers are considered as possible adversaries and would not receive actual location of users. Instead, users only interact with them the perturbed location information, which is difficult for deducing exact locations of users.

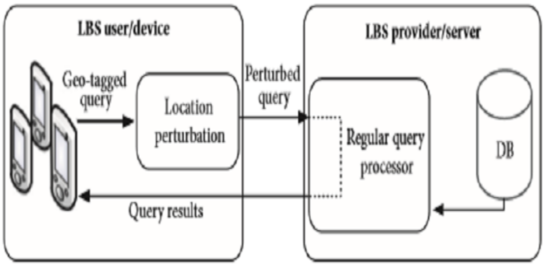

Figure 9: Decentralized System Architecture

Limitations of previous works

Kita et al. (2018) emphasis on the part where many previous works on location anonymizing failed to realize adversaries are not limited to attacks to/from LBS providers, rather they can infiltrate network infrastructure such as routers as well. Similarly, Li, Salinas and Li (2013) stated that attacks such as mobile work attack, channel jamming, sabotaging security protocols among system users and denial-of-service (DoS) are beyond their research. They have also added that they assume the system runs under semi-honest mode in which they trust all involved entities in the system will not work against the protocol of the business. However, in location-based awards, there are numerous possibilities to cheat the system unless protected otherwise.

For instance, mobile users may try to collect a reward pretending to be someone else or try to redeem a reward that has already been redeemed earlier. In a similar scenario, adversaries can pretend to be legit MUs to collect or redeem rewards. In some cases, MUs and reward collectors may conspire against reward distributors for a shared benefit.

On the methodology followed by Zhang et al. (2018) to include contextual data of the LBS, it is stated that the only user information the authors considered to be compromised by adversaries is the approximate location of mobile users. All other peripheral information that can be known about users is yet to be researched on.

Yazji et al. (2014) argued that due to the advancements in mobile technology, the number of mobile device users has increased dramatically. Likewise, the devices are enabled to store huge amount of data both that are personal and sensitive and those that are not. Hence, securing such devices comes to grip everyone’s attention. Earlier works on security focused mainly on physical and access control mechanisms. Since such techniques do not overcome the issues of protecting private data from stolen devices, certain applications use the GPS feature of the device to track and locate devices in case of loss. Unfortunately, even this technique does not meet the required need for security. A method that involves the routine path or location of mobile device users would come as a better approach to overcome the above-mentioned shortcomings. Although the attack-detection system developed by the authors have shown great results, they have recommended to add features like identifying especial cases of users visiting new places without considering it as theft case. The system can also be upgraded to include scenarios in which the mobile device is disconnected from the cloud server for long period of time.

Amerasinghe and Walpola (2015) point out certain areas in which the security for LBS can be improved that are not discussed in their own research or by others. One such recommendation is to include technologies to identify location of users other than the usual GPS coordinates. Such inclusion could help expand the use of LBS even inside buildings and other indoor establishments. In addition to the indoor coordinate system, integrating LBS in cloud-based application is crucial aspect as current trends tend to move towards such technologies. The main improvement recommended by the authors is to include malware behaviours that focus on low level system calls. If attackers imitate legitimate users in a network and access users’ mobile devices to access low level system calls such as making call, sending SMS and browsing user data, they will gain stronger access to the private data such as location information. Hence, it is incumbent to build on the current system and develop further improvements for enhanced security of Mobile Users. In general, they argue that all security related development that are implemented for mobile devices ought to put context/location of the devices into consideration for satisfying results.

Analysis and Findings

It is undeniable that internet applications are on a rise. Many of the transactions are being processed on the internet. As vast as the global network is, it becomes crucial to limit the type and depth of information users receive based on their geographical location. Many scholars, researchers and authors alike have described the benefits of Location-Based Services in great detail. Nevertheless, users are willingly required to expose their location information to access those services provided. This characteristic puts user in a challenging spot between getting services and surrendering sensitive information that, could be misused by third party of service providers themselves. Hence, finding the maximum allowable threshold for exposing privacy has been centre of many studies. Unless dealt carefully, these types of data can be misused by many to leverage it to their own economic gain, to study people, different types of harassment or even threaten the lives of many users.

Many of the proposed mechanism tend to revolve around two basic architecture of encapsulating users' location information: centralized and decentralized. Centralized privacy prevention mechanism utilizes central server (mainly called anonymizer) that attempts to disguise LBS users' exact location by either merging it with other users around or with generated fake location data (pseudo-location or dummies). On the contrary, the decentralized privacy prevention mechanism tends to eliminate the usage of central servers. Instead, it leaves it to the users themselves to cloak their real identity while communicating with LBS providers. This can be achieved by letting mobile users create their own dummy locations with their own algorithms, a task that was done by the anonymizing server. Another approach to this would be collect as many LBS queries as possible in a cache (within users themselves) and distributing the queries amongst each other whenever needed, limiting the need to interact with LBS server that could result in data leak.

