Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Hiding Location Privacy in Location Based Services

Amit Kumar Tyagi[1], Dr. N. Sreenath[2]
Research Scholar[1], Professor[2]
Department of Computer Science and Engineering,
Pondicherry Engineering College, Puducherry-605014, India.
amitkrtyagi025@gmail.com, nsrenath@pec.edu

ABSTRACT- With the rapid development of wireless technologies, Privacy of personal location information of Vehicle Ad hoc Network (VANET) users is becoming an increasingly important issue. Privacy is a human right and should be respected whenever users interact with electronic systems. LBSs are not exceptions. Vehicle Users wish to maintain their information is known only to those legally authorized to have access to them and remain unknown to anybody unauthorized. As existing various methods like: mix zone, silent period, pseudonyms etc., used to enhance user's privacy in location-based services (LBSs). Location-Based Services (LBSs) provide mobile users with valuable (can be confidential) information about their surroundings such as traffic status (e.g., Beat the Traffic, or INRIX Traffic Maps, Routes & Alerts), nearby points of interest (e.g., Google Maps), or friends' activities (e.g., Foursquare or Google Latitude) etc. But no one efficient against such types of attacks for example: timing, transition, continuous queries, and range queries attacks etc. The main goal of this work is to propose a new solution to provide trustworthiness services among vehicles users. Finally, this work conation an architecture to protect privacy which exploits into twofold i.e. Trusted Computing Environment (TCE) and Private Information Retrieval (PIR). In summary, this work proposed a novel approach in spite of mix-zone approach i.e. to maximize the location privacy, minimize computational complexity and also takes into account the cost induced by mix zones to mobile nodes.

Index Terms- *Location Privacy, Location Based Services, Security, Certificate Authority, Trusted Computing.*

1. INTRODUCTION

The fast advances of mobile devices and positioning technologies has led to the flourish of Location-Based Services (LBSs). Vehicle plays an important part of everyday life for billions of people around the world. Today's people want to enjoy wireless services everywhere like in hotels, colleges, etc. LBSs that allow vehicle users to release their location to third parties can be implemented in a similar way. The only change for the service provider is that the generated map should be encrypted with the public key of the third party, which can be contained in the signed query. To provide a secure and private communication between vehicle (mobile) users during accessing services inside LBSs is becoming an important issue. *Authentication is a crucial security service for both inter-vehicle and vehicle roadside communications.* The ubiquity of mobile phones has led to the introduction of LBSs. A location-aware service provides services that distribute on demand information for a certain geographic area of interest by taking advantage of vehicular communications. During this communication with trusted authorities, LBSs could track a mobile user and raise an alarm when the user leaves a boundary area. On other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non-repudiation. The concept of privacy is subject to change over time; it is contextual and cultural. Privacy has 3 dimensions: (a) *personal privacy* of an entity—demanding protecting an entity against undue interference (such as physical searches) and information that violates moral sense of the entity; (b) *territorial privacy*—calling for protection of the area surrounding the entity (such as laws on trespassing); and (c) *informational privacy [2]*—requiring protection of gathering, compilation and dissemination of information. Among all LBS service categories, location privacy becomes extremely critical issue when the user's location information reveals his personal attributes, for example: special diseases, hobby, or home address etc. Moreover, security is not privacy and privacy also not security. Security and Privacy are two different, dependent terms. It is important to understand the difference between privacy and security. Security can both be an ally and an enemy to privacy. Privacy is generally approached as a social consideration, whereas security is seen as a technical concern. Vehicle users using a service (like coarse-grained, fine grained location information, etc.) must trust the service provider i.e. not to misuse or leak their location information.

Most location service providers (LSP) probably have good intention with their services. Nonetheless, software bugs or computer break-ins can inadvertently leak location information. In particular, we examine the question "Whether it is possible for a service provider to offer location based

services *without* learning the location of mobile users or not". As main contribution of this proposed architecture for LBSs users is "where mobile users can keep their location hidden from a service provider while benefiting from location-based services". In simple form, LBSs deliver information to a vehicle user based on his/her current physical location [4]. Location privacy is an important issue in vehicular networks since knowledge of a vehicle's location can result in leakage of sensitive information [4, 7, and 21]. Location-Based Services can be defined in different categories as:

- Position-aware and Location-Tracking Services:
- Reactive and Proactive Location-Based Services
- Location-of-target and Target-at-location
- Self and Cross Referencing LBSs
- Single and Multi-target
- Content and Application-orientation:
- Outdoor and Indoor

