Social Network Analysis and Mining (2018) 8:41
https://doi.org/10.1007/s13278-018-0518-x

REVIEW ARTICLE

An investigation into the requirements of privacy in social networks and factors contributing to users' concerns about violation of their privacy

Razieh Malekhosseini[1] · Mehdi Hosseinzadeh[2,3] · Keyvan Navi[4,5]

Received: 2 June 2017 / Accepted: 30 May 2018

Abstract

Social networks are specific types of social media which consolidate the ability of omnipresent connection for users and devices to share user-centric data objects among interested users. Taking advantage of the characteristics of both mobile social networks (MSNs) and online social networks (OSNs), MSNs are capable of providing an efficient and effective mobile environment for users to access, distribute, and share data. OSNs provide capability of search, data sharing, and online social interactions for users through Internet sites. However, the lack of a protective infrastructure in these networks has turned them into convenient targets for various risks. This is the main purpose why social networks including MSNs and OSNs carry disparate and intricate safety concerns specially privacy-preserving challenges and what has been done to improve these challenges. In addition, what types of data should be protected and what are the different architectures provided for each of these networks? In this paper, we aim to provide a clear categorization on privacy challenges and a deep exploration over some recent solutions in MSNs and OSNs. In particular, in MSNs, proposed scheme to protect data types is categorized, and in OSNs, all types of proposed architectures, along with the proposed mechanisms for privacy, are classified. To conclude, several major open research issues are discussed, and future research directions are outlined.

Keywords Social networks · Mobile social networks (MSNs) · Online social networks (OSNs) · Privacy challenges · Privacy violation

1 Introduction

The sites of social networks have witnessed a significant growth in recent years in terms of the number of users and popularity (Statista 2016). The term 'social networks' was first used in 1954 and a social network was first defined as a gathering of people in certain groups of 100–150 into a community (Barnes 1954). Depending on the type of platform that is used to provide social communication services, social networks can be divided into two categories: Mobile and Online. An online social network (OSN) is a social network on the Internet and refers to a website that is related to online communities with Internet users. The main purpose of OSNs is to simulate social interactions in people's lives (Ho et al. 2008). Hence, social networks sites allow users to share favorite objects and activities with others. In terms of service type, OSNs can be divided into two categories: centralized and decentralized architectures (Boyd and Ellison 2007). In a centralized architecture, the privacy requirements are borne by a component or a limited number

✉ Mehdi Hosseinzadeh
Hosseinzadeh.m@Iums.ac.ir

Razieh Malekhosseini
malekhoseini@srbiau.ac.ir

Keyvan Navi
navi@sbu.ac.ir

[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Iran University of Medical Sciences, Tehran, Iran

[3] Computer Science, University of Human Development, Sulaimaniyah, Iraq

[4] Nanotechnology and Quantum Computing Lab, Shahid Beheshti University, G.C., Tehran, Iran

[5] School of Computer Science, Institute for Research in fundamental science (IPM), Tehran, Iran

Published online: 11 June 2018

of components, rather than by social networks users. In contrast, in a decentralized architecture, the responsibility of meeting users' privacy requirements lies with the users, and the need to trust a central administrator is eliminated.

Mobile social networks (MSNs) represent special types of social media that provide connectivity anywhere for users/devices to share user-centric data objects among interested users. In terms of service type, there is unanimous agreement among researchers in the field that there are basically two types of MSNs: centralized and decentralized (Kayastha et al. 2011; Vastardis and Yang 2013). In both of them, mobile devices receive the data. Centralized MSNs make use of social networks services, whereas decentralized MSNs make use of wireless technologies, such as Bluetooth and Wi-Fi.

The increased attention that has been paid by users to social networks has changed the mode of communication between users. In addition to the facilities that social networks provide for users, they create some safety, security, and privacy challenges (Najaflou et al. 2013). The violation of user privacy due to the disclosure of user information by unauthorized data access or information inference is one of these challenges. This is especially important in the case of personal data that contains sensitive information about users (Li et al. 2011). The level of concern of a user about the disclosure of information depends on the importance of the data from the user's point of view, which varies from user to user. Different associations have provided different definitions for personal data and the risks of their breach (European Council 1995; European Commission 2012a, b).

In the data protection directive 95/46/EC of the European Union (EU), personal data are defined as any information relating to an identified or (directly and/or indirectly) identifiable natural person (European Council 1995). The personal data which might pose a risk to the privacy of private life and family life are composed of the information about individuals' race, political view, philosophical belief, religion, and sect or other beliefs, foundation, association and union membership, health, private life, and conviction (European Commission 2012a). Among the primary data concerning user privacy are telephone number, identity records, address information, e-mail address, photos, identity number, institutional or student number, education background, online user accounts, posts on social networks sites, banking information, and health records (European Commission 2012b). IP address, genetic information, biometric information, location information, online identity, and cookies taken from the visited Internet sites are other important data that reveal cultural and social identity.

Lack of adequate data protection and violation of user privacy is a cause for concern, and sometimes reluctance, in using social networks (Xu et al. 2013). Therefore, efforts to protect user privacy can have important impacts on the popularity and growing use of social networks. Because users need privacy on social networks, social networks are obligated to provide privacy services. Indeed, in addition to providing social networks services and access to data, they must also provide basic privacy services (Schneier 1996).

1.1 Social network services

A social network is a great source of personal information (Boyd and Ellison 2007). A user's name, photo, date of birth, contact details, marital status, religious–political views, interests, hobbies, and school records are some of the information that could directly or indirectly be obtained from social networks sites. The importance of this information is such that according to some reports from Microsoft, 75% of companies use social networks sites to obtain information about job candidates in their companies (Google plus 2017).

The vast amount of information on social networks is created by communicating between users and sharing information. A social network, in addition to social services (aimed at creating social interactions among users in cyberspace), should also provide privacy requirements of users. In this paper, response to the privacy requirements of users is in the form of providing a privacy service.

1.1.1 Privacy services

Sharing various types of information on social networks without full management over their privacy has resulted in the violation of user privacy. Regarding the use of social networks, people who are sensitive to the protection of their privacy initially refuse to become members of social networks; however, in practice, since most of their friends are interacting with each other in this environment, they are encouraged to use these networks (Chang et al. 2011).