Both centralized and decentralized approaches have their own benefits and drawbacks. Using anonymizer saves users from overloading their mobile devices with computation and storage costs. All Mobile Units need to do is send their location to the anonymizing server and receive the list of anonymized locations. They will not be required to run any sort of algorithms. However, since all the sensitive data is stored in such portals, a data breach would mean compromising the privacy of the entire user collection in a given anonymized region. Additionally, unless equipped with additional security measures, anonymizers cannot distinguish real users from forgers. Since their task is only to accept anonymization request from anyone in a given region, they can be used by intruders to gain access into the LBS environment.

On the other hand, decentralized model, removes the need for an anonymizer, which solves the dependency on third-party servers. Nonetheless, it opens a can of worms of its own. It allows users to set their own privacy level based on their location and their type of service request. However, for devices that have limited processing capacity and storage media, it creates a load that might be hard to bear. Moreover, not only will they need to generate their own dummies, they need to verify the validity of each to guarantee the efficiency of location cloaking. Otherwise, an adversary can easily distinguish the real location data from the dummies that are generated under poor algorithm. In case the decentralized LBS architecture implements a cache approach, whoever holds such data can also turn against users and misuse the data within. Thus, users in decentralized mode are required to protect themselves not only from outside attack but from enemy within as well.

Certain researchers have proposed to include encryption/decryption while contacting both service providers and other involved entities. Encryption can be used for extremely important transactions where safety is required more than other computational expenses. However, for routine transactions that take place almost every minute or second, the added computational and storage overhead makes it unfeasible for every small transaction.

Perhaps one of the biggest discussions in LBS is concerning one time LBS request versus continuous requests. The two, although seem similar, they have quite huge differences upon implementation. Security feature that works for sending location information just once does not apply for those who are sending their data continuously. Storing and processing of such requests are also quite different in both scenarios that requires careful attention when developing an algorithm that can be implemented for both.

Although, every proposed model, architecture and/or algorithms tend to solve a part of the LBS concerns, none have been able to address all the loopholes in LBS. This truly could be one of the best examples to use the phrase: “There are no right and wrong answers” when it comes to selecting a technique to protect users’ privacy. Henceforth, just as the expansion of LBS usage is dramatic, so is the everlasting search for the most efficient privacy preserving mechanism.

3 Discussions and Conclusion

In the era of continuous online transactions, the safety and security of users becomes vital part of the daily routine. Especially in LBS, where users have to surrender their sensitive data willingly to gain access to services, the concern over unauthorized access and misbehaving service providers has gained popularity. This popularity spans across both LBS constituents and researchers alike. Thus, one can easily notice that many of nowadays researchers tend to be involved in some kind of location-based (context aware) oriented studies.

Many researches have attempted numerous methods to overcome the issues pertaining LBS and guarantee users that their privacy would be intact during the course of LBS transactions. Obviously, there are overwhelming number of techniques, models and frameworks that are proposed and tend to enhance the LBS experience to some extent. They all address one or more issues from previous studies and they too will fall short of one or more other issues. Although, the cycle might seem endless, the general LBS environment is improving and enhancing the security features.

Generally speaking, location-aware regions require to consider a couple of things to ensure smooth and secured transactions amongst all connected entities. The first of this element has something to do with the security of the trusted anonymizer itself. If this crucial part of the framework is not under strict and vigorous security measures, it can turn into one-stop access point for adversaries to collect all the sensitive data of users. The other part concerning the anonymizer is the fact that it is the only element that handles all the requests of every mobile user in the LBS region. In such cases, depending on the number of users, the frequency of user requests and capability of the server itself, we may end up with a bottleneck scenario in which it cannot handle all the required processed in due time. If such circumstances cannot be resolved, the number of dropped user requests will pile up deteriorating the overall experience of the environment.

The other concern about LBS area is related to the limited resources of mobile users. In a scenario where users are required to anonymize their own location data and/or store several POIs, the limited battery, storage and processing capacities of these devices will be put to the ultimate test. In many cases, the QoS worsens greatly. Not to mention, the lack of awareness about the authenticity of other users and unavailability of universal governing procedures, makes mobile units an easy target to several misbehaving actors.