Privacy in LBSs: Privacy is a multifaceted, relativistic, and context-dependent concept. It has been defined by Westlin as the "claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [3]. When making use of LBSs, users expose their locations and queries. Both of them can be explored by attackers to infer users' private information. Such malicious inference in turn threatens users' privacy in LBSs. First, locations can serve as a piece of subsidiary information to peek users' personal life. For instance, hospitals are public places and the location of a hospital itself does not carry any sensitive information about users. However, it will become sensitive when the functionality of hospitals and the purpose of people in hospitals are taken into account. An appearance in a cancer centre reveals that a person may suffer from a bad health problem. In order to avoid the abuse of inferred personal information, users desire the protection of location privacy in LBSs. Second, even if where users are located does not reveal any sensitive information, their queries may still put their privacy at risk. By query, we mean the specification of the information or functionality a user wants to acquire from LBS for example, a query for nearby casinos will reveal a user as a fan of gambling which is usually not accepted as a healthy hobby. The potential leakage of privacy by queries leads to users' requirement for query privacy.

In this work, proposed architecture discussed two main concepts from cryptography and security research point of views is: *Private Information Retrieval (PIR) and Trusted Computing Environment (TCE). In Private Information Retrieval,* it avoids that a service provider learns a vehicle user's location by observing which of its location-specific information is being accessed [1, 5, and 6]. In PIR, a mobile user can retrieve location-specific information from a service provider without the provider being able to learn the location the requested information. Trusted Computing Environment is used to build a platform that is trusted by a mobile user to properly implement both PIR algorithm and some additional algorithms required by location-based services [5]. *In Trusted Computing Environment module*, it ensures that a location-based service operates as expected by vehicle users and that information about the vehicle user's location becomes inaccessible to a location-based service upon a compromise of the service. Furthermore, with the help of TCE, ensure that the platform can access a user's location only when the platform is not compromised. Trust computing (or trusted third party) means who providing services in a trusted environment. To explain about trusted computing, i.e. needed requirement are discussed in section 4 i.e. any changes to the software by an intruder will make a user's location inaccessible to the platform and hence to the malicious users. To providing strength to vehicle users, mechanisms resisting the attacks on both authentication and privacy are required. For authentication purposes, this work uses asymmetric key concept. Using asymmetric key based authentication because it is widely adopted because of the separate keys used for encryption and decryption [7]. This work can serve as operators (mobile networks and service providers) of LBSs as a map-guide to design a trusted and secured communication between two authentic parties. We hope that the proposal will help create a secure, trustworthy, and privacy preserved environment for vehicle users to access location services. In extension of this work, we will show, our approach is powerful enough to support several existing LBSs without revealing identity of the vehicle users. This paper provides a novel approach that provides trustworthiness of a desired level of the agents of other vehicles' users, in order to receive the most effective information.

Finally, the contribution of this paper is organized as follows: Section 2 discusses about motivation behind writing this paper. Section 3 presents our system and threat models. Section 4 introduces about proposed architecture to maintain location privacy for LBSs users. Next in section 5, it explains about "How to provide some location-based services in proposed architecture". Finally, section 6 concludes this work in brief. In the following sections, this work does not differentiate terms "vehicle," "object," "users "and "moving object".

2. MOTIVATION

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Privacy Enhancing Technologies (PETs) is a system of ICT (Information and Communication Technology) that measures protecting informational privacy by eliminating (or minimizing) personal data, i.e. preventing unwanted processing of personal data, without the loss of the functionality of the information system [6]. Location privacy is a system-level capability of location systems, which controls the access to location information at different spatial granularity and different temporal and continuity scale, rather than stopping all access to location information. Ultimately, privacy is about feeling, and it is awkward for one to scale her feeling using a number [6, 13]. Access control is (a tool to limit the number of people) used by service provider to access the location information in location based services (LBSs). In [10, 11, and 12], a personal agent (or device) controls access to VANETs user's location. But to provide privacy to mobile users (or control to access user's location) in LBSs, we must prioritize trusted technologies inside LBSs. The drawback of a distributed architecture [10, 11, and 12] is that cyclic dependencies can make difficult to implement some location-based services. *So we moved for centralized concept.* A centralized architecture does not suffer from this kind of drawback arises in decentralized systems. Further Myles et al. and [8] suggest the usage of pseudonyms. But in [8], some LBSs require user's true identity, such as a service to locate nearby friend's location. In [7], author discussed a centralized architecture that exploits multiple sources of location information. Our proposed architecture in [7] supports services that require to protect user's true identity, also guaranteed perfect response quality without revealing any location information to service provider. *As advantage of this proposed approach, it avoids that service provider who knows the vehicle user's location.* In past several work has been explored on privacy issues to recover them, but no one has this property.

