Security Journal (2023) 36:165–200
https://doi.org/10.1057/s41284-022-00334-5

ORIGINAL ARTICLE

PISA: A proximity-based social networking (PBSN) protection model

Asslinah Mocktoolah Ramtohul[1] · Kavi Kumar Khedo[1]

Accepted: 7 March 2022 / Published online: 28 March 2022

Abstract

The widespread adoption of Proximity-based Social Networking (PBSN) applications has been accompanied with several privacy concerns involving location information. As a result, many studies were directed towards innovative privacy-preserving solutions to provide a secure platform for mobile users. Despite the success of these solutions, there is a research gap in terms of the evaluation and analysis of their protection features. An in-depth evaluation of the privacy and security provisions in PBSN systems is necessary to assess the protection properties. In this paper, a comprehensive protection assessment model, the PISA model, is proposed to evaluate the privacy and security features of PBSN frameworks. The main objectives of this study refer to defining the protection goals of PBSN systems by reviewing the privacy and security requirements, analyzing the associated location privacy threats, and formulating the PISA model based on the quantification of the related protection goals using the privacy metrics. The study adopts an exploratory research methodology and explores four distinct research questions. The PISA model enables an extensive evaluation of privacy-preserving PBSN frameworks concerning their privacy and security features which can be further useful for researchers during the development of privacy-preserving algorithms to prevent flaws in advance and improve where necessary. Future works of the current research can focus on the analysis of privacy policies and adversary models based on their assumptions, resources, and capabilities.

Keywords Privacy assessment · Evaluation metrics · Location-based systems · Proximity-based social networking · Security analysis

✉ Asslinah Mocktoolah Ramtohul
ashlinahmee@gmail.com

[1] Faculty of Information, Communication and Digital Technologies, University of Mauritius, Réduit, Mauritius

Introduction

The continuous development of technologies during the past decade has changed the way people live and carry out their daily activities. Based on this trend, a new paradigm called the Internet of Things (IoT) has been introduced offering a 3A connectivity service, that is, anyone can be connected at any place and anytime (Arseni et al. 2015). As a result, the way people interact and communicate with each other changed drastically, with the advent of the Internet and especially with today's craze: Online Social Networking (OSN). With the emergence of smartphones, OSN gained further popularity since access to these networks is now more convenient and easier. According to Pew Research Center (2018), it is known that 92% of teens go online daily using their mobile phones.

Based on the recent advances of mobile devices and OSN applications, a new type of networking has emerged—Proximity-based Social Networking. Proximity-based Social Networking (PBSN) can be referred to as social networking services provided to physically proximate users on their mobile devices through Wi-Fi, Bluetooth, or Cellular Networks using their location information. The main activity on these networks, known as "check-in," allows the users to share their real and current geographical location automatically in their posts. Users can discover friends in the vicinity, pick out nearby restaurants, or select routes based on traffic information. As a complement to traditional web OSN platforms, PBSN allows more tangible face-to-face interactions among the users.

As more people embraced the PBSN phenomenon, much emphasis has been directed towards the security and privacy of the users. Securing data and information of PBSN users are known to be more crucial than that of OSN in such a way that real locations of the users can be exposed and movements of the users can be followed via a map displaying all the places that the users have checked in (Kong et al. 2014). In addition to the information of the users' usual routes being leaked, the mode of transport used also can be predicted according to Puttaswamy and Zhao 2010. On top of that, private and confidential location information such as visits to hospitals or bars can be exposed (Li et al. 2016). Hence, people are more reluctant to share their location information due to the dangers associated such as being stalked, robbed, or sexually assaulted (Liu 2009). Consequently, many PBSN frameworks have adopted privacy-preserving techniques in their system models to further encourage users to make the most of these services such as k-anonymity, obfuscation, spatial cloaking, and cryptography among others (Zhu and Cao 2011; Sun et al. 2016; Xue et al. 2016; Ravi et al. 2019; Song et al. 2015; Li et al. 2011). Vu et al. (2012) use a trust server known as the anonymizer to obtain K-anonymous location privacy by removing the user's ID and opt an anonymizing spatial region (ASR) which takes into consideration the user and at least K-1 users in the vicinity. Applaus employs a location proof system in which an authorized verifier cross check the trustworthy level of the location (Zhu and Cao 2011). Additionally, dynamic pseudonyms are used in each device as additional protection for the location data, hence, protecting the users' identity and location details. PrivCheck (Yang et al. 2016) is a customizable privacy-preserving framework where the user check-in data are obfuscated to minimize user private data leakage under a given data distortion budget to prevent inference attacks. Song et al. (2015) proposed a cloaking system model called anonymity of motion vectors (AMV) which provides anonymity for spatial queries, thus, preventing the real locations of mobile users to be revealed. User queries can be addressed and the CR is minimized by predicting user movements based on their motion. Werner (2016) makes use of strong cryptographic functions to enable a good trust relationship between users. The system makes use of Locagrams which act as the basic messaging system of the PBSN service.

Despite the success of these privacy-preserving solutions to protect the location information and the corresponding personal information such as the identity of the users, it is observed that limited analyses have been carried out to assess how secure the solutions are and how well the privacy requirements are enforced. The existing literature is either directed to the assessment of the security and privacy performance by addressing only part of the privacy requirements or to demonstrate how a particular attack is prevented. For instance, Buchanan et al. (2013) carried out an analysis on privacy-preserving methods of recent works by assessing the techniques used in the studies which further reduce the impact of location tracking. Jiang et al. (2021) outlined the potential risks associated with location-based servers and performed an analysis of the existing LPPMs (Location Privacy-Preserving Mechanisms) in terms of the level of privacy and performance. On the other hand, the study of Sun and Xue (2020) focused on the assessment of online Automated Privacy Policy Generators (APPGs) by analyzing the completeness of privacy policies of applications to determine the missing categories and items in the policies. Nevertheless, there is a research gap in evaluating the privacy-preservation techniques in terms of the privacy and security goals, location-related threats, and risks associated with the privacy-preserving solutions. This prevailing paucity is addressed in this study by carrying out a comprehensive assessment of the protection features of PBSN frameworks by introducing the PISA model. The latter will be useful to evaluate existing privacy-preserving PBSN systems and carry out a thorough analysis of the privacy-preserving solutions that they proposed. It will also help improve the algorithms during their development to avoid any potential loopholes or weaknesses in advance.

The objectives of this study are detailed as follows:

1. Review the different privacy and security requirements of existing privacy-preserving algorithms of PBSN systems and categorize them into a series of protection goals.
2. Carry out an in-depth analysis of the different threats associated with PBSN systems including the information that can be accessed during an attack or the resources available to adversaries.
3. Formulate a protection assessment (PISA) model for PSBN based on the quantification of the related protection goals using the privacy metrics.
4. Evaluate recent PBSN frameworks using the PISA model highlighting the protection features and shortcomings based on the threat models.

The rest of the paper is organized as follows. Section 2 presents the methodology of the study and the PISA model is introduced in Sect. 3 outlining the protection goals, threat models, and evaluation metrics. An exhaustive assessment of recent PBSN frameworks is carried out in Sect. 4 based on the PISA model, and the paper is rounded off with some concluding remarks and future works in Sect. 5.

Methodology

The exploratory research methodology has been adopted in this study by conducting a thorough analysis of the privacy requirements and privacy threats of PBSN systems. The following steps of the evaluation process have been identified accordingly:

Step 1 Identification of protection goals

The privacy and security requirements of PBSN systems are identified based on the secured identities of the users and their private locations. This step will help elucidate the goals of the assessment. The protection goals presented in this paper are derived from the privacy and security requirements of location-based systems. They cover most of the privacy and security prospects of PBSN systems and refer to data privacy, spatial privacy, unlinkability, trust, and security.

Step 2 Scrutiny of threat models

Location privacy of users can be threatened in different ways based on the characteristics of the PBSN system and based on the services provided to the users (Lee et al. 2013). Before assessing privacy and security, it is important to outline the threat models related to location privacy and also identify the resources or information which can be available to the adversary.

Step 3 Definition of evaluation metrics

The most important step of an assessment model is to define the appropriate metrics. This step is also regarded as the core process of the evaluation (Shokri et al. 2010). These privacy metrics are useful to quantify the protection goals. Additionally, the identified protection goals and threat models determine which kinds of metrics can be used and how these metrics can be assessed.