Usually, the information that is shared will remain permanently on social networks servers. In some cases, if a user deletes the data from his or her page on the social network, or removes or deactivates his or her account, they will remain on the social networks servers for a long time. Therefore, social network providers have unlimited access to information that was shared by users. In other words, they have full control over user information (De Cristofaro et al. 2012). Property rights of data are another area that may cause a violation of privacy. Once users are registered on a social network, they agree implicitly to allow providers to store, display, or/and use their information. In other words, according to this agreement, ownership of user data is transferred to the provider of the social network. Thus, providers obtain all necessary rights to use and distribute users' data (Facebook statement 2017; Facebook Privacy 2017; Google Privacy 2017; Luo and Lee 2009). Using property rights of data, social network providers provide users' personal data for marketing purposes. In this case, social network providers claim that the data are distributed in an anonymous format; however, given the effectiveness of Deanonymization algorithms, this claim is baseless (Luo et al. 2009; Ding et al. 2010). In some cases, if users delete data on their pages on the social network or remove/disable their accounts, their information remains on backup servers of social networks (Facebook statement 2017; Facebook Privacy 2017; Google Privacy 2017; Luo and Lee 2009). Agreement concerns, in addition to the inability to add or delete provisions, the possibility that the provider will change the terms of the agreement after registration, and the lack of user notification, have led to challenges of OSNs.

Due to privacy issues and privacy rights, when designing and developing a social network, privacy services must be provided in addition to social networks services. The privacy service required by users on a social network must provide confidentiality, which access control and fairness (Schneier 1996).

Confidentiality: In a social network which ensures that the social network provider and non-friends cannot access user data. Considering that a user needs to create different groups based on his social relationships with his friends, the confidentiality of both the shared data and the user's social relationships with friends (against the service provider and non-friends) is necessary (Defrawy et al. 2009).

Access control: On a social network, only the user who owns the data can have access control over shared data and he specifies his data audience. In general, the access control provided to a social network user should have three levels: fine-grained, flexible, and dynamic (Krishnamurithy and Wills 2008).

Fine-grained access control: The quality of the social communication of a user with each friend is not the same, nor is the sensitivity of disclosing each item of information to each friend. Therefore, the user should be able to determine to what data each of his or her friends have access (Krishnamurithy and Wills 2008; Xiaohui et al. 2011). With fine-grained access controls, multiple sets of the user's friend are allowed to access shared data, and for any item of shared data, the level of access can be defined independently of other access policies. The user can group his friends in such a way that each friend belongs only to a single group (single membership); however, it is desirable to be able to add a friend to more than one group (multiple membership).

Flexible access control: There are many ways in which the user can combine his defined groups to define the intended audience. In other words, it is desirable for the user to be able to specify a fully flexible policy for accessing his or her shared information, so that a new policy can be defined by combining different relationships and friend IDs (Krishnamurithy and Wills 2008).

Dynamic access control: The social relationship between a user and his friends is time-dependent. This means that the user, at any time, may remove a friend from a social group or add a friend to another group. He may also revoke all defined communications with a friend. In a social network, it is desirable for the user to have the ability to add, remove, and cancel friends and social relationships at any time (Krishnamurithy and Wills 2008).

Fairness: The concept of fairness is another fundamental issue in privacy which generally focuses on encouraging users to collaborate in a network. Fairness is related to privacy, since unfair communication between nodes makes heavy congestion in a particular collaborative node. This node can be a potentially dangerous point for malicious nodes for intruding into the network and gaining an unauthorized access to valuable resources (users shared data). In addition, users' interests and identification information are considered valuable resources in MSNs. The direct revelation of identity information to unauthorized users in an unfair situation is inconvenient. The definition of the social fairness comes from this concept (Dramitinos et al. 2009; Mtibaa and Harras 2011).

To date, very few attempts have been made at classifying user privacy challenges for the two categories of social networks: mobile and online social networks. One such study was carried out by Beach et al. (2009), in which privacy and security issues were investigated in MSNs, along with methods for improving their implementation. They divided the challenges into three groups: anonymity issues, indirect or *k*-anonymity issues, and attacks (eavesdropping, spoofing, replay, and wormhole). In addition, they expanded their scheme by designing an identity server (IS) that adopts established privacy and security technologies to provide solutions for such problems (Beach et al. 2009).

Najaflou et al. (2013) conducted research in the field of safety challenges and their solutions in MSNs. They offered a clear classification of the safety challenges and called for in-depth research of some recently proposed solutions in MSNs. In their research, given the similarities of MSNs with opportunistic and fault-tolerant networks, their investigation ranged from safety challenges and their solutions, namely, technical opportunistic networks (OPPNets) and delay-tolerant networks (DTNs), to mobile networks in the areas of security, privacy, and trust.

Although the studies discussed above are significant in that they provide a classification of privacy challenges of users (Beach et al. 2009; Najaflou et al. 2013), the privacy requirements from the users' point of view are not fully covered and they have not paid attention to the factors related to users' concerns about privacy breach and practices for preserving privacy. The purpose of this research is to classify social networks in terms of the type of platform used in both the online and mobile categories, and then, in terms of the type of service and the type of architecture used, classify them such that the similarity of both groups is, to some extent, also shown. Then, we classify the privacy challenges of social networks users that have already been raised and the solutions that have been proposed for them. In addition, we determine the open challenges that still threaten to violate user privacy. We also examine the factors that affect the privacy concerns of users and how these factors can be used to personalize users' privacy settings (which are now the same for all users).

As outlined in the introduction, the main purpose of this paper is to examine models, proposed solutions, and fundamental open challenges in protecting the privacy of social networks users; determine the factors that influence user concerns about privacy violation; and provide conditions for increasing flexibility in privacy settings. To this end, in this paper, we study the research that focuses on providing a model for protecting user data in social networks. Accounting for the concepts and privacy requirements, we categorize the mobile and online social networks, and compare them at the end of each section in terms of the capabilities that they support. We focus on research that addresses the factors that affect privacy concerns. This research usually involves users' perception of privacy settings and their behaviors. Depending on the actions of users, factors that affect privacy concerns are identified for use in designing future social networks.