Gruteser and Grunwald [14] introduce "location *k*-anonymity", where a vehicle user's location is cloaked spatially or temporally such that at least *k* vehicle users are visited same location (or within the same timeframe). In [14], a user reports an obfuscation area to a client containing his position and the positions of *k*–1 other users instead of his precise position that is protected by a pseudonym. Gedik and Liu [15] and Duckham and Kulik [16] also exploit cloaking concept. The drawback of cloaking is that*"it might decrease the quality of a response received from a location-based service"*. Further in [17], to assure certain level of privacy, the degree of cloaking needs to be reduced. Mokbel et al. [18] also discusses spatial cloaking to return a superset of the information of interest to vehicle users. A spatio-temporal cloaking algorithm allows the vehicle user's location to be indistinguishable from k people. Spatio-temporal cloaking approach create problem for mobile users due to lack of bandwidth and processing constraints. In [19], a service provider migrate the code to implement service to a network operator. The operator uses information flow control to ensure that the code does not leak a vehicle user's location to the service provider. This approach is targeted at services that exploit aggregate location information and does not support services that require precise location, such as a tracking service. In last, this paper defines three sets of metrics that will be used to evaluate the proposed approach. The first set of metrics is used to evaluate the level of privacy protection, and includes relative k-anonymity (krel), relative s-anonymity (srel), and segment entropy (H(S)). The second set of metrics is used for evaluating the level of utility preserved in the cloaked subgraph produced by a cloaking algorithm. Finally the third metrics, anonymization success rate (R) and anonymization time t, is used for evaluating the cloaking algorithm performance. The concept behind using *k-anonymity* is, it provides the guarantee that in a set of *k* objects (in our case, VANET users) the target object is indistinguishable from the other *k* –1 objects. So as discussed above, one question arises here "Can you guarantee secrecy of a user even if an adversary can eavesdrop on your location privacy" if yes then How?

3. SYSTEM AND THREAT MODEL

As discussed, three important metrics used to measure the level of location privacy (in guarantee) one could provide: (i) location *k*-anonymity, (ii) location *l*-diversity, and (iii) road segment *s*-diversity [6, 7]. Each of these metrics represents an orthogonal perspective of the location privacy of mobiles in LBSs. As discussed above, one question arise "how can a data holder release a version of its private data with scientific guarantees". In relate to this, it introduces architecture with various existing location-based services as:

3.1 System Model: In our proposed model, assume that network operators and service providers are separate (business) entities. A network operator implements an application programming interface (API) that is used by a service provider to offer location based services for example: several network operators in USA, such as Vodafone or Orange. Like as Sprint and Bell Canada use Wave-Market's Family Finder technology [20] to allow parents to track their children's location in emergency. Three types of privacy arise for example: data privacy, location privacy and identity privacy. This paper focus

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

only on protects user's identity with location when they are using LBSs. In our proposed model, a network operator always knows its vehicle user's identity and location (unless a vehicle user's mobile is turned off). In several location-based services mechanism, a service provider also becomes aware of the vehicle user's location with identity.

3.2 Threat Model: As main threat, service provider (assuming that it is an intruder) becoming aware of a vehicle user's location in LBSs. A service provider, *who* provides location-based services to subscribed mobile devices. These services can be broadly classified into two groups: *event-driven requests* and *per-use requests*. It allowed to learn the identity of the vehicle users (at the time of using services) but vehicle user's location should not be reveal to provider. But a malicious service provider could exploit location information of a user for purposes not sanctioned by any mobile user for example; the information could leak to criminals planning on robbing the vehicle user or to stalkers. Due to this leakage, leakage of location information from non-malicious providers is still possible. Threat model can be discussed in two views from attacker views like firstly Weak Adversary Attack Model i.e. weak adversary has little knowledge about the participators. It is only aware of the set of participators moving in and out of the mix-zones but not of their time intervals and trajectories. In this case, the type of probability distribution function suggests the same uniform probability for the entire trajectory mapping indexes. And secondly, Strong Adversary Attack Model i.e. strong adversary can launch the time attack such as first in first out (FIFO) by gathering entering time and exiting time intervals. Hence, besides the number of participators, the effectiveness of the mix-zones also relies on the time intervals. As discussed, in a time interval participators arrive at the mix-zones, where is determined by the mean arrival rate. Additionally, we argue that the data collection time of each participator spends in the mix-zones follows normal distribution. In this case, the strong adversary can record the arrival time and leave time intervals. When adversary observes a participator exiting, he tries to map the exit participator to the related pseudonym identity.