Step 4 Evaluation and analysis

Once the protection goals and threat models have been identified, the evaluation of PBSN systems can start with respect to the privacy metrics. The evaluation metrics are determined based on the identified protection goals and threat models. Once the evaluation is done, the results are analyzed and criticized.

Additionally, four research questions that address the different dimensions of the proposed model are identified. These research questions will help define the fundamental steps of the assessment model.

RQ1 Which privacy and security requirements should be considered by template protection to define privacy-preserving algorithms in PBSN systems?

RQ2 What are the protection goals that substantiate the privacy and security requirements of PBSN systems?

RQ3 What are the most influential privacy threat models that apply to PBSN systems?

RQ4 Which evaluation metrics are needed to quantify the protection goals?

PISA model

In this section, the PISA model is proposed to carry out a comprehensive protection assessment of PBSN systems and has been inspired by the work of template protection for biometric systems by Zhou (2011). The protection goals are defined to cover the essential privacy and security requirements that privacy-preserving algorithms aim to achieve. Threat models of PBSN systems are also outlined to define the privacy threats, risks, capabilities, and resources available to the adversary. The evaluation metrics associated with location privacy are proposed and are used to quantify the protection goals.

Figure 1 illustrates the proposed evaluation PISA model, which addresses the challenge of full-scale security and privacy assessment of PBSN systems in practice and can be helpful during the development of any location privacy-preserving algorithms.

The first step in the assessment of PBSN frameworks is to identify the privacy requirements of the privacy-preserving solution. From this diagnosis, the protection

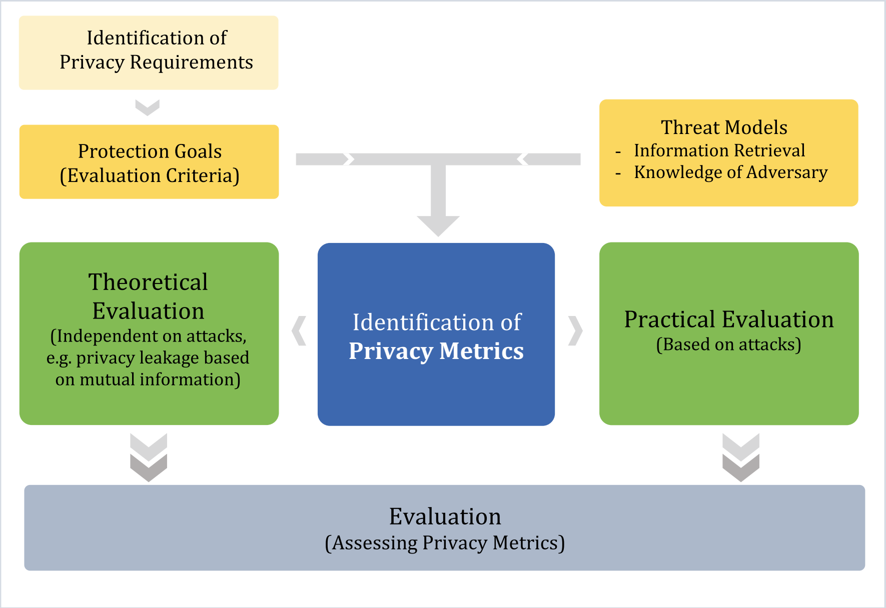
Identification of Privacy Requirements
Protection Goals (Evaluation Criteria)
Threat Models
- Information Retrieval
- Knowledge of Adversary
Theoretical Evaluation
(Independent on attacks, e.g. privacy leakage based on mutual information)
Identification of Privacy Metrics
Practical Evaluation
(Based on attacks)
Evaluation
(Assessing Privacy Metrics)

Fig. 1 The PISA model

goals are described. The threat models of the frameworks are analyzed and classified. The privacy metrics are then construed to design the evaluation process based on which the evaluation starts. The evaluation can be carried out in two different ways: the practical evaluation and the theoretical evaluation. The practical evaluation measures the different attacks of the adversary by taking into consideration his/her prior knowledge and his/her resources and by measuring the efficiency of the attack by the adversary's success rate or recovery rate. The theoretical evaluation is independent of the adversary's attacks but refers mainly to the measure of information theoric metrics such as entropy, mutual information, etc. The results with the evaluation metrics are obtained, and an analysis process is carried out. If more than one privacy metric is used, the evaluation will be done for each and the results should be compared with each other.

An alternative way to assess the privacy of PSBN frameworks is to identify the privacy policies of the application. These privacy policies should be analyzed and studied based on which the data practices are gathered and thereafter assessed. Different criteria characterizing the privacy policies are identified based on which the privacy requirements may be derived. The policies will differ in terms of privacy level, location, and privacy threats. Another direction to privacy evaluation is by making use of different use cases such as security use cases, location-tracking use cases, or misuse cases. The use-case-driven modeling method can be adopted to assess the security and privacy requirements in a more structured form.

These methods require further analysis and have not been covered in this study but can be considered as future works.

Protection goals

The preliminary step before starting an evaluation is to define the evaluation criteria, which corresponds to the privacy aims of the assessment model and outline the threat models. Based on the frequently changing context of PBSN users, it should be noted that omitting the privacy requirements of the PBSN application will affect the user's privacy and will imply how the PBSN application is being adopted or used (Thomas et al. 2014). Figure 2 gives an overview of the privacy and security requirements of PBSN applications. Considering these properties, the following evaluation criteria are proposed: data privacy, spatial privacy, unlinkability, trust, and security. The privacy and security assessment framework can be quantified with these protection goals and enable empirical evaluation.

Threat models

Privacy-preserving techniques prevent different types of attacks on personal information and location information. To carry out a thorough privacy and security assessment, it is crucial to identify the various privacy threats that can be faced by PBSN users. Additionally, the information and resources available to the adversary should be taken into consideration. Based on the privacy threats proposed by recent surveys (Do et al. 2019; Babar et al. 2010; Solove, 2005), a set of 16 threat models,

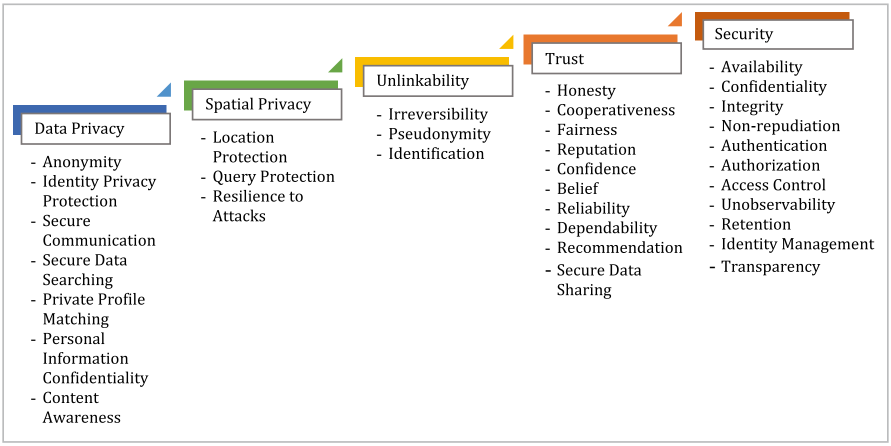

Fig. 2 Taxonomy of privacy and security requirements

applicable for PBSN systems, are presented in this paper. The classification of the selected privacy threats has been inspired by the work of Solove, 2015 and is illustrated in Fig. 3.

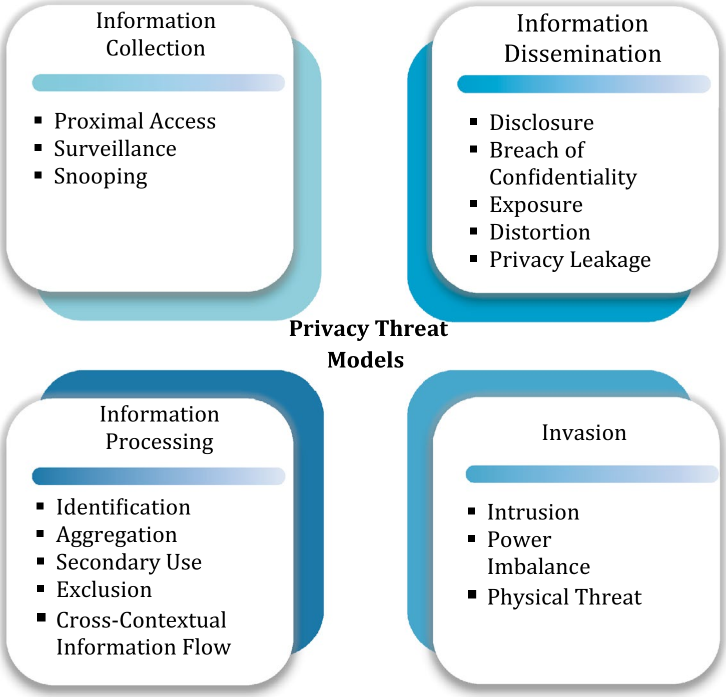

Fig. 3 Privacy threat models

Based on the classification of privacy violations as proposed by Solove, 2015 and taking into consideration privacy threats relevant to location-based applications, the threat models are presented as below:

Information collection

Information collection in PBSN systems refers to the process of data gathering among targeted users located in proximity (Raschke et al. 2014). The information collection can be possible based on the data available due to proximal access, surveillance, and snooping. Table 1 provides a detailed description of each privacy threat for Information Collection.