The rest of the paper is organized as follows. First, in Sect. 2, we describe the privacy challenges in both mobile social networks and online social networks. Then, in Sect. 3, we discuss the findings in detail, and finally, in Sect. 4, we conclude the paper.

2 Privacy challenges on social networks

Individual privacy on a network is a function of its ability to determine the type and amount of information to show and the way in which to show it to others or hide it from them (De Capitani di vimercati et al. 2012). When studying privacy, it is important to specify what defines a failure to preserve privacy. A privacy breach occurs when a piece of sensitive information about an individual is disclosed to an adversary, which is someone whose aim is to compromise privacy (Mani et al. 2009).

Depending on the type and extent of use of a social network, challenges and privacy concerns vary. In the following, the privacy challenges of online and mobile social networks are described separately.

2.1 The challenges of privacy in MSNs

In MSNs, the level of privacy depends on the application, the point of view (sender and recipient), and the level of trust between entities (Chin and Zhang 2013). In addition, the types of data that are sent and the sending mechanisms may pose a threat to privacy (i.e., in content-based transmission, message content is directly linked to the destination profile. The content of an exchanged message must be protected from unauthorized access) (Ardagna et al. 2013).

Privacy and submission of information, in terms of requirements, are contradictory. The former (privacy) requires encryption, which increases the computational overhead, while the latter (sending) requires access to the filters (Chin and Zhang 2013). Accordingly, different mechanisms have been proposed to strike such a balance and address privacy challenges. Each of these mechanisms focuses on protecting the privacy of a different type of data.

In MSNs, depending on the type of architecture (centralized or decentralized), different data have different sensitivities. This means that the mechanisms can be distinguished based on the focus on the user data type. In research on decentralized MSNs, protective mechanisms revolve around one sensitive data, user location data, or data about social relationships of users (Ardagna et al. 2013). Given that the purpose of this paper is to investigate social networks based on social networks services without geographical constraints, therefore, the discussion about centralized MSNs (which is based on Bluetooth or Wi-Fi communication based on distance) is ignored.

Therefore, it is easy to categorize these mechanisms based on the types of data that they protect, such as sensitive data, including personal and professional information, social relationships, and user locations.

2.1.1 Privacy preserving the privacy of sensitive data and social relationships in decentralized MSNs

All personal, identity, social, and professional information may be considered as belonging to the category of sensitive information. Sensitive information obfuscation is one of the approaches that enable users to modify their data in an organized way. Obfuscation is a form of a mask that is used with the objective of scrambling data to prevent unauthenticated access to sensitive information (Najaflou et al. 2013). Obfuscation refers to the type of encryption that is used to obscure data and provide fine-grained access control for users. Obfuscation of users' interests to prevent attackers from identifying users was presented in (Dóra and Holczer 2010), in which an obfuscation-based defense mechanism is implemented by focusing on the anonymity of the users' interests. Similar to identity information, users' interests represent valuable information that must be protected from unauthorized access. Direct disclosure of this information to unknown users as a result of unfair conditions that ensue from the misbehavior of other users is undesirable. The type of behavior of components of social networks in the disclosure of such information depends on their fairness (Mtibaa and Harras 2011; Feng et al. 1998; Xiaohui et al. 2011). Establishing social fairness in this type of network involves challenges such as distinguishing between unfair cheating behavior and unpredictable disconnection, information traceability and identifiable of untrustworthy and short-term neighbors, and time sensitivity of location-based services (Feng et al. 1998). One approach for establishing social fairness is controlling the behavior of the components of MSNs. Third-party mediation is another suggested method for ensuring full social fairness. Another solution is to establish trust gradually by exchanging private messages, with a special emphasis on information that the parties are allowed to access. In this regard, the gradual exchange protocol (GEP) was suggested to ensure the gradual establishment of trust (Blum 1983). GEP allows users to gradually disclose their secrets to each other. In this way, the parties disclose their information to each other as long as they trust each other.

Access control policies are other methods that can be used to protect the privacy of sensitive data. Fine-grained and coarse-grained access control schemes are some solutions in this category. In coarse-grained schemes, privacy is achieved by matching the set of attributes between two user's profiles. FINDU (Li et al. 2011) presented a privacy-protection mechanism for personal profiles that is based on coarse-grained access control in social networks, in which the user has the ability to control access to each level. Coarse-grained schemes cannot differentiate between users with similar characteristics. In other words, these designs are perfect for groups or large collections with different characteristics. This means that, for two users with the same characteristics in one set, these schemes are not able to meet the privacy requirements for each user. To address these issues, fine-grained schemes have been presented. A fine-grained scheme can distinguish one user from other users, and two users can communicate with each other without having to disclose sensitive information. Distance scale is one measure that is used to distinguish between users. Multiple protocols have been proposed based on the concept of user profile distance. In one of the protocols, the distance level is considered the level of privacy. The distance level is calculated based on the sum of the absolute differences between the two users in each attribute. Another protocol is based on a similarity threshold between two users. Moreover, calculating the maximum distance among attributes is another method that can be used to determine the distance between users or their level of privacy (Qi and Hengartner 2011).

Wang et al. (2015) proposed a novel privacy-preserving matchmaking framework that can help users to find new friends in MSNs without leaking their private information. In their framework, a user (called the initiator) can find another user who shares the maximum number of common attributes with him (called the best match) among nearby users (called candidates), and only exchange an attribute intersection set with the best match, while other candidates only know the size of the attribute intersection set. This framework was based on a trusted server and its matchmaking protocol had two phases. Phase 1 was used to find the best match by computing the size of the intersection set of the initiator and each candidate, and phase 2 was used to exchange intersection sets with the best match. At the end of phase 1, the initiator and each candidate should only know the size of their intersection set. At the end of phase 2, the initiator and the best match should learn their intersection set (Wang et al. 2015). In the following, Abbas et al. (2016) presented a privacy-preserving matchmaking protocol in which users share encounter information and later utilize a cloud server to postencounter information to privately match their profiles with those of unknown users with whom they shared the encounter. In their protocol, neither the users nor the cloud server is able to discover the interests of any participant during matchmaking, and only users who shared an encounter are able to run the matchmaking protocol with each other later, so sensitive data are protected by the non-friend users. Moreover, for location privacy, the location obfuscation method is used (Abbas et al. 2016).