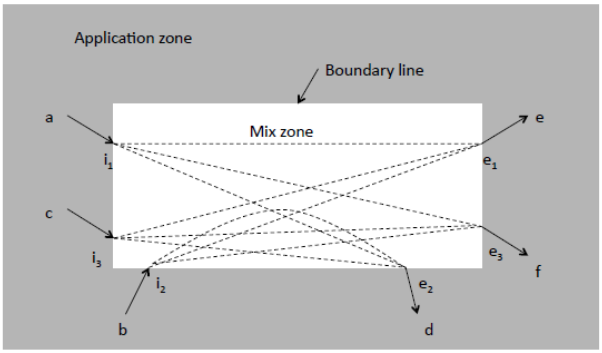

Fig.1. Example of Mix Zone

In figure 1, let '*a'* refers to any entity formed by one or more malicious parties (by colluding) whose aim at learning the locations associated with mobile users' true identities. Several attacks can hit in a mix-zone (at the time of providing location services of VANETs users) like transition, timing, inference and continuous query attacks etc. every information like health report, daily report of any user is to important and risky to reveal his/her identity to unauthorized users. Accidental leakage of a user's real identity may become *side information* to an adversary. In past, various techniques has been proposed [6, 7, 21] including one as mix zone to recover from these measured attacks in LBSs. Thus paper divide mix-zone techniques into two groups like system-centric mix zones and user-centric mix zones. *A system-centric mix zone* is an area predefined by the system. Users have to go through the area to "mix" their pseudonyms. *On the contrary, in user-centric mix zones*, users do not need to go to a predefined area. As enhancements of mix zones approach are Mobi-mix, Silent Mix Zone, Mini Mix zones and Pro Mix Zone [6, 21] etc. An intruder running into LBS can passively monitor the service (vehicle user's location) or the attacker can actively query a network operator for location information of any user. This threat model (Refer: figure 1) classified three types of privacy attacks as: *attack on vehicle's identity, attack on vehicle's location and attack on location based service*.

Suppose vehicle users are accessing several services in mix zones in LBSs. In that, a lot of data/information is collected by service provider, but users have a fear about to disclose their private information with unauthorized parties. To learn a vehicle user's location, a service provider (SP) can sniff traffic exchanged between itself and a network operator to perform various traffic attacks, and set up an environment for Man in-the Middle attack, DoS attack, Sybil attack etc. There are also some active and passive types of attacks that are easily detectable by a user (Refer: section 4.2). Namely, if the service providers executed such type of attacks on road-traffic [22],

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

then vehicle users could detect these attacks and would stop using the respective malicious provider's services. Privacy and trust are related to each other. Security and Privacy are two integrated issues in the deployment of vehicular networks.

- **Trust**: It a paradigm of security, it belief that someone or something is reliable, good, honest and effective. It defines as "reliance on the integrity, ability or character of a person or thing". Mayer et al. [23] define trust as: *"... the willingness to be vulnerable based on positive expectation about the behaviour.*
  - Does the LBS context already involve a low level of trust?
  - If the LBS context involves a moderate to high level of trust, why are LBS being considered anyway?
  - Will the use of LBS in this situation be trust-building or trust-destroying?
- **Security:** It is the degree of resistance to or protection from harm. It applies to any vulnerable and valuable asset, such as person, dwelling, community, nation, organization [24]. It can be network security, information security etc.
  - What restrictions are placed on organizations (and their employees) that handle location information?
  - How well protected are the LBS electronic systems and subsequent support systems?
  - What measures are in place to manage mandatory LBS users?
  - What backup measures are in place in case the system fails?
- **Privacy:** It means "hide yourself from others" i.e. hiding your personal information, location etc. from unknown/unauthorized persons [6, 7, 9, 13, 21]. Privacy is the information that you don't want others to know i.e. it means entity's abilities to control the availability and exposure of information about yourself. In a vehicular network, user's privacy is important while communication with other users and also with infrastructure, user always worry about their personal data and their location.
  - Who has access to location information?
  - Can an individual wearing a tracking device deactivate it?
  - Do the benefits that accrue from LBS in a given context outweigh the impacts of seriously invading an individual's privacy?
  - Is this individual's privacy worth more than the safety and security of society
- **Others:** like who is controlling to who, and How?
  - Who is controlling whom, and for what reasons?
  - Does the person to be monitored need to consent?
  - Is an individual too impaired to consent to their own monitoring? If so, who should be able to make the decision for them?
  - If an individual does not consent to monitoring, are there special circumstances (e.g. an indictable crime), that warrants control without consent?
  - How can it be ensured that inaccuracies in reported location do not adversely affect the individual being monitored?

This section discusses about system models, threat models and arise issues in LBSs. Now next section will dealt with proposed architecture in detail.