Information processing

Information Processing is the usage, storage, and manipulation of collected data and relates to different ways of connecting data together and linking the data to another set of information or persons (Mamonov and Benbunan-Fich 2018). Further details about the privacy threats of information processing are presented in Table 2.

Information dissemination

The dissemination of information is the act of spreading or transferring personal data or the threat to do so (Lilien & Bhargava, 2006). It comprises the following privacy threats: disclosure, breach of confidentiality, exposure, distortion, and privacy leakage. Table 3 illustrates the description of each and the privacy harms associated.

Invasion

Invasion refers to the deliberate intrusion on a user's personal details or private activities and does not always involve information (Chamarajnagar and Ashok 2019). It relates to attacks conducted rather than activities involving data. The different privacy threats associated with invasion are described in Table 4 with their corresponding privacy harms.

Privacy metrics

The privacy metrics related to proximity mobile systems are presented in this section and a brief description of each is given. Also known as, the evaluation metrics, the privacy metrics are important to quantify the protection goals. Wagner and Eckhoff (2018) described four characteristics of privacy metrics namely adversary models, data sources, inputs, and output measures. These characteristics are helpful to classify the privacy metrics and similarly to the survey done, in this study, the classification is based on the output measures. Metrics from different output categories can provide a more comprehensive estimate of privacy as reported by the authors. However, only the appropriate

Table 1 Information collection

Privacy threat	Description	Privacy harms
Proximal access	The proximal access of users located in closed proximities leads to the availability and accessibility of a pool of information for unintended recipients	Loss of reputation Loss of anonymity Loss of freedom Embarrassment
Surveillance	Surveillance is the close monitoring of user activities or user behavior in the network by observing, listening, or recording their moves	Inhibition Emotional harm Physical harm
Snooping	Service providers are curious about the personal information of the users and try to retrieve available information by observation or collect data from the communication between other users by eavesdropping	Loss of reputation Emotional harm

Table 2 Information processing

Privacy threat	Description	Privacy harms
Identification	Retrieving users’ personal information or linking any information to particular users	Identity theft Loss of anonymity
Aggregation	Different datasets of a user can be combined or can be linked using the collected information to produce new types of information about the user without his/her consent	Discrimination
Secondary use	Collected data can be forwarded to third parties, which will be used for additional purposes than it was intended to without the user’s consensus	Emotional harm Loss of reputation
Exclusion	Refraining from informing users concerning the data collected for them or not notifying them about how their data are being used	Betrayal of trust Emotional harm
Cross-contextual information flow	Information collected for a user in one context may be used in another context to infer new information or simply to use it in a harmful way	Loss of reputation Discrimination

Table 3 Information dissemination

Privacy threat	Description	Privacy harms
Disclosure	Disclosure is the act of revealing or exposing information about a user resulting in a negative impact on the user	Reputational damage
Breach of confidentiality	Violation of trust while making confidential information known to others, e.g., when private information is disclosed to a third party without the consent of the data owner	Betrayal of trust Emotional harm Relationship Breakdown
Exposure	Exposure involves the uncovering of sensitive and emotional attributes of a user-causing privacy harms such as humiliation or embarrassment	Humiliation Embarrassment Relationship Breakdown Physical danger
Distortion	Distortion is the act of the dissemination of inaccurate, misleading, or incomplete information about an individual	Emotional harm Loss of reputation
Privacy leakage	Unauthorized spread of data within a network to any external recipients even if defined privacy rules are set to protect the corresponding information	Physical danger Loss of anonymity Loss of freedom

Table 4 Invasion

Privacy T privacy threat heart	Description	Privacy Harms
Intrusion	Intrusion involves the information flow by interfering into a user’s life causing a disturbance in his/her daily activities or destroying his/her freedom, e.g., an attacker may stalk a user to deduce his/her daily route or work location	Loss of freedom Emotional harm
Power imbalance	Malicious users may follow closely a user’s daily activities, collect information about the user’s personal life, and ultimately use sensitive data to control the user	Loss of freedom Relationship breakdown
Physical threat	Users may be victims of physical harassment if the user identity information or sensitive location details are known by attackers	Physical harassment stalking

metrics related to location-based systems are studied in this paper outlining the related classifications. Figure 4 presents the output measures relevant to PBSN systems and the metrics associated with each are illustrated.

Uncertainty metrics

Uncertainty metrics measure the ambiguity of an adversary, that is, how uncertain he/she is about his/her estimate (Thuiller et al. 2019). For example, in location-based systems, the uncertainty metrics measure how uncertain an adversary is to associate a user with his/her current location. Table 5 provides an insight into the different uncertainty metrics related to location-based systems.

Error metrics

Error-based metrics quantify the error an adversary makes while estimating the user's identity or location (Al-Dhubhani et al. 2019). Table 6 describes the two error-based metrics identified for PBSN systems.