2.1.2 Privacy preserving the privacy of user location data in decentralized MSNs

Social networks provide users with the possibility of sharing locations, sharing content based on location, tracking friends, sharing photos, etc. The use of these services by users requires them to disclosing their locations on social networks. Similar to sensitive information, user location information should have the possibility of management and access control (Xu 2009). This means that the user should be able to customize the time and location that are displayed or hide this information, so that the use of location-based services is not impaired. Moreover, there should not be any threat to the user's privacy. In other words, a user needs to strike a balance between revealing/hiding the location information and privacy, without interrupting the use of location-based services. Location-based services are so important that MSNs are considered combinations of OSNs and location-based services (Gongjun et al. 2009). Since the main purpose of social networks is to facilitate relationships, this combination provides the possibility of rendering new services, such as information services, to a friend when friends are present in the network. In other words, distance fades away in friendships. Therefore, the protection of location privacy is considered an independent aspect of privacy in research and several schemes have been presented (Duckham and Kulik 2005; Gedik and Ling 2008; Beach et al. 2009; Magkos et al. 2010; Wei et al. 2012; Liang et al. 2012; De Montjoye et al. 2013; Cheng and Aritsugi 2014; Wu et al. 2015; Abbas et al. 2016Xiao et al. 2017). Proposed schemes are inseparable in terms of trade practice and academic practice. The commercial schemes seek to provide better ways for designing social networks apps. The purpose of these solutions is to enable users to determine when to report location information. However, the academic solutions are generally based on the establishment of the third-party servers to protect the privacy of the user's location (Chang et al. 2011). From the Chao and Dongyu's (2013) point of view, research into location privacy can be classified into two main categories: studies based on the anonymity of location and studies that use obfuscation (Chao and Dongyu 2013).

From the perspective of research that was conducted by Najaflou et al. (2013), research into location privacy is in line with one of the schemes based on obfuscation, social, key management with a focus on key anonymity, and dynamic pseudonymity (Najaflou et al. 2013). Regardless of the type of approach used to protect privacy, all the approaches for protecting privacy have a major challenge: Most privacy-protection mechanisms are based on hiding the user's location, which makes it difficult to send this information to a location-based data service. In some cases, sending is interrupted or is completely disconnected. This is because for location-based services to be capable of providing service, they must be visible to users. On the other hand, to protect privacy, the location must be hidden from unauthorized audiences. Therefore, it is necessary to compromise between the level of location privacy and the users' location settings based on the spatial and temporal conditions. In addition, establishing fair social interactions between users when location-based services are used requires fairness in the participation of users. The participation of users involves the intrusion of privacy, including location privacy. Without policy management, this issue can be a threat to user privacy.

One of the first notable schemes for protecting location privacy was the obfuscation-based scheme that was introduced by Duckham and Kulik (2005). Their proposed formal framework for privacy in computing environments contains an effective mechanism for high-quality information services, to meet the needs of users in terms of location privacy. In this framework, the user's privacy is protected from the location-based service provider: the service provider is only able to access the information that is necessary for providing high-quality service. In fact, the proposed mechanism prevents unauthorized access of user location by the service provider (Duckham and Kulik 2005). Cheng and Aritsugi (2014) proposed a user-sensitive privacy-preserving system based on an obfuscation method for MSNs. Their scheme is composed of four fundamental elements: mobile devices, an SNS server, an LBS server, and an obfuscate server. The obfuscation method in their proposed system transforms the geographic data from the LBS server into an obfuscate region map. Users' actual locations are then cloaked and replaced with obfuscated region's coordinates from the obfuscate region map. The obfuscating process is based on the user profile, which includes the user-specified sensitivity level for certain features in the area, corresponding threshold, and query range (Cheng and Aritsugi 2014).

The integration of social characteristics of MSNs users has led to the formation of social-based schemes for protecting location privacy. In this context, privacy protection in Geo-social networks was a leading scheme. A mechanism for preventing the invasion of user location data and intrusion into friendships on MSNs was presented in (Wei et al. 2011). This coping mechanism made use of the capability of location spoofing in social networks. This technique increases the level of user location privacy without the need for a trusted third party. To strike a compromise between the need for location privacy and users' demands for hiding information from unwanted contacts based on social characteristics, a scheme has been provided by LBS. Wu et al. (2015) proposed a personalized privacy-protection model that considers the social relationship strength in MSNs for cloaking a user's location. The approach focuses on measuring the level of privacy between the user and his/her friend, and combines the features of personalization and flexibility to generate the cloaking range by introducing a probability distribution model (Wu et al. 2015).

To compromise between the need to protect the location privacy and the demand of users to hide their locations from unauthorized audiences, a social morality plan is presented based on social characteristics. The plan focuses on encouraging users to participate with the least threat to privacy and provides privacy through the users' appropriate participation in the location-based location-sharing service. Although this scheme uses social features of users for privacy, the selection of indicators that represent more precise social characteristics of users is subjective; therefore, the results are not generalizable and largely depend on the selection of features. Moreover, the plan relies on user participation; thus, if there are selfish users who are less willing to participate, privacy protection will be difficult, because selfish nodes may try to use the social features of users to obtain unauthorized additional information (Liang et al. 2015).

If a user's location is not well protected, it is possible to track the behavior of the user at different times, although this is difficult and time-consuming; it is a breach of privacy, especially in terms of guessing the mobility information of users. The mobility information of users is gathered from sensitive data, especially the associated locations and times (De Montjoye et al. 2013). Mobility data contain the approximate whereabouts of individuals and can be used to reconstruct individuals' movements across space and time. Approximation of a user's location at specific times means accessing additional information about the user, which is not necessarily desirable to the user. This approximation is estimated from geographic user locations, for which the number of points is closely related to the degree of the user's uniqueness: the fewer the points, the more unique the traces are and the easier the traces are to re-identify. Moreover, the uniqueness of mobility traces depends on the spatial and temporal resolution of data; increasing the size of the region or reducing the temporal resolution of the data set makes re-identification harder. The traces are more unique when they are coarse on one dimension and fine along another than when they are medium-grained along both dimensions. When the mobility traces are highly unique, one can be re-identified using outside information. Given the amount of information that can be inferred from mobility data, as well as the large number of simply anonymized mobility data sets, the privacy concern is growing (De Montjoye et al. 2013).