REFERENCES

1. Aloui, A., Kazar, O., Bourekkache, S., & Omary, F. (2020). An Efficient Approach for Privacy-Preserving of the Client's Location and Query in M-Business Supplying LBS Services. International Journal of Wireless Information Networks, 1-22.
2. Alrahhal, H., Alrahhal, M. S., Jamous, R., & Jambi, K. (2020). A Symbiotic Relationship Based Leader Approach for Privacy Protection in Location Based Services. ISPRS International Journal of Geo-Information, 9(6), 408.
3. Amerasinghe, D. N., & Walpola, M. J. (2015). Location aware security for smart mobile devices. Paper presented at the 2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer).
4. Chow, C.-Y., Mokbel, M. F., & Aref, W. G. (2009). Casper* Query processing for location services without compromising privacy. ACM Transactions on Database Systems (TODS), 34(4), 1-48.
5. Gkoulalas-Divanis, A., Verykios, V. S., & Eleftheriou, D. (2009). PLOT: Privacy in location based services: An open-ended toolbox. Paper presented at the 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware.
6. Hashem, T., Hasan, R., Salim, F., & Mahin, M. T. (2018). Crowd-enabled processing of trustworthy, privacy-enhanced and personalised location based services with quality guarantee. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(4), 1-25.
7. Jency, I. (2017). Location Based Query Processing By Anonymizer. i-Manager's Journal on Computer Science, 5(4), 7.
8. Jin, H., & Papadimitratos, P. (2019). Resilient privacy protection for location-based services through decentralization. ACM Transactions on Privacy and Security (TOPS), 22(4), 1-36.
9. Jin, L., Li, C., Palanisamy, B., & Joshi, J. (2018). k-Trustee: Location injection attack-resilient anonymization for location privacy. Computers & Security, 78, 212-230.
10. Kita, K., Kurihara, Y., Koizumi, Y., & Hasegawa, T. (2018). Location privacy protection with a semi-honest anonymizer in information centric networking. Paper presented at the Proceedings of the 5th ACM Conference on Information-Centric Networking.
11. Li, M., Salinas, S., & Li, P. (2013). Locaward: A security and privacy aware location-based rewarding system. IEEE Transactions on parallel and distributed systems, 25(2), 343-352.
12. Liu, Y., Wang, H., Li, G., Gao, J., Hu, H., & Li, W.-S. (2016). ELAN: An efficient location-aware analytics system. Big Data Research, 5, 16-21.
13. Mamoun Hadidi, Maen Al-Rashdan, Saleh Hadidi, Yaseein Soubhi (2020) Comparison Between Cloud Erp And Traditional ErP. Journal of Critical Reviews, 7 (3), 140-142. doi:10.31838/jcr.07.03.26
14. M. Tubishat, M. Alswaitti, S. Mirjalili, M. A. Al-Garadi, M. T. Alrashdan and T. A. Rana, "Dynamic Butterfly Optimization Algorithm for Feature Selection," in IEEE Access, vol. 8, pp. 194303-194314, 2020, doi: 10.1109/ACCESS.2020.3033757
15. Mokbel, M. F., & Chow, C.-Y. (2006). Challenges in preserving location privacy in peer-to-peer environments. Paper presented at the 2006 Seventh International Conference on Web-Age Information Management Workshops.
16. Parmar, D., & Rao, U. P. (2020a). Dummy Generation-Based Privacy Preservation for Location-Based Services. Paper presented at the Proceedings of the 21st International Conference on Distributed Computing and Networking.

17. Parmar, D., & Rao, U. P. (2020b). Towards Privacy-Preserving Dummy Generation in Location-Based Services. Procedia Computer Science, 171, 1323-1326.
18. Saravanan, P. S., & Balasundaram, S. (2018). Protecting privacy in location-based services through location anonymization using cloaking algorithms based on connected components. Wireless Personal Communications, 102(1), 449-471.
19. Saleh Hadidi, Maen Al-Rashdan, Mamoun Hadidi, 2020. Impact Web On Decision Support Systems On The Organizations. Journal of Critical Reviews, 7(3):2020
20. Yang, C., & Yan, W. (2019). Location Privacy Protection Scheme Based on Location Services. Paper presented at the Proceedings of the 2019 the 9th International Conference on Communication and Network Security.
21. Yazji, S., Scheuermann, P., Dick, R. P., Trajcevski, G., & Jin, R. (2014). Efficient location aware intrusion detection to protect mobile devices. Personal and Ubiquitous Computing, 18(1), 143-162.
22. Zhang, X., Huang, H., Huang, S., Chen, Q., Ju, T., & Du, X. (2018). A context-aware location differential perturbation scheme for privacy-aware users in mobile environment. Wireless Communications and Mobile Computing, 2018.