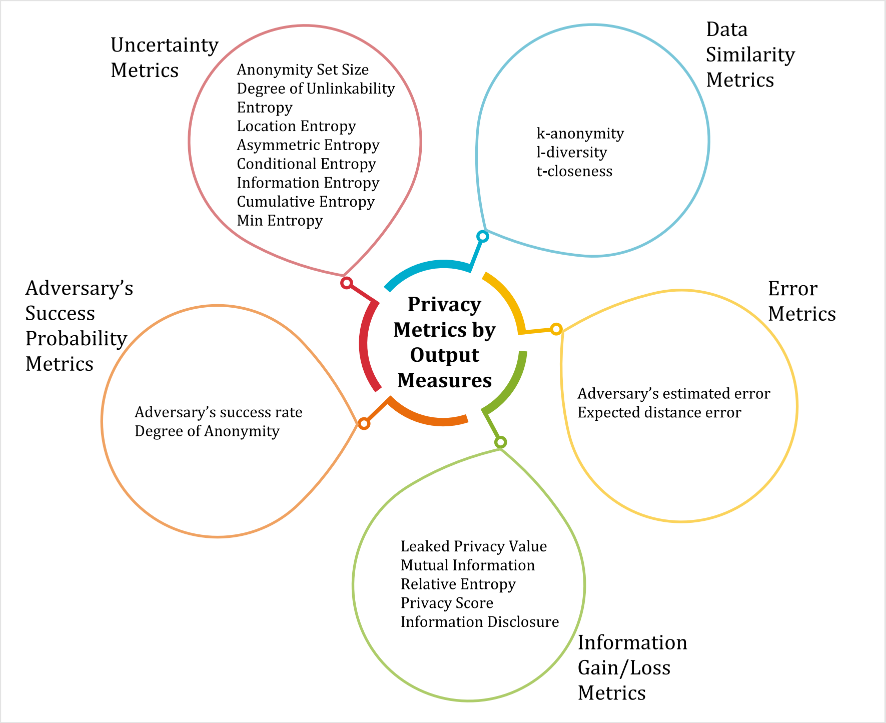

Fig. 4 Privacy metrics classified by output measures

Table 5 Uncertainty metrics

Uncertainty metrics	Description	Application of metric in location privacy
Anonymity set size	Set of other proximity users that the adversary cannot differentiate from a particular user	Anonymity sets can be applied to locations and location pairs such as home/work
Degree of unlinkability	The uncertainty of the adversary is measured on how items are related and the prior knowledge of the adversary is taken into consideration	The degree of unlinkability masks the correlation between the user's identity and his/her location
Entropy	The uncertainty to predict the value of a random variable. Entropy decreases with the increased information of the adversary	Entropy measures how well an adversary can disclose the position of a user
Location entropy	Location entropy can be defined as the uncertainty to determine the real location of a user from other users. It also represents the miscalculation of the user's planned next destination while he is at a certain place	Can be used in cases where privacy is measured at different points in time, e.g., the adversary tracks users during a certain timeframe and thus entropy is estimated at every point in time
Asymmetric entropy	Asymmetric entropy is used instead of entropy when the adversary has prior information about the distribution	It is used when the adversary has some information about the user's location or routes
Conditional entropy	The conditional entropy, with respect to two random variables, measures how much information is needed to describe the second variable if the first one is known	A user's work location can be deduced by his/her location during weekdays. A user's religion or even health state can be revealed by his/her visits to churches and clinics
Information entropy	The quantitative measure of how much information is associated with a set of data and the uncertainty over a probability distribution	Finding the link between a user's old and new pseudonym in a mix zone when users make use of different pseudonyms in different locations
Cumulative entropy	Cumulative entropy measures how much entropy can be collected on a route through a series of independent mix zones	Entropy is calculated in each mix zone on a user's path to estimate the adversary's uncertainty
Min-entropy	Min-entropy is known as a pessimist metric since it measures the certainty of the estimate of the adversary	It represents the worst-case scenario where the adversary has the highest probability at a certain location

Table 6 Error metrics

Error metrics	Description	Application of metric in location privacy
Adversary's expected estimated error	The adversary's estimated error refers to the incorrectness of the adversary's probability of error	The adversary's correctness is measured by calculating the expected distance between the real location and the estimated location using a distance metric
Expected distance error	The expected distance error measures the distance between the adversary's estimated location and the user's current location. As the adversary's strength in estimating the location decreases, the distance error increases	Different locations are assigned hypotheses and the distance between the correct user location and the location in the hypothesis gives the expected distance error

Data similarity metrics

The similarity metrics, as described in Table 7, measure the similarity between the estimate of the adversary and the real information (Kim et al. 2019).

Information gain/loss metrics

This category of privacy metrics focuses on the amount of information acquired by the adversary. The less information gained by the adversary relates to higher privacy and the more information is disclosed corresponds to the privacy lost by users (Amar et al. 2018). Table 8 provides the description and application of the metrics in location privacy.

Adversary's success probability metrics

The adversary's success probability metrics measure the success of the adversary, that is, the number of nodes that have been identified correctly by the adversary (Wagner 2015). Table 9 provides more details about this type of metric.

Evaluation and analysis

Table 10 provides an overview of the different metrics discussed above. The metrics quantify the protection goals based on the different threat models. The measurability details show how the metrics are applicable in practice. Table 10: Privacy Metrics for Assessment of Privacy and Security Protection.

Table 10 provides an empirical evaluation giving a substantial measurement of the privacy metrics. The measurability provides an insight into how applicable these metrics are in practice. The uncertainty metrics show that high privacy correlates

Table 7 Data similarity metrics

Data similarity metrics	Description	Application of metric in location privacy
k-Anonymity	The k-anonymity metric protects against identity disclosure in such a way that it ensures that a particular user cannot be identified from a group of k-users	This metric can be used where the location information in a location query corresponds to an area where the query sender is indistinguishable from at least k–1 other users also present in that area
l-Diversity	l-diversity caters for attribute disclosure, unlike k-anonymity where each value of the sensitive attributes is distributed in a well-represented sequence in an anonymized table	l-diversity is efficient in cases where users are not located close to each other
t-Closeness	In t-closeness, the distance of the distribution of a sensitive attribute is not more than a specified threshold, t to the distribution of the attribute in the overall table	The distance between 2 users must be smaller than the threshold t

Table 8 Information gain/loss metrics

Information gain/loss metrics	Description	Application of metric in location privacy
Leaked privacy value	The leaked privacy value refers to an average amount of information accessible to the adversary. Information is considered leaked when the estimate of the adversary for the true outcome is above the set threshold	Information leaked may correspond to the user's location or can be related to the user' personal information which can be associated with his/her location
Mutual information	Mutual information relates to the amount of information that is shared between the adversary's estimate and the true value. The more information shared, the lower is the privacy	Mutual information is calculated between the true location of the user and the data based on the adversary's observation
Relative entropy	Relative entropy measures the difference between the distribution of the adversary's estimate and the real value. It is an estimate of the additional information that is needed by the adversary to construct the true value	For example, in a location privacy scenario, the adversary may aim to find out which points of interest a user has visited
Privacy score	The privacy score refers to the privacy risk associated with any visible or shared information on the user's profile, e.g., the user's gender	If a user shares his/her religious belief, e.g., being a Christian, the adversary may estimate his/her location on a specific day, i.e., user-visiting church on a Sunday
Information disclosure	Information disclosure is the exposure of information to users or third parties who are not supposed to have access to that information	Different geographic locations are disclosed to the adversary when a user travels on a certain path

Table 9 Adversary's success probability metrics

Adversary's success probability metrics	Description	Application of metric in location privacy
Adversary's success rate	The adversary's success rate indicates how likely the adversary is to succeed in estimating the user's identity or location	For example, the estimate can reflect the percentage of the vehicles tracked correctly
Degree of anonymity	The degree of anonymity refers to the probability assigned by the adversary to a particular user. This information is useful to determine the anonymity set by the system for a user in a worst-case situation	This degree depends only on the number of users closely located to each other, and no other information is available on how distinguishable the user is within the anonymity set

Table 10 Privacy metrics for assessment of privacy and security protection

Privacy metrics	Privacy threat models	Protection Goals	Measurability	Comments
Uncertainty metrics				
Anonymity set size	Identity disclosure Proximal access Identification	Data privacy spatial privacy	Medium	Anonymity Set Size is useful when used together with normalized entropy
Degree of unlinkability	Cross-contextual information flow	Unlinkability	High	Used to measure the relationships between users
Entropy	Surveillance Disclosure	Security	High	Uncertainty to predict the value of a variable
Location entropy	Physical threat Exposure	Spatial privacy	High	Uncertainty to determine the real location of a user from other users
Asymmetric entropy	Physical threat Exposure Aggregation	Data privacy Spatial privacy Security	Medium	Asymmetric Entropy is used instead of Entropy when the adversary has prior information on the user
Conditional entropy	Cross-contextual information Flow Power Imbalance	Security	Medium	Measures the amount of information to determine a second variable if the first is known
Information entropy	Misinformation Identification Distortion	Unlinkability	Medium	Can be used to determine the link between old and new pseudonyms of a user in a mix zone
Cumulative entropy	Surveillance	Spatial privacy Unlinkability	Medium	For location and routes
Min-entropy	Physical threat Exposure Disclosure	Security irreversibility	Medium	The adversary has the highest probability (worst-case scenario)
Error metrics				
Adversary’s estimated error	Misinformation Identification	Security Data privacy Spatial privacy	Medium	Incorrectness of adversary
Expected distance error	Aggregation	Security Spatial privacy	Low	Difference between the adversary’s estimate and the true location

Table 10 (continued)

Privacy metrics	Privacy threat models	Protection Goals	Measurability	Comments
Data similarity metrics				
k-anonymity	Identity disclosure	Data privacy Trust	Medium	Similar to anonymity set size but does not consider the adversary
l-diversity	Attribute disclosure	Data privacy Security	Medium	l-diversity does not consider semantic meanings of sensitive values
t-closeness	Attribute disclosure	Data privacy Security	Medium	Privacy is measured by the information gain of an observer
Information gain/loss metrics				
Leaked privacy value	Privacy leakage Exposure Proximal access Secondary use Aggregation	Data privacy Spatial privacy Trust	High	Information is accessible to the adversary. A high value indicates low privacy
Mutual information	Cross-contextual information Flow Privacy Leakage	Data privacy Spatial privacy	Medium	Mutual information shows the secrecy leakage
Relative entropy	Intrusion	Security	Medium	Used for the location to determine places users have visited
Privacy score	Exposure Aggregation Exclusion	Data privacy Security	Medium	Privacy score increases with the sensitivity of data and visibility
Positive information disclosure	Disclosure Power imbalance Breach of confidentiality	Data privacy Spatial privacy Trust	Medium	Exposure of information to other users or third parties
Adversary's success probability metrics				
Adversary's success rate	Surveillance Aggregation Physical threat	Data privacy Spatial privacy	High	Measurability of how successfully an adversary can estimate a user's identity or location

Table 10 (continued)

Privacy metrics	Privacy threat models	Protection Goals	Measurability	Comments
Degree of anonymity	Secondary use Identification	Data privacy Security	Low	Determine the anonymity set of a user

with the high uncertainty in the adversary's estimate. Most of the uncertainty metrics are built upon the information-theoretic concept such as entropy, min-entropy, etc. It is observed that privacy is strongly related to security, which is consequently dependent on entropy. Security improves when the entropy data increase and can be measured with entropy, conditional entropy, and min-entropy. Min-entropy provides the lowest security and privacy, and it is also known as the worst-case performance (Zhao and Wagner 2020). The error-based metrics, on the other hand, demonstrate how the high correctness of the adversary's estimate and small errors are related to low privacy. For example, as mentioned by Shokri et al. (2011), correctness is the metric, which quantifies the privacy of a user compared to certainty or accuracy. This metric evaluates the success of the attacker or determines how close the adversary's estimate is to the real value.