Although the capability to change the location provides uncertainty in communication in terms of local identity, through anonymity, we can also protect location privacy. In other words, by making appropriate changes, it is possible to prevent detection attacks on user location. A simply anonymized data set does not contain a name, home address, phone number, or other obvious identifier (De Montjoye et al. 2013). In this area, Magkos et al. (2010) proposed a distributed scheme to deal with location tracking to improve security and privacy on MSNs. The plan protects privacy by applying access control policies. In addition, through this scheme, it is possible to prevent network traffic analysis attack. Encryption methods with the capability of key management, including secure key generation/distribution, represent another method that has been proposed for preserving location privacy. In general, these methods have been presented to deal with vulnerabilities caused by misbehavior of users in MSNs. Key anonymity methods are effective and flexible methods for location privacy (Magkos et al. (2010). Gruteser and Grunwald (2003) first introduced k-anonymity into location privacy. It meets location k-anonymity when the location of a mobile user cannot be distinguished from other (k–1) users. This method protects the location privacy by sending a minimum cloaking region which contains at least k users to the LBS instead sending a single user's exact location. In this method, a trusted third party is employed to generate these minimum cloaking regions through collecting the locations of different mobile users (Gruteser and Grunwald 2003).

The anonymisation of user location by perturbation algorithms is presented by Gedik and Ling (2008). In the proposed scheme, location k-anonymity is customized for an extended range of users with sensitive information. The important capability of this scheme lies in its location anonymization method of removing identity information and hiding the time and location information. The mobility of MSNs has turned users' need for privacy in real time into a challenge, because real-time performance requires a direct assumption on quasi-identifiers (Gedik and Ling 2008).

Another scheme is Social-k which ensures location privacy in real time. Anonymity should be such that the probability of being unique is low and re-identification is reduced. In other words, an external attacker with little information cannot identify the user with high probability (Beach et al. 2009). In 2012, MobiShare was proposed as a flexible privacy-preserving location-sharing system in MOSNs. In MobiShare, a user owns one real fake identifier and (k–1) dummy fake identifiers to prevent LBS from knowing the users' real fake identifiers. LBS merely have the probability of 1/k to select the real fake identifier of one user and his location in the database. Unfortunately, in the request phase, when the user sends out a friends' or strangers' location query, LBS can effortlessly distinguish his true record (Wei et al. 2012).

Xiao et al. (2017) proposed CenLocShare as A centralized privacy-preserving location-sharing system for mobile online social networks. CenLocShare is independent from the third-party server and integrates social networks sites and LBS into one server, and uses the dummy locations and the dedicated mapping protocols between LSSNS and Cellular Tower (CT) to share privacy-preserving locations. In the CenLocShare the storage load has considerably decreased. This is because CT does not save users' information (Xiao et al. 2017). Ye et al. (2016) to deal with the problem of privacy concerns when the location server is an untrusted on, proposed a proximity detection method which is based on the transfer of neighbor relation. Specifically, each user request in their method only needs to submit a nearby reference list to the social network server. Then, the SNS searches the neighbors of the request user by judging whether their nearby reference lists have a common item. The proposed method protects location privacy of users from server. Moreover, users can only get information about nearby users, not other extra information (Ye et al. 2016).

The relationship between privacy risk and utility is complex and highly dependent on the context and purpose of use. There is currently no international consensus on the best approach for anonymizing mobile phone data. Due to the growth in geospatial data, anonymization is more difficult than previously believed. Without proper anonymization, re-identification may cause harm to individuals and vulnerable groups, as well as to mobile network operators (UN Global Pulse 2015).

Table 1 briefly shows that each of the above studies meets the aspect of user privacy. In addition, which method is used?

Table 1 Classification of proposed scheme to protect the privacy of user data types (including sensitive information, user relations, and location data) in decentralized mobile social networks

Proposed solutions	Sensitive information/relation privacy					Location privacy				
	Scheme based on obfuscation	Scheme based on social fairness	Scheme based on access control		Scheme based on anonymity	Scheme based on obfuscation	Scheme based on social	Scheme based on access control	Scheme based on key management	
			Fine-grain	Coarse-grained					Anonymity	Encryption
Dóra and Holczer (2010)	✓	-	–	–	–	–	–	–	–	–
Feng et al. (1998)	–	✓	–	–	–	–	–	–	–	–
Blum (1983)	–	✓	–	–	–	–	–	–	–	–
Li et al. (2011)	–	–	–	✓	–	–	–	–	–	–
Qi and Hengartner (2011)	–	–	✓	✓	–	–	–	–	–	–
Wang et al. (2015)	–	–	✓	✓	–	–	–	–	–	–
Abbas et al. (2016)	–	–	✓	✓	–	✓	–	–	–	–
Duckham and Kulik (2005)	–	–	–	–	–	✓		–	–	–
Cheng and Aritsugi (2014)	–	–	–	–	–	✓		–	–	–
Wei et al. (2012)	–	–	–	–	–	–	✓	–	–	–
Liang et al. (2012)	–	–	–	–	–	–	✓	–	–	–
Wu et al. (2015)	–	–	–	–	–	–	✓	–	–	–
Magkos et al. (2010)	–	–	–	–	–	–	–	✓	-	–
Gruteser and Grunwald (2003)	–	–	–	–	–	–	–	–	✓	–
Gedik and Ling (2008)	–	–	–	–	–	–	–	–	✓	–
Beach et al. (2009)	–	–	–	–	–	–	–	–	✓	–
Ardagna et al. (2013)	–	–	–	–	–	–	–	–	–	–
Ye et al. (2013)	–	–	–	–	–	–	–	–	–	✓
Xiao et al. (2017)	–	–	–	–	–	–	–	–	✓	–
De Montjoye et al. (2013)	–	–	–	–	–	–	–	–	✓	–

In the proposed methods, we have "✓" if the scheme satisfies the property; "–" if not

2.2 The challenges of privacy in OSNs

To protect the privacy of users and supplement the privacy services, different models are presented in OSNs. In this study, we divide them into two categories, namely, centralized and decentralized, in terms of service type, data storage, and accessibility. It is necessary to explain that, in some research, this model is referred to as a peer-to-peer model based on client–server features; because of their similarities in terms of the type of service and data storage, in this study, we examine them in a decentralized category. Although each of these proposed methods tries to protect the privacy of users in some way, they still face challenges, which are described in detail.