4. PROPOSED ARCHITECTURE

There are a number of various researches representing the state of the art techniques to protect location privacy for example: Mobi-mix, Silent Mix Zone, Mini Mix zones, etc. [6, 21]. Figure 2 illustrates proposed architecture for location-based services (LBSs) that does not reveal location information of vehicle users to a service provider. When a vehicle user sends a query to a network operator then it forwards the query to a service provider. After received request by service provider (SP), it generates a response and forwards it to the network operator, which forwards it to the vehicle users. We can say that network operator work as sender and service provider as receivers i.e. each tern can discusses as:

4.1 Network Operator: A network operator implements the Query/Response Forwarder module, User Information database (UID) and Locator module. First the Query/Response Forwarder module forwards a query from a vehicle user to a service provider and then forwards a response from the service provider to the vehicle user. Received response received by vehicle user can be valid or not. There can be multiple service providers in an environment to provide LBSs. A vehicle user can pick up to a service provider for his /her query, where his /her network operator knows of his/her choice beforehand. Communication (Data traffic) between a network operator and a mobile user can be in different forms like SMS (or MMS) messages or GPRS using

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

TCP/IP protocol. The response received by a network operator from a service provider is encrypted with the public key of the network operator. The Query/Response Forwarder module decrypts the response and checks whether the obtained plaintext corresponds to a dummy response. Primarily, the goal of position dummies is to secure a VANETs user's true position by sending multiple false positions ("dummies") to the location server (LS) together with the true position. Dummy responses can be required to thwart traffic analysis attacks (refer section 3.2) and are not forwarded to a vehicle user. The Query/Response Forwarder module forwards an (encrypted) non-dummy response to the vehicle user. And for non-dummy responses, a second layer of encryption is used; it also encrypted with a vehicle user's public key. Using this process, provide encrypted data on both side (sender and receiver). During this communication, the network operator cannot learn any potentially confidential information returned by a service provider to the vehicle user.

The User Information database (UID) contains information about vehicle users, such as billing information their list of subscribed services, communication links with other people. Remember that, for each vehicle users, there is a public key, which will be used for encrypting their privacy information (Refer: figure-2). The vehicle user's information and the public key are established when a vehicle user signs up with the network operator. Finally the Locator module provides a mobile user's current location with identities to a service provider. The module always encrypts a user's location with his /her public key and kept it in the vehicle user information database. Traffic simulation can learn the vehicle user's location before handling the information to the service provider. To avoid tampering (or bogus) information or man in middle attacks etc. to maintain certain privacy level, the module also signs a vehicle user's location with its private key.

4.2 Service Provider: It provides LBSs to subscribed mobile devices. A service provider implements the UID, the Location Information database (LID), the Query Scheduler module, and the Trusted Computing Environment (TCE) module. The Vehicle User Information database keeps vehicle user-specific and service-specific configuration information required for answering queries from a vehicle user for example: a tracking service stores the identity of people that are allowed to track a mobile. Location Information database (LID) stores service-specific information about locations, such as places of interests (POI), weather or road conditions, road maps, or satellite pictures. The Query Scheduler module receives vehicle user's queries from a network operator and forwards them to the Trusted Computing module for further processing. After finishing of this process, the Query Scheduler module returns the generated response by the TCE module to the network operator. The TCE module has two main properties likely as *first;* it is possible for a vehicle user to remotely ensure that the module can access the mobile user's location only if the module's software corresponds to a configuration approved by a vehicle user (or a third-party auditor on the vehicle user's behalf). And *second,* the service provider deploying the TCE module cannot learn location privacy information of vehicle i.e. being processed by the TCE module.

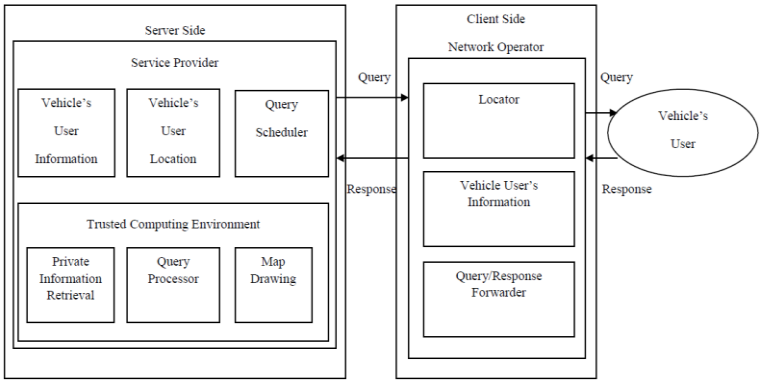

Fig. 2. Architecture for location-based services. The vehicle user sends a query via the network operator to the service provider, which uses the Trusted Computing Environment module for processing the query and generating a response.