On the other side, data similarity metrics do not consider any adversary but the focus is on the properties of the observable or published data. The privacy level is derived from the structures of the disclosed data. The information gain/loss metrics pertain to the measurement of information loss or gain by the information gained by adversaries or the privacy lost by disclosure of information. From the analysis done, it is observed that security and privacy assessment are strongly dependent on the threat models, for example, privacy leakage can cause linkability and increases with decreasing secrecy performance where mutual information reveals the secrecy leakage. Hence, privacy leakage can be measured with mutual information and entropy loss. Mutual information measures the average leakage case whereas entropy loss measures leakage in a worst-case scenario. The metrics of the adversary's success probability depend on the adversary model and measure how success is attained. The adversary's success rate should also consider false-positive and false-negative rates in addition to cases where correct estimates are done. The false-positive cases relate to where an adversary identifies an incorrect user or location and the false-negative ones correspond to cases where the identification of a user or location is a failure. The adversary depends on surveillance and aggregation in addition to physical threats such as stalking to ensure a high success rate in identifying a user or his/her location.

Further to the evaluation, a mapping of the privacy threats with the protection goals is carried out as follows:

Table 11 helps determine which protection goals are needed to counteract the existing privacy threats. These privacy criteria help alleviate the harms associated with the privacy threats if not eliminate them. The threat models as presented in this study can be tackled by using one or more privacy criteria in a PBSN application.

PBSN frameworks assessment

Based on the recent advances in PBSN together with the outburst usage of smartphones, many platforms have been created to ease the development of such applications. This section outlines some of the popular and recent PBSN frameworks and emphasizes on the privacy and security provisions.

Table 11 Mapping of privacy threats to protection goals

Privacy Threats	Protection Goals				
	Data Privacy	Spatial Privacy	Unlinkability	Trust	Security
Proximal Access	☑	☑			
Surveillance		☑	☑	☑	
Snooping	☑				☑
Identification			☑		
Aggregation			☑		
Secondary Use				☑	
Exclusion				☑	
Cross-Contextual Information Flow	☑		☑		☑
Disclosure	☑	☑		☑	☑
Breach of Confidentiality				☑	
Exposure	☑	☑	☑		☑
Distortion			☑		
Privacy Leakage					☑
Intrusion					☑
Power Imbalance	☑	☑			
Physical Threat		☑			☑

FINE framework

FINE refers to a fine-grained privacy-preserving location-based service framework designed for mobile devices (Shao et al. 2014). It follows the data-as-a-service (DaaS) model and consists of three main parties: the provider, a cloud server, and the users. The provider outsources its data to the cloud server which acts as a third party, which subsequently executes the queries of the users. FINE achieves several privacy properties such as fine-grained access control, location privacy, confidentiality, and accurate query result by making use of a ciphertext-policy anonymous attribute-based encryption (CP-AABE) technique. However, the cloud server is known to be honest but curious in such a way that it can launch passive attacks to retrieve the maximum secret information available, for example, the location information of the mobile users. Additionally, even though the cloud server will not collude with the server provider, it can collude with malicious users to retrieve the location information of users and the data of the server provider.

PLAM framework

A privacy-preserving request aggregation protocol is applied in the PLAM framework to obtain k-anonymity and l-diversity (Lu et al. 2014). PLAM ensures identity privacy, secure past, and future location privacy and attack resistance. User preference privacy is achieved without the use of a trusted anonymizer server, and to protect the past and future locations of users, an unlinkable pseudo-ID technique is adopted by using changing pseudo-IDs for users at different locations. Additionally, the protocols of PLAM are secure against adversary attacks, hence, ensuring authentication, data integrity, and availability. The system model of the PLAM framework consists of users in a local area with a provider and a trusted authority. The latter, though is fully trusted in the system, is honest but curious and can snoop into the user's privacy preference to retrieve some side information. The users are also known to be privacy curious in such a way that they can disclose the privacy of other users from available information. Moreover, a user's pseudo-ID can be correlated to his/her real identity by strong adversaries if some side information at a specific location is available.

TTP-FREE privacy framework

The TTP-free privacy framework protects both user's identity and location without the use of a trusted third party by making use of a strong cryptography mechanism (Al-Badawy et al. 2018). Fake identities are generated on the users' mobile phones to ensure identity protection. A key agreement protocol is applied to ensure secure channels for communications between the users. Only authorized users can use the system with an authentication process. The locations of the users and the secure communication channel are encrypted using elliptic curve cryptography. However, server operators can be attackers and ultimately reveal the locations of users, their identities, and the mapping of the user's pseudo-ID to their real names.

SOCIOTAL EU framework

The SOCIOTAL EU framework is a privacy-preserving securing framework based on the Architecture Reference Model (ARM) for IoT systems ensuring content generation, publishing, and data sharing in a reliable, secure, and private manner (Bernabe et al. 2014). It consists of different security components such as authentication, authorization, identity management, group manager, and trust and reputation. The privacy-preserving identity management ensures anonymity, data minimization, and unlinkability. The access control component employs XACML to make authorization decisions based on access control policies that can specify which actions a user or group of users is/are allowed to perform over a specific resource under certain conditions. The group manager uses an attribute-based encryption mechanism (CP-ABE) and allows sharing information securely and privately such that only specific users satisfying particular identity attributes can decrypt the data.

APPLET framework

APPLET is a secured framework for location-based recommender systems by protecting user privacy information (Ma et al. 2017). In addition to locations, recommendation results are also protected since leakage of user privacy can be leaked while generating recommendations. The system model of APPLET refers to a Service Provider (SP) of which role is to own attributes and collect historical ratings, a Cloud Platform (CP) who is responsible for storage and computation, a Trusted Authority (TA) which generates private keys and the Recommendation Users (RUs). Figure 5 illustrates the APPLET framework. The Pailler homomorphic encryption is used when the similarities of the venues are computed by SP, and the encrypted ratings and attributes are sent to the CP in a ciphertext. Other cryptography methodologies are used such as comparable encryption to protect the users' locations during a recommendation. In this process, the locations of venues are compared with the users' requesting areas in the ciphertext. Using comparable encryption, the venues found in the users' areas can be filtered, hence, not revealing the locations of the users. In addition, commutative encryption is used to protect the leakage of venue attributes namely the names of the venues and their corresponding locations from SP during the response of the CP to a user's recommendation result. A security analysis is carried out in the study proving that user information is kept private during the recommendation process including the historical ratings and similarities of venues, and no information is leaked.