2.2.1 Privacy in centralized OSNs

One of the architectures that is used in social networks is a centralized approach in the form of a client–server. In this structure, users in the role of client and server play the role of social networks' service providers. The client requests the required services from the server and the server responds to the requests. Using encryption techniques is one of the most effective methods for meeting the requirements of privacy in a centralized architecture. In the centralized social networks, one or a limited number of components (other than the social network users) are responsible for production management and distribution of encryption keys (Challal 2005). Given this interpretation, it seems that most giant social networks, such as Facebook, WhatsApp, and Telegram, use this method. The currently proposed method is generally based on maintaining the basic requirements for user privacy and data accessibility. BE-PEKS uses broadcast encryption to control access to data. In this method, management and access control of users' sensitive data are considered. In BE-PEKS, a social networks' service provider is responsible for producing, distributing, and managing keys for all users. To preserve user privacy, a primary task is assigned to the user in this structure. In this task, the user defines a series of roles and each of his/her friends is mapped to one of these roles. The broadcast encryption system defines appropriate access rights for each role. Hence, those who are mapped to a role also benefit from all the rights of the role. At the time of removing and adding a friend to a role, functions related to the definition of the access rights are re-executed. Thus, for a newly added user or a newly deleted user, requirements for forward secrecy and backward secrecy are guaranteed. In forward secrecy, when a member is added to a group, the new member is not able to access the data that was previously sent in the group. In backward secrecy, when a member is removed from or abandons a group, the member cannot access future data in the group (Sun et al. 2010).

In BE-PEKS, the social networks' service provider has the most important role in the encryption system. In addition, since the service provider is responsible for key generation and distribution operations, there should be complete trust. Therefore, the concept of user data confidentiality can be at risk. Furthermore, users with defined roles and users mapped to these roles determine the nature of their relationships and interactions. Thus, relation privacy is not guaranteed. Since each user can be mapped to only one role, fine-grained access control is not entirely provided in this structure. Assigning much of the responsibility for encryption operations to the social networks' service provider requires full trust in the service provider; therefore, the confidentiality of shared data is compromised. Thus, the division of labor between various elements of the social network may partly solve this problem.

GCC (Zhu et al. 2010) is a method in which the social network provider, as a system administrator, generates a series of general parameters. At the time of registration, using a general parameter, the user generates a private key. In addition, when the user adds a friend, he or she produces an access key using his or her private key, which will be sent to the friend. In this method, a series of users are considered core users. Core users are responsible for preserving privacy. The user maps his/her friends to a series of associations. After the mapping operation, the user contacts core users and, by combining their private keys, core users generate a key for the community. Then, the user generates a random session key by combining the private key and the community key. When the user wants to share data with a friend's community, he/she encrypts the data using the random session key. To access the shared data within the community, a friend can use his/her private and access key to obtain and decrypt the shared data session key (Zhu et al. 2010). In the GCC, users must have full confidence in the core users. In addition, core users need to be online at all times and synchronized with one another. In other words, the core users should always be state-full, which requires very high costs. In GCC, there is no flexibility in terms of access to data.

2.2.2 Privacy in decentralized OSNs

The decentralized methods, as their name suggests, shift the focus from one point (the social network provider) to several other components (the users themselves or third parties). In this architecture, the responsibility for a large part of the privacy, confidentiality, access control, encryption, decryption, etc., is assigned to a component other than the social network provider. Usually, in this architecture, one of the main goals is to eliminate or diminish the role of the social network provider and the need to trust a central manager (Luo et al. 2009). Accounting for the privacy requirements, this type of architecture has many similarities with social networks features, where the responsibility for maintaining and operating the social network is shifted from the provider to the users, but the accessibility and privacy requirements must still be adequately satisfied (Buchegger and Datta 2009; Schiberg 2008; Afifty 2008). This means that shared user information that is independent of the online or offline owner of the data must be accessible at any time by the authorized audience. Therefore, in addition to satisfying privacy requirements in such networks, the availability of data must also be guaranteed.

The Vis-`a- Vis method is based on the elimination of the role of the social networks service provider that uses individual virtual servers for storing user data. The storage space may be users' machines, cloud storage space, or a combination of both. When a user is online, stored data are shared on his/her machine and on some trusted friends' machines, whereas when the user is offline, the data are sent to the cloud storage (Shakimov et al. 2011). The privacy level of this approach is dependent on the amount of trust in the cloud storage space and friends' machines as the hosts of user data. In this method of sending data to a storage space, no encryption technique has been applied. Data confidentiality is not considered, and the data are stored in an unencrypted way in the cloud storage. In addition, there is no specific policy for data access control; therefore, once the data have been stored, the storage space owner has full control over the data. Two factors affect the accessibility of data: the online times of the user or his or her friends, as well as the availability of selected cloud storage servers. Similarly, to eliminate the role of the service provider, LifeSocialKOM (Graf et al. 2011) utilizes a peer-to-peer structure (where users must provide all their resources on a social network, such as storage space to store their shared data). In this method, an appropriate encryption technique is used to ensure the confidentiality of user data against the service provider and non-friend users. Each user is added to the network using a pair of public–private keys; the public key serves as an identifier for establishing communication. In this technique, the user's confidential data (personal or sensitive data) are encrypted with a symmetric key. In the process of encryption, the symmetric key is encrypted using the public key, which is available to all audiences and is stored beside the encrypted data. In LifeSocialKOM, confidential data are stored in encrypted format; however, this approach does not account for the accessibility and access control when the data owner is in offline mode. In other words, circumstances may occur in which authorized contacts are not able to access the shared data. This method does not guarantee the availability of shared data (Graf et al. 2011).