4.3 Working: First this paper suggested Trusted Platform Module (TPM), to implement this module. This paper exploits the concepts of sealed storage and remote attestation to guarantee certain level of privacy to mobile users. Sealed storage prevents certain encrypted information from being decrypted on a computer unless the software running on a computer corresponds to a given configuration. Remote attestation, lets an entity that verify whether the software running on a remote computer corresponds to an expected configuration or not. These two concepts used in proposed architecture like as: Each vehicle user creates an asymmetric (or public) key pair and gives these public key pairs to his /her network operator, which stores the key in the UID (refer section 3.1). The Locator module uses this public key pair for encrypting the vehicle user's location when being processed by the service provider. The user gives the corresponding private key to the TCE module only in one

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

condition, if the vehicle users approve the software configuration of the respective module. This process exploits remote attestation concept. To avoid the private key leaks upon a compromise of the module, the module keeps the key in sealed storage. In this way, if the module gets compromised and its configuration changed by any intruders, the private key becomes inaccessible (or useless) and the module can no longer decrypt the vehicle user's location.

To ensure that, the service provider (SP) deploy the TCE module i.e. it cannot get any location information of a vehicle user from TCE module. Some additional precautions used here like;

- *First,* the software running on this module never provides output location information in plaintext form.
- *Second,* developers of the software should take special care to ensure that location privacy information of mobile users is immediately erased after its usage to decrease the risk of this information being swapped to disk.
- *Third*, the service provider's privileges for the machine on which the module runs should be limited. The provider cannot inspect the memory of the module, even if the provider has administrator rights on the machine.
- *Fourth*, a TPM (as suggested by the TCG) protects against software based attacks for example: sematic errors, syntactic errors, Trojan attacks, wormhole attacks, Sybil attacks etc., but not against (i.e. more expensive) hardware based attacks (for example: system errors etc.).

This paper can defend against this kind of attacks (software and hardware attacks) by implementing the TCE module on the XOM processor architecture [25] or in a secure coprocessor. The XOM architecture is not as widely used as TPMs and other secure coprocessors due to be expensive and to have limited computational power.

A vehicle user should review the software configuration of the TCE module. This software includes the operating system (OS) and algorithms that are required by LBSs. The vehicle users can require that the OS corresponds to a specific configuration for example; Linux kernel 2.6.17.8. In proposed architecture, our aim is to keep the algorithms easy and simple. And for additional security, the module uses the concept of employ secure logging [26]. Secure logging ensures that log entries cannot be modified. The vehicle users can validate processing of the module retroactively using secure logging. Moreover this, the components of Trusted Computing Environment module can discuss as: First there is Query Processor component, which runs service-specific algorithms, as required by a location-based service. PIR algorithm [1] allows the TCE module to retrieve an entry from the LID database without the permission of administrator of the database becoming aware of that "which entry is being accessed". The Map Drawing component is given a road map, as retrieved from the LID by the PIR component, and draws additional valuable information on the map like: the location of a vehicle user's friends or relatives. In this processing, a response generated by the TCE module might allow the SP (service provider) to learn the user's actual location and also provide additional functionalities. The network operator (or a traffic sniffer) learns other potentially sensitive information about the vehicle users. So to avoid these types of attacks, the module encrypts its response with the user's public key. Namely, the vehicle user creates a second asymmetric key pair, in addition to the one used for encrypting the vehicle user's location, and presents the public key to the TCE module after inspecting the module. The module generates a certificate that binds the public key to the vehicle user's identity. Private Key stores the generated certificate in the UID. Later queries received from the vehicle users should be signed with its private key to avoid tampering or bogus information or false messaging attacks. Moreover this, the module should also sign responses with its private key due to same reason. *(Note that*-Accuracy, certainty and correctness is the metric that determines the privacy of users. And entropy in k-anonymity is a measure of amount of information required to break the anonymity provided by the system).

This section proposed an improvement cryptographic model that maximizes the achieved location privacy for vehicle users, minimize computational complexity and takes into account the cost induced other approaches to mobile nodes and also develop a method of providing feedback to VANET users. In next section, this paper discusses various privacy enhanced LBSs in brief.

5. PRIVACY-ENHANCED LOCATION-BASED SERVICES

Let's now discuss "how we can exploit the architecture" presented in previous section to implement a tracking service and nearby information, locate friends' service etc. Privacy-Enhancing Technologies aim at allowing users to take one or more of the following actions related to their personal data sent to, and used by, online service providers, merchants or other users [6]. Privacy enhanced location based services can be discussed as:

Volume 5, Issue 5
October 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

5.1 Tracking Service: It allows a vehicle user to track a third party i.e. when a third party left any boundary area, the vehicle users warned about it. The Query Scheduler module needs to ensure that the third party has given consent to being tracked, as indicated in the party's privacy preferences stored in the UID. If there is consent, the module queries the Locator module for the location of the third party and hand over the following information like: vehicle user's query, the encrypted location, and the boundary area to the TCE module. This work can address timing, transition, range query attacks by moving consent checking into the TCE module and by having a party digitally sign its privacy preferences. However, this service makes the TCE module more complex. This paper prefers a retroactive approach, where the TCE module employs secure logging to log all requests. This way, a third party can identify a malicious service provider and stop using the provider's services by revoking the public key used by the Locator module to encrypt the party's location.