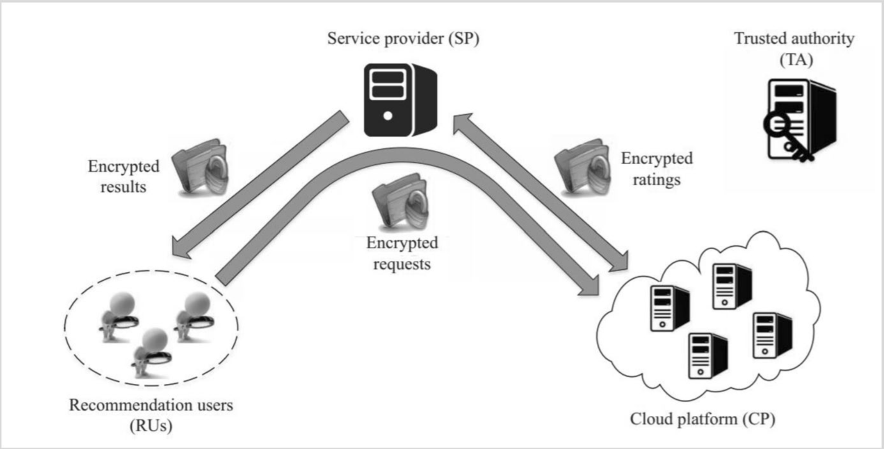

Fig. 5 APPLET framework

A privacy-preserving framework for outsourcing location-based services to the cloud

Zhu et al. (2019) proposed a privacy-preserving framework for outsourcing Location-Based Services (LBS) to the cloud with multi-location queries and per-query privacy limits. In this solution, a query scheme is proposed where user can specify their locations of interest with a minimum privacy degree. For each location, the cloud service returns an area containing the location where the latter cannot be inferred. In addition, the cloud service can perform a search while protecting the privacy of user queries and identities. The search by location attributes and locations is carried out by using an auxiliary index structure over encrypted data. A hierarchical index reflecting the geographical hierarchical locations is built where each node in the index is replaced by a Bloom filter. Furthermore, to protect the searched data and pattern of the Bloom filter, function-hiding inner product encryption (FHIPE) is employed to encrypt the Bloom filter. The number of matching bits is calculated to search by location or location attributes, and the query vector is matched with the index vector by the cloud service by comparing the number of matching bits for locations and attributes. In addition, a fine-grained access control scheme is integrated with the framework which uses blind signatures to prevent the service provider from learning any information in the query during the authentication process. A key policy attribute-based encryption (KPABE) is used to encrypt data records in the database. The authors confirmed that data (locations and user identities) are kept confidential from the cloud and no leakage of information is present when the cloud performs location queries and searches.

Evaluation of PBSN frameworks with the PISA model

An evaluation of the PBSN frameworks discussed in the above section is carried out using the PISA model by taking into consideration the existing privacy threats of the frameworks and the protection goals that each framework provides. Based on this information, the frameworks are assessed with respect to the privacy metrics associated as illustrated in Table 12.

The protection goals Data Privacy, Spatial Privacy, Unlinkability, Trust, and Security are abbreviated to DP, SP, U, T, and S, respectively, in the table for easier understanding.

Discussions

Based on the above evaluation of the PBSN frameworks, it is observed that at least three protection goals are met for each framework, e.g., the FINE framework ensures Data Privacy, Spatial Privacy, and Security while the TTP-FREE framework guarantees Data Privacy, Spatial Privacy, Unlinkability, and Security based on the privacy requirements that are identified in the frameworks.

Table 12 Evaluation of PBSN frameworks with the PISA model

	PBSN frameworks	Privacy threats	Protection goals					Privacy requirements	Privacy metrics				
			DP	SP	U	T	S		Uncertainty	Data similarity	Information (Gain/Loss)	Adversary's success probability	Error
1	FINE Shao et al. (2014)	Intrusion Proximal Access Physical Threats Cross-Contextual Information Flow	✓	✓			✓	Fine-grained access control Confidentiality Location protection	Location entropy	k-anonymity	Leaked privacy value Mutual information	Adversary's success rate	Adversary's estimated error
2	PLAM Lu et al. (2014)	Aggregation Power Imbalance Intrusion Disclosure	✓	✓	✓		✓	Anonymity Authentication Data integrity Availability Identity privacy Resilience to attacks	Location entropy Degree of unlinkability Asymmetric entropy	k-anonymity l-diversity t-closeness	Mutual information Relative entropy	Adversary's success rate	
3	TTP-FREE Al-Badawy et al (2018)	Identification Proximal Access Disclosure Exclusion Breach of confidentiality	✓	✓	✓		✓	Identity protection Location protection Authorization Authentication Secure Communication	Entropy Location entropy	k-anonymity	Information disclosure	Adversary's success rate	

Table 12 (continued)

	PBSN frameworks	Privacy threats	Protection goals					Privacy requirements	Privacy metrics				
			DP	SP	U	T	S		Uncertainty	Data similarity	Information (Gain/Loss)	Adversary's success probability	Error
4	SOCIOTAL EU Bernabe et al. (2014)	Identification Disclosure	✓		✓	✓	✓	Anonymity Data minimization Unlinkability Authentication Authorization Access control Integrity Secure data sharing Identity management Contextual Management Trust management Reputation	Entropy Degree of unlinkability	l-diversity	Information disclosure		
5	APPLET Ma et al. (2017)	Disclosure Breach of confidentiality Invasion Surveillance Secondary Use	✓	✓				Identity protection Location PROTECTION	Location entropy		Leaked privacy value		Adversary's estimated error

Table 12 (continued)

	PBSN frameworks	Privacy threats	Protection goals					Privacy requirements	Privacy metrics				
			DP	SP	U	T	S		Uncertainty	Data similarity	Information (Gain/Loss)	Adversary’s success probability	Error
6	Zhu et al. (2019)	Surveillance Aggregation Power Imbalance Privacy Leakage	✓	✓			✓	Fine-grained access control Confidentiality Query protection Secure data Searching	Location entropy		Leaked privacy value	Adversary’s success rate	Adversary’s estimated error

However, most of them are still prone to several privacy threats and some of the frameworks comprise trusted authorities, which are honest but curious. The PISA model is, hence, used to evaluate the frameworks based on their protection goals and privacy threats based on which the privacy metrics of each framework are deduced.

Initially, to start the evaluation of privacy-preserving PBSN frameworks, the privacy solutions as presented by the respective authors are analyzed, from which the privacy requirements are outlined and subsequently the protection goals of the PBSN frameworks are deduced based on Fig. 2. The threat attacks, information leakage, or knowledge of the adversary also are considered in the different frameworks, and these shortcomings in terms of privacy are explored and they are associated with the privacy threat models as presented in Fig. 3. Based on the protection goals and privacy threat models gathered as the evaluation criteria, the assessment of the PBSN frameworks can start by taking into consideration the related privacy metrics as illustrated in Table 10.

FINE, as depicted in Table 12, is subjected to the privacy threat Intrusion, among others, where the cloud server launches attacks to retrieve information. Even though Shao et al. (2014) claim that any attack is stopped at the very beginning, no further details are obtained on how they are prevented (). The privacy metric adversary's success rate is the correct measure to validate this statement. For instance, to confirm if the adversary, in this case, the cloud server is not successful in trying to find any information, the rate value will be zero. If the value is no other than zero, it means that some attacks were attempted. The success rate of the Location-based Service (LBS) provider determines how FINE is protected by any information collection privacy threat such as surveillance and evaluates the success of the LBS provider when trying to retrieve information from the communication between the cloud server and the users. On the other side, mutual information is an important metric to assess how much information the LBS provider retrieves from the communication by validating the adversary's estimate and the true value. In addition, the cloud server colludes with malicious users to obtain some information. However, the authors insist that even if it colludes with malicious users, only the basic information such as if a ciphertext can be decrypted or not will be available. The metric-leaked privacy value further evaluates this breach of confidentiality to check how much information is being disclosed. To have a complete privacy assessment of FINE, the use of the location entropy metric is important to ensure that privacy is protected even if some attempts of attacks are done by the cloud server and LBS provider. The privacy metric refers to the additional information the adversary needs to identify the location of a user or find his/her position.

The metric degree of unlinkability is the main privacy metric to assess the unlinkable pseudo-ID technique in the PLAM framework. It is helpful to estimate if the pseudo-id can be correlated to the real identity of a user if any side information is present. Additionally, asymmetric entropy measures the uncertainty of the adversary to associate the pseudonyms with his/her true identity. PLAM also uses a trusted authority that is honest but curious and tries to retrieve user information by surveillance. Relative entropy and adversary's success rate are the two privacy metrics that are used to evaluate the distribution of the adversary's estimate and the true value.

The TTP-Free privacy framework provides complete privacy protection, that is, identity and location protection in the absence of a trusted third party. To evaluate the identity protection of the TTP-Free privacy framework, entropy is useful to detect the remaining information that an adversary needs to identify a user or find any other attributes related to the user. Similarly, location entropy is used to assess the location protection ensured by the framework through the cryptographic mechanism used. Entropy is calculated at different points in time to find out the position of the user. If users are located very close to each other, the exact positions of the users can be exposed even if they are high entropy locations. However, though it is a TTP-Free framework, the social server and location server are assumed to be dishonest and will try to retrieve user information. The TTP-Free framework is also susceptible to privacy threats such as disclosure, exclusion, and breach of confidentiality since server operators can act as attackers and reveal user information. The positive information disclosure value provides an estimate of the breach of confidentiality in different scenarios such as prior knowledge of adversary, relative security, etc.