LotusNet (Aiello and Ruffo 2012) is another model that protects user relationships and their identity based on public key encryption. In this model, a pair of public/private keys is created for each user and, according to the time and type of data access, the user defines access control policies for his/her friends. In other words, for each friend, the user produces a signed certificate with an expiration date, which determines what type of data that the user has permission to access. In addition, the duration of the validity of data access is determined based on the certification date. LotusNet makes use of trusted friends for storing shared data. Friends need to be authenticated by the user to access shared data. To accomplish this, first, the confirmed certification must be sent by the user to the node that stores the data. Upon confirmation, the user can access the shared data. Moreover, the accessibility depends on the storage nodes. In addition, privacy depends on the amount of trust in the storage nodes. In the case of access control, because the expiration date of friendship is specified in the certificate, if the need arises to revoke the relationship, it is necessary to wait until the certificate expires. This means that all aspects of user access control cannot be achieved (Aiello and Ruffo 2012).

Each friend of a user may have different attributes, which is due to some common elements with the user in his friends list. Depending on the characteristics and the number of shared friends, different social relationships are formed, which the user needs to manage and control. DECENT (Jahid et al. 2012) uses an attribute-based encryption method and, according to the characteristics of his friends, produces the appropriate keys. This structure uses the object-oriented design concept and data are considered a set of objects. Each object contains two parts: one part contains the content and the other part stores a set of references to other objects. Moreover, each user has a root object, which contains information related to user profiles with references to other objects. The DECENT architecture uses the public key and the Friends attribute key to obtain the policy for controlling the access level. After authorization by the policy to share data with a specific friend, the encryption operation is carried out. At the time of reading the shared data, first, the authorized friend finds the reference to data; then, with the permission given to him/her by the access policy, he/she receives the decryption key to access the content of the message. With DECENT, it is possible to combine the exceptional operator, friends' IDs, and their attributes (Jahid et al. 2012). In DECENT, there is the issue of revocation of friends and no details have been given about the availability of data.

PeerSON (Buchegger and Datta 2009) focuses on access control using symmetric cryptographic techniques and a public key for confidentiality. In the proposed method, users are classified into different groups and a public/private key pair is assigned to each group. In this method, if the number of groups is large, then the computational overhead of key generation for each group is huge. In this method, an attempt has been made to improve the situation of user access control with a combination of symmetric encryption and a public key; nonetheless, all aspects of access control (flexible, dynamic and fine-grained) have not yet completely been implemented. Moreover, PeerSON does not focus on shared data accessibility between users. In addition, there are uncertainties about friend revocation from a group and the process of key re-generation/distribution. An improved version of PeerSON uses a concept called Link to distinguish each friend. A link folder specifies to which groups each friend is a member. Moreover, the link to the encrypted data that the user is able to decode is placed in this folder. In this method, the user can encrypt the shared data with a symmetric key and store it in a storage space, since data links represent an authorized audience that can access the shared data; the confidentiality of authorized friends is protected. In other words, the privacy of the user's relations with friends is ensured. After this step, using a broadcast encryption system, the user encrypts the data encryption key, and then, the encrypted data along with a link to the encrypted data are stored in the relevant folder (Buchegger and Datta 2009).

Although the ability to store user data in a location other than the service provider's space is helpful for reducing the role of the provider and the need to trust it, providing access to data at any time has become a challenge. The social network service must provide data access capabilities at any time, independent of the online or offline owner of the data. Porkut has focused on the accessibility of data on social networks and has proposed a method for selecting the data storage node. In Porkut, node selection for data storage is based on online status. That is, a greedy algorithm based on online time offers all the user's friends more online time compared to others. In this algorithm, the online presence of friends in a social network is considered at fixed-length intervals. The activation of a friend is also a desirable parameter. This means that a friend is chosen that has the most willingness to receive and exchange messages with the user. In the Porkut method, the assumption is that there is complete trust in the storage nodes. With the assumption of complete trust, access control for shared data is meaningless. Moreover, the shared data are stored on storage nodes without encryption (Narendula et al. 2010a, 2011; Narendula 2010b).

PESCA (Raji et al. 2014) is a service that is composed of a privacy-enabled setup for users' social communications and an adaptive replica placement strategy for ensuring the availability of users' shared data. In PESCA, the user's data privacy, that is, the confidentiality of the user's shared data and the user's ability to completely control access to his/her shared content, is preserved. Full access control capability (including coarse-grained, fine-grained, flexible, and dynamic access control) on shared data and social communications, and using a combination of trusted friends to support data availability, are outstanding characteristics of PESCA. PESCA addresses the big-brother privacy problem in existing OSNs by fully decentralizing the OSN structure and employing cryptographic access control. By focusing on choosing the best combination of online direct/indirect friends as replicas, PESCA has removed the OSN provider role; however, using the traffic analysis technique that results in the extraction of user activities from a social graph, it may indirectly disclose user information (Raji et al. 2014).

Mistrustful P2P decentralized model is presented by da Silva and Dias (2017). The Mistrustful P2P model is built on the concept of mistrusting all the entities participating in the P2P network, and therefore, users are not required to establish any trust links to participate in the content sharing. Some capability of Mistrustful P2P model includes: it has no trust requirements, prevents user legal liability in case of legitimate usage, and ensures deterministic protection of user content interests against attacks of a size up to a configured level. The Mistrustful is based on two main building blocks—content interest disguise and mistrustful sharing—and aims at hiding user content interests through plausible deniability, in untrusted P2P networks, while overcoming the main limitations of P2P file sharing systems including (1) peers are required to advertise what they download enabling passive attacks; (2) protection against active attacks is only achieved by introducing either trust requirements or considerable network overhead; (3) the privacy protection against both passive and active attacks is probabilistic (da Silva and Dias 2017).