5.2 **Locate-Friends Service:** It allows vehicle users to locate their friends. When receiving a vehicle user query, the Query Scheduler Module (QSM) ensures that the vehicle user's friends have consented to this information exchange. Next, the module retrieves the friend's encrypted location from the Locator module. The Query Processor component in the TCE module decrypts the information and hands it over to the Map Drawing component, which generates one or several maps. The Query Processor component encrypts these maps and then QSM returns them to the vehicle users. This service is subject to an attack where a service provider becomes a vehicle user and locates himself as good friends (trustworthy) to other vehicle users.

***5.3 N*earby-Information Service:** In this service, vehicle users informs to service provider about their current locations. And the service provider returns valuable information about these current locations like places of interest, advertisements or weather and traffic alerts. This paper implements the services such that the vehicle users can retrieve information about their location from the provider without revealing their location to the provider.

5.4 **Locate-Me Service (Proximity Service):** In this, it allows vehicle users to learn their current location. Upon receiving a vehicle user's query, the Query Scheduler module retrieves the vehicle user's encrypted location from the Locator module and hands over the query and the location to the TCE module. The Query Processor component decrypts the location and invokes the Map Drawing component to visualize the information. Next, the Query Processor component signs and encrypts the generated map and returns it to the Query Scheduler module. The Query/Response Forwarder module must forward the response to the third party which forwards it to the mobile users via the Query/Response Forwarder module.

5.5 **Nearby-Friends Service:** It is similar to the locate-friends service, but it locates friends who are nearby only. Ideally, the service provider cannot learn which of a vehicle user's friends are nearby. In this, the first step is identical to the locate-friends service. This approach provides a benefit that only a single query needs to be sent to the network operator.

5.6 **Similar-Interests Service:** In this, it reveals a list of nearby people with similar interests to the vehicle users. Upon receiving vehicle user's queries, the Query Scheduler module first retrieves encrypted location of all the people who have signed up to the similar-interests service from the network operator. Querying for the location of all the vehicle users who have signed up to this service is not efficient. Later, we discuss "how the closeness function (as provided by the Locator module) can make querying more efficient"? For each person signed up to the similar-interests service, the network operator will return her identifier and her encrypted location. The Query Scheduler module hands over the identifier and location to the TCE module, which determines people nearby the vehicle user issuing the query. Next, this module retrieves these people's interests using the PIR component from the vehicle user information database (UID). Through this, the service provider cannot infer which people are nearby. A vehicle user identifier should not be encrypted with the public key of the vehicle user. Otherwise, the TCE module would have to search all of its vehicle users' private keys for a matching decryption key, which is not efficient.

5.7 **Personal-Navigator Service:** It offers directions to a target location. Namely, vehicle users submit their target location to the service provider. Then, the service provider queries the network operator for the location of the vehicle users i.e. generate directions from this location to the target location, and send them to the vehicle users. We could implement this service in a similar way as the other services and have the TCE module decrypt a user's current location, as received from the Locator module, and have it compute a path to the target location. This service depends only on the target location; the vehicle user's current location and it is independent on the

identity of a vehicle user. This approach does not allow a service provider to identify a vehicle user directly, but the provider can still track the vehicle user's path to the target location and potentially identify the vehicle users indirectly with the help of a physical observer.

Finally this section discusses about privacy enhanced technologies to protect location privacy in LBSs like proximity service: tracking service; nearby information, personal navigator etc. Next section concludes this work in brief.

6. CONCLUSION AND FUTURE WORKS

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. Perfect privacy is clearly impossible as long as communication takes place. Beside this, to recover above defined issues, various approaches and models have been proposed by several researchers. But there is not a single privacy preserving technique that covers all privacy requirements to maintain location privacy in secure way due to some advantages and disadvantages w.r.t changing in privacy requirements. In Mix zone, each vehicle will keep silent in transmission, and randomly update its pseudonym when it travels out of it and becomes reactivated. But mix-zones are also prone to continuous query (CQ)-attacks when the mobile clients obtain continuous query services, and work efficiently only in crowded area. However, now considering a system without using pseudonyms suffers from different other problems for instance; missing accountability or high communication overhead due to broadcasting (or huge storage required) or fast verification or fast key generation process. This paper proposed an improvement mathematical model of mix-zone approach i.e. maximizes the achieved location privacy in the system with minimizing computational complexity.