Even though the SOCIOTAL EU project framework provides privacy protection, security, and trust, it is noted that a minimum amount of information can be disclosed in the Identity Management process. K-anonymity and positive information disclosure refer to important privacy metrics for this framework to evaluate how users are being identified or how other private information can be deduced. The degree of unlinkability is equally important in this assessment to measure the unlinkability provided by the framework and l-diversity to measure the minimal disclosure of attributes.

Nevertheless, though it is mentioned that no privacy leakage happens during a recommendation in the APPLET framework, the service provider and cloud provider are curious about the recommendation results and the provider will try to know the service provider's historical ratings and similarities. This privacy leakage is measured with mutual information and entropy loss, and the results obtained will highlight the degree of privacy leakage of the APPLET framework. Additionally, the leaked privacy value further confirms this privacy leakage. Moreover, even though there is an invasion of adversaries when they try to eavesdrop on all data transmission between the cloud provider, service provider, and the users, the authors claimed that adversaries should not learn anything about the data. The adversary's estimated error metric demonstrates the incorrectness of the adversary and confirms the fact that adversaries do not retain any information.

Zhu et al. (2019) ensured protection goals such as data privacy by protecting the privacy of user queries and identities, spatial privacy by ensuring that private locations are kept secured with the use of FHIPE and minimum privacy degree and security by providing fine-grained access control and confidentiality. Location entropy measures the protection of the private locations and calculates the uncertainty to determine the real location of a user from other proximate users. The framework is prone to privacy threats such as surveillance, aggregation, and power imbalance since the cloud server and LBS provider are assumed to be honest but curious and will attempt to infer information. Additionally, the framework provides a leakage function that ensures complete preservation of data privacy preventing any adversary to gain information about the users since to have access to any user details, he must be able to break one of the FHIPE algorithms, the blind signature mechanism and the database encryption algorithm. The metrics leaked privacy value and adversary's estimated error to measure the leakage of information and the incorrectness of the adversary to estimate any details about the user.

The values obtained from the privacy metrics determine the level of privacy provided by the frameworks, and hence, the protection features can be further improved based on the results of the evaluation.

Table 13 gives an overview of the security implications associated with each of the most used location privacy-preserving techniques. It is observed that these techniques do not protect users' data fully and different attempts to collect data or manipulate available data are possible. Adversaries can also eavesdrop on all traffic and ultimately deduce information on the users. It should be noted that many privacy-preserving solutions adopt two or more of these techniques to provide better privacy to the users.

Table 13 Security implications of location privacy-preserving techniques

Privacy Threats	Location Privacy-Preserving Techniques						
	K-Anonymity	Obfuscation	Cryptography	Spatial Cloaking	Pseudonyms	Mix Zones	Dummy Locations
Proximal Access	☑			☑			☑
Surveillance	☑	☑	☑		☑		
Snooping	☑	☑	☑		☑		☑
Identification		☑	☑	☑	☑	☑	☑
Aggregation		☑	☑		☑	☑	☑
Secondary Use		☑	☑		☑		☑
Exclusion							☑
Cross-Contextual Information Flow			☑		☑		☑
Disclosure	☑						
Breach of Confidentiality	☑						
Exposure	☑						
Distortion	☑						
Privacy Leakage	☑		☑			☑	
Intrusion		☑				☑	☑
Power Imbalance		☑			☑	☑	☑
Physical Threat		☑			☑		

Contributions of PISA

As discussed above, the PISA model allows a rigorous analysis of the different privacy and security provisions in PBSN frameworks. It facilitates the evaluation of PBSN frameworks in terms of privacy by following the below approach:

The privacy and security requirements of the PBSN framework are analyzed thoroughly by taking into consideration the privacy techniques used, the privacy protection methods, and the architecture of the framework.

Based on the analysis of privacy and security requirements, the potential protection goals of the PBSN framework are identified based on the data in Fig. 2.

The PBSN framework is further analyzed in terms of the privacy loopholes and the existing threat models are pointed out by identifying the privacy threats that may exist in the PBSN framework though privacy-preserving techniques are implemented.

Additionally, based on the perceived threat models, the resources or information that may be available to any adversary are detected. The prospective knowledge of the adversary is also considered.

Based on the information gathered such as the protection goals and the threat models, the privacy metrics of the framework are derived based on the PISA model as illustrated in Table 10.

Once the privacy metrics of the PBSN framework are obtained, the analysis and evaluation of the framework can be carried out. The evaluation metrics help quantify the protection goals. These metrics can be used to evaluate the different privacy algorithms or techniques used in the framework.

Each privacy metric defined provides a different level of assessment and evaluation, for instance, entropy metrics indicate the information that a variable may contain, e.g., location entropy measures the uncertainty that an adversary can disclose the position of a user. Similarly, min-entropy and conditional entropy can be used in the security assessment of cryptographic algorithms where min-entropy measures the irreversibility and conditional entropy measures the number of attempts needed to retrieve the target data. On the other hand, error metrics such as expected distance error measures how accurately an adversary can estimate a user's position while information gain/loss metrics such as leaked privacy value outline the amount of knowledge an adversary can learn.

By making use of the different privacy metrics, different types of assessment can be done for each framework to unveil the privacy and security aspects of the framework.

The PISA model can be useful to privacy-preserving algorithm designers so that different privacy aspects can be considered in advance. This allows a defensive perspective during the development of the algorithms and allows any improvement to the algorithms to avoid any flaws or loopholes. Additionally, this model can be used as an indispensable tool to endorse or popularize any new privacy-preserving algorithms in PBSN systems by conducting an exhaustive analysis of the privacy and security provisions.

Future works and conclusion

In this paper, a privacy assessment framework called PISA is proposed to evaluate privacy-preserving PBSN frameworks and systems. It provides a thorough analysis of the privacy and security goals in PBSN systems by taking into consideration the possible location-related threats to privacy-preserving systems. A comprehensive evaluation of privacy and security requirements for location-based systems is firstly done, based on which, five protection goals of PBSN systems are proposed: data privacy, spatial privacy, unlinkability, trust, and security. A series of location privacy threats are investigated and classified to identify the resources and information available to adversaries. Privacy metrics associated with PBSN systems are defined and used to quantify the protection goals presented. The PISA framework allows the assessment and comparison of the different privacy features of PBSN frameworks based on several evaluation criteria. The PISA framework was used in this study to evaluate six recent PBSN frameworks in terms of their privacy and security requirements, protection goals, threat models, and privacy metrics. The results validate that the PISA framework ensures an extensive analysis, evaluation, and comparison of different privacy-preserving solutions. Future works of the current research include extending the framework to consider different adversary models based on their assumptions, goals, and capabilities and investigating other threat models involving locations. Additional privacy metrics can be considered to provide a more extensive evaluation. The measurability ratings of the assessment can be improved by providing appropriate weight scoring for different evaluation metrics. To obtain better results on the assessment of privacy-preserving solutions, the proposed PISA model should extend the empirical evaluation on a large scale on other PBSN systems and privacy-preserving algorithms. Different methods of privacy evaluation can be considered apart from analyzing privacy requirements such as analyzing privacy policies or adopting a use-case modeling method to assess the privacy and security criteria.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Al-Badawy, A.M., H.M. Abbas, and M. Belal. 2018. A TTP-Free Location Privacy Framework for Mobile Social Networks with Key Agreement Protocol. *International Journal of Applied Engineering Research* 13 (14): 11540–11547.

Al-Dhubhani, R.S., Cazalas, J., Mehmood, R., Katib, I. and Saeed, F. 2019. A Framework for Preserving Location Privacy for Continuous Queries. In: International Conference of Reliable Information and Communication Technology, Johor, Malaysia, pp. 819–832. Springer, Cham, 22–23 September 2019.

Amar, Y., Haddadi, H. and Mortier, R. 2018. An Information-Theoretic Approach to Time-Series Data Privacy. In: Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems, Porto Portugal, pp. 1–6. EuroSys, 23–26 April 2018.

Arseni, S.C., Halunga, S., Fratu, O., Vulpe, A. and Suciu, G. 2015. Analysis of The Security Solutions Implemented In Current Internet of Things Platforms. In: 2015 Conference Grid, Cloud & High-Performance Computing in Science (ROLCG), Cluj-Napoca, Romania, pp. 1–4. IEEE, 28–30 October 2015.