This paper has demonstrated that it is possible to build location based services for which the provider of these services does not become aware of vehicle user's location. Our next work concerns about implementation result of this proposed work, with a detailed comparison among other existed privacy protection methods. However, research into location privacy is a relatively young field and many of the research issues/challenges outlined in [4] are likely to be addressed in the near future.

ACKNOWLEDGEMENT

The authors have declared that they have no acknowledgement.

REFERENCES

1. B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private Information Retrieval," in Proceedings of 36th IEEE, Symposium on Foundations of Computer Science, October 1995, pp. 41–50.
2. https://www.cs.purdue.edu/homes/bb/CLEAN--z--SHORTEST--Privacy-Trust_Tradeoff.pdf
3. http://satoss.uni.lu/members/phd-theses/xchen14-thesis.pdf
4. Amit Kumar Tyagi, N. Sreenath, Future Challenging Issues in Location Based Services, IJCA, March, (0975 – 8887) Volume 114 – No. 5, 2015.
5. U. Hengartner, "Enhancing User Privacy in Location-based Services," Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR 2006-27, August 2006.
6. Amit Kumar Tyagi, N. Sreenath, A Comparative Study on Privacy Preserving Techniques for Location Based Services, BJMCS, July, 2015 10(4): 1-25, 2015.
7. Amit Kumar Tyagi, N. Sreenath, Preserving Location Privacy in Location Based Services against Sybil Attacks, IJSIA Vol.9, No.12 (2015), pp.189-210, December, 2015.
8. G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," Pervasive Computing, vol. 2, no. 1, pp. 56–64, January-March 2003.
9. Amit Kumar Tyagi, N. Sreenath, Providing together Security, Location Privacy and Trust for moving objects, IJHIT Vol.2, No.3 (2016), pp. 221-240, March, 2016.
10. M. Spreitzer and M. Theimer, "Providing Location Information in a Ubiquitous Computing Environment," in Proceedings of SIGOPS '93, Dec 1993, pp. 270–283.
11. J. I. Hong and J. A. Landay, "An Architecture for Privacy-Sensitive Ubiquitous Computing," in Proceedings of Second International Conference on Mobile Systems, Applications, and Services (MobiSys 2004), June 2004, pp. 177–189.
12. K. Tang, J. Fogarty, P. Keyani, and J. Hong, "An Anonymous and Privacy Sensitive Approach to Collecting Sensed Data in Location-Based Applications," in Proceedings of ACM Conference

on Human Factors in Computing Systems (CHI2006), April 2006, pp. 93–102.
13. Amit Kumar Tyagi, Dr.N.Sreenath et. al., Providing Privacy Preserved Location and Trust Enabled Services for Location Based Services‖, International Conference on Soft Computing, Intelligent Systems and Applications, 8-9 April, 2016, Springer, Bangalore, India.
14. M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in Proceedings of First International Conference on Mobile Systems, Applications, and Services (MobiSys 2003), May 2003.
15. B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," in Proceedings of 25th International Conference on Distributed Computing Systems (ICDCS 2005), June 2005.
16. M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," in Proceedings of Third International Conference on Pervasive Computing, May 2005, pp. 152–170.
17. R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," in Proceedings of 6th Workshop on Privacy Enhancing Technologies (PET 2006), June 2006, pp. 40–58.
18. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," in Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB 2006), September 2006, pp. 763–774.
19. N. Ravi, M. Gruteser, and L. Iftode, "Non-Inference: An Information Flow Control Model for Location-based Services," in Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS 2006), July 2006.
20. WaveMarket, Inc, "Family Finder," hTC://www.wavemarket.com, accessed February 2007.
21. Amit Kumar Tyagi, N.Sreenath, "Location Privacy Preserving Techniques for Location Based Services over road networks", ICCSP, 2-4 April, India. 2015.
22. http://crypto.stanford.edu/~dabo/papers/locpriv.pdf
23. Mayer, R., Davis, J., Schoorman, F.D.: An integrative model of organizational trust. Academy of Management Review 20(3), 709–734 (1995).
24. https://prezi.com/3rv6asny2jsu/security-is-the-degree-of-resistance-to-or-protection-from/
25. D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell, and M. Horowitz, "Architectural Support for Copy and Tamper Resistant Software," in Proceedings of 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-IX), November 2000, pp. 168–177.
26. B. Schneier and J. Kelsey, "Cryptographic Support for Secure Logs on Untrusted Machines," in Proceedings of 7th Usenix Security Symposium Proceedings, January 1998, pp. 53–62.