Babar, S., Mahalle, P., Stango, A., Prasad, N. and Prasad, R. 2010 Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Third International Conference on Recent Trends in Network Security and Applications, Chennai, India, pp. 420–429. Springer, 23–25 July.

Bernabe, J.B., Hernández, J.L., Moreno, M.V. and Gomez, A.F.S. 2014. Privacy-Preserving Security Framework for a Social-Aware Internet of Things. In: International conference on Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services, Belfast, United Kingdom, pp. 408–415. Springer, Cham, 2–5 December 2014.

Buchanan, W.J., Z. Kwecka, and E. Ekonomou. 2013. A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services. *Mobile Networks and Applications* 18 (5): 728–737.

Chamarajnagar, R. and Ashok, A. 2019. Privacy Invasion through Smarthome IoT Sensing. In: 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, pp. 1–9. IEEE, 10–13 June 2019.

Do, Q., B. Martini, and K.K.R. Choo. 2019. The Role of the Adversary Model in Applied Security Research. *Computers & Security* 81: 156–181.

Jiang, H., J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar. 2021. Location Privacy-Preserving Mechanisms in Location-Based Services: A Comprehensive Survey. *ACM Computing Surveys (CSUR)* 54 (1): 1–36.

Kim, T., I.R. Chen, Y. Lin, A.Y.Y. Wang, J.Y.H. Yang, and P. Yang. 2019. Impact of Similarity Metrics on Single-Cell RNA-Seq Data Clustering. *Briefings in Bioinformatics* 20 (6): 2316–2326.

Kong, L., Z. Liu, and Y. Huang. 2014. Spot: Locating Social Media Users Based on Social Network Context. *Proceedings of the VLDB Endowment* 7 (13): 1681–1684.

Lee, C., Y. Guo, and L. Yin. 2013. A Framework of Evaluation Location Privacy in Mobile Network. *Procedia Computer Science* 17: 879–887.

Li, H., H. Zhu, S. Du, X. Liang, and X. Shen. 2016. Privacy Leakage of Location Sharing In Mobile Social Networks: Attacks and Defense. *IEEE Transactions on Dependable and Secure Computing* 15 (4): 646–660.

Li, M., Cao, N., Yu, S. and Lou, W. 2011. Findu: Privacy-Preserving Personal Profile Matching In Mobile Social Networks. In: 2011 Proceedings IEEE INFOCOM, Shanghai, China, pp. 2435–2443. IEEE. 10–15 April 2011.

Lilien, L., and B. Bhargava. 2006. A Scheme for Privacy-Preserving Data Dissemination. *IEEE Transactions on Systems, Man, and Cybernetics-Part A* 36 (3): 503–506.

Liu, L. 2009. Privacy and Location Anonymization in Location-Based Services. *SIGSPATIAL Special* 1 (2): 15–22.

Lu, R., Lin, X., Shi, Z. and Shao, J. 2014. PLAM: A Privacy-Preserving Framework for Local-Area Mobile Social Networks. In: INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, pp. 763–771. IEEE, 27 April-2 May 2014.

Ma, X., H. Li, J. Ma, Q. Jiang, S. Gao, N. Xi, and D. Lu. 2017. APPLET: A Privacy-Preserving Framework for Location-Aware Recommender System. *Science China Information Sciences* 60 (9): 1–16.

Mamonov, S., and R. Benbunan-Fich. 2018. The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors. *Computers in Human Behavior* 83 (3): 32–44.

Pew Research Center. 2018. Teens, Social Media & Technology Overview 2015. Available at: http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ Accessed 30 Aug. 2021.

Puttaswamy, K.P. and Zhao, B.Y. 2010. Preserving Privacy in Location-Based Mobile Social Applications. In: Proceedings of the 11th Workshop on Mobile Computing Systems & Applications, Annapolis, MD, USA, pp. 1–6. ACM, February 2010.

Raschke, R.L., A.S. Krishen, and P. Kachroo. 2014. Understanding the Components of Information Privacy Threats for Location-Based Services. *Journal of Information Systems* 28 (1): 227–242.

Ravi, L., V. Subramaniyaswamy, M. Devarajan, K.S. Ravichandran, S. Arunkumar, V. Indragandhi, and V. Vijayakumar. 2019. SECRECSY: A Secure Framework for Enhanced Privacy-Preserving Location Recommendations in Cloud Environment. *Wireless Personal Communications* 108 (3): 1869–1907.

Shao, J., Lu, R. and Lin, X. 2014. FINE: A Fine-Grained Privacy-Preserving Location-Based Service Framework for Mobile Devices. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, pp. 244–252. IEEE, 27 April-2 May 2014.

Shokri, R., Theodorakopoulos, G., Le Boudec, J.Y. and Hubaux, J.P. 2011 Quantifying location privacy. In: 2011 IEEE symposium on security and privacy, Berkeley, CA, USA, pp. 247–262. IEEE, 22–25 May 2011.

Shokri, R., Troncoso, C., Diaz, C., Freudiger, J. and Hubaux, J.P. 2010. Unraveling an Old Cloak: K-Anonymity for Location Privacy. In: Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, Chicago Illinois USA, pp. 115–118. CCS, 4 October 2010.

Solove, D.J. 2005. A Taxonomy of Privacy. *The University of Pennsylvania Law Review* 154 (3): 447–564.

Song, D., J. Sim, K. Park, and M. Song. 2015. A privacy-preserving continuous location monitoring system for location-based services. *International Journal of Distributed Sensor Networks* 11: 8.

Sun, G., D. Liao, H. Li, H. Yu, and V. Chang. 2016. L2P2: A location-label based approach for privacy preserving in LBS. *Future Generation Computer Systems* 74: 375–384.

Sun, R. and Xue, M. 2020. Quality Assessment of Online Automated Privacy Policy Generators: An Empirical Study. In Proceedings of the Evaluation and Assessment in Software Engineering, Trondheim, Norway, pp. 270–275. ICPS Proceedings, 15–17 April 2020.

Thomas, K., Bandara, A.K., Price, B.A. and Nuseibeh, B. 2014. Distilling Privacy Requirements for Mobile Applications. In: Proceedings of the 36th international conference on software engineering, Hyderabad, India, pp. 871–882. ICSE, 31 May 2014- 7 June 2014.

Thuiller, W., M. Guéguen, J. Renaud, D.N. Karger, and N.E. Zimmermann. 2019. Uncertainty in Ensembles of Global Biodiversity Scenarios. *Nature Communications* 10 (1): 1–9.

Vu, K., Zheng, R. and Gao, J. 2012. Efficient algorithms for k-anonymous location privacy in participatory sensing. In: 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, pp. 2399–2407. IEEE, 25–30 March 2012.

Wagner, I. 2015. Genomic Privacy Metrics: A systematic Comparison. In: 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, pp. 50–59. IEEE, 21–22 May 2015.

Wagner, I., and D. Eckhoff. 2018. Technical Privacy Metrics: A Systematic Survey. *ACM Computing Surveys (CSUR)* 51 (3): 1–38.

Werner, M. 2016. Privacy-Protected Communication for Location-Based Services. *Security and Communication Networks* 9 (2): 130–138.

Xue, M., Y. Liu, K.W. Ross, and H. Qian. 2016. Thwarting Location Privacy Protection in Location-Based Social Discovery Services. *Security and Communication Networks* 9 (11): 1496–1508.

Yang, D., Zhang, D., Qu, B. and Cudré-Mauroux, P. 2016. PrivCheck: privacy-preserving check-in data publishing for personalized location based services. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, New York, USA, pp. 545–556. ACM, September 2016.

Zhao, Y., and I. Wagner. 2020. Using Metrics Suites to Improve the Measurement of Privacy in Graphs. *IEEE Transactions on Dependable and Secure Computing* 19 (1): 259–274.

Zhou, X. 2011. Privacy and Security Assessment of Biometric Template Protection. Doctoral dissertation, Technische Universitt Darmstadt, Germany.

Zhu, X., E. Ayday, and R. Vitenberg. 2019. A Privacy-Preserving Framework for Outsourcing Location-Based Services to The Cloud. *IEEE Transactions on Dependable and Secure Computing* 18 (1): 384–399.

Zhu, Z., Cao, G. 2011. Applaus: A Privacy-Preserving Location Proof Updating System for Location-Based Services. In: 2011 Proceedings IEEE INFOCOM, Shanghai, China, pp. 1889–1897. IEEE, 10–15 April 2011.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.