Access control by defining different access levels for different users in social networks is one of the user requirements. In Persona (Baden et al. 2009), the user is allowed to classify his/her friends into different groups, with different access levels for each group. In this way, the confidentiality of user data is guaranteed against the service provider and non-affiliated users through attribute-based encryption. First, the user assigns a series of attributes to his/her friends. Then, based on the defined attributes, keys are produced for friends using a key-based encryption technique. Data encryption is performed using a symmetric key, so only friends with the same attribute can decrypt the data. When a user receives shared data, through encryption techniques based on attributes, he/she can access the data. In Persona, attributes that are assigned to the groups are constant, and only at the time of defining the group is it possible to add friends (Baden et al. 2009). However, over time, it may be necessary to remove or add an attribute to a specific group, which is not supported in this method. The dynamics of friendship and the possibility of friends changing over time have not been considered. This means that flexible and dynamic access control is not supported by Persona.

Using a trusted third party to reduce the role of the service provider and protect data and user relationships is another approach that has been used in some decentralized models. FlyByNight, EASiER, Safebook, FaceCloak, NOYB, and

Lockr are some of these models (Jahid et al. 2011; Lucas and Borisov 2008; Cutillo et al. 2009; Luo et al. 2009; Guha et al. 2008; Tootoonchian et al. 2008, 2009).

EASiER (2011) was designed to improve the dynamic access control capability by changing attribute-based encryption in Persona. In particular, this approach focuses on third-party trust-based access control, coupled with the ability to revoke friends. In this method, similar to Persona, the user first defines a set of attributes. Then, according to the type of relations, it assigns friends to these attributes and, using the attribute-based encryption technique, it encrypts shared data for friends with special features. In EASiER, if a friend has been revoked, a proxy key is generated for the revoked friend and the information is sent to the third party with the relevant data. The third party changes the encrypted shared data with the proxy key and the applied changes are such that authorized friends using attribute-based encryption techniques will be able to decrypt the data (Jahid et al. 2011). In EASiER, groups must be formed and attribute assignments to groups must be made at the beginning. This means that the user is not able to create groups at any other time. In other words, there is no flexibility in terms of the time at which groups can be created. In addition, when an attribute is assigned to a group, this attribute applies to all members. Excluding a member from an attribute is possible only with relationship revocation. In other words, there is no flexible access control on the combination of friends and relations. As for the possibility of friend revocation from a relationship, EASiER uses a threshold. Exceeding the threshold will eliminate the possibility of a friend's revocation. Moreover, to support friend revocation from a group or a relationship, all possibilities of revocation should be considered at the same time as groups are created. Hence, despite the focus of EASiER on dynamic access control by adding the possibility of friend revocation, dynamic access control is not fully guaranteed (Jahid et al. 2011).

The FlyByNight Lucas and Borisov (2008) method uses a trusted third-party server for proxy encryption. In this way, each user generates a private/public key pair for her friend and classifies them as a group. For each group, a public/private key pair is considered. When a friend is added to a group, using proxy encryption techniques, a proxy key that is associated with the friend is produced and sends the key-related friends to a third-party server. At the time of data sharing in the group, the user performs an encryption operation on the group key and sends the result to a third-party server. For a friend of the group to access the shared data, the third-party proxy server performs encryption using a friend proxy key to prepare the encrypted data that correspond to the friend (Lucas and Borisov 2008).

In the FlyByNight method, the key generation cost is high. In addition, to remove or revoke a member of the group, all key generation operations must resume. In addition, no attention is paid to access control, especially dynamic and flexible capabilities.

Given that the OSNs are designed to simulate the social interaction of users in the Internet environment, it should be possible for users to share their data based on social relationships with their friends, since the social relationship that exists between a user and each of his friends is different (Fogel and Nehmad 2009). For example, social network friends may be classmates, close friends, family members, and others. In terms of confidentiality, each of these groups is at a different level, and each level has different privacy requirements in proportion to their relationship distance from the user. This means that the user has a specific border with each of them. Safebook, which is presented by Cutillo et al. (2009), is a circular structure with a boundary for the user with each of his friends. In this model, when a user registers on a social network, a set of user friends named Matryoshkas group into this structure. In the Matryoshkas structure, the user is in the center of a circle and his friends are around him/her based on their friendship. In this structure, the more reliable the friend, the closer to the center he/she will be on the circle. This means the trusted friends of user are on the first circle. The second circle contains trusted friends of the first circle and this circle continues in this way. The number of circles in the structure of Matryoshkas is determined by the user. Matryoshkas specifically provides end-to-end confidentiality and distributed storage space with privacy preservation for users. Given that the first circle contains the trusted friends, the user stores the shared data on all of them. In this method, access control is carried out, using anonymity techniques and public key encryption and on behalf of the user; the user's friends will have access control. Through this structure, the user's trusted friends can access all the shared data of the user.

A user may have different social relationships with a friend who needs to be classified into multiple groups, which is not considered in this structure. Moreover, users' social relationships may change over time; thus, it must be possible to update Matryoshkas at any time. This means that the circle of user communications has been changed or expanded, but, in this structure, because Matryoshkas must be specified at the beginning, this feature is also not supported. Therefore, it can be claimed that Safebook cannot guarantee flexible access control and dynamism in user relationships. Moreover, the privacy greatly depends on the reliability of trusted friends (Cutillo et al. 2009).

Trust in the social networks service provider is one of the major challenges in guaranteeing user privacy. Removing or decreasing the role of the social network provider using the third-party server is proposed as one of the approaches for overcoming this challenge. FaceCloak (Luo et al. 2009) uses a third party to store encrypted shared data and stores fake data instead of shared data on the social network. To encode shared data on the third-party server, the user generates a key set and sends the keys to her friends. When the user requests shared data, this request is sent to both the social network and FaceCloak. In response to this request, first, the social network sends fake data, and then, FaceCloak communicates with the third-party server to obtain the actual encrypted data. After the encrypted data are made available to FaceCloak, it decrypts them and replaces the fake data received from users. This method focuses only on the confidentiality of data and protecting them against non-friend users, especially the social network provider (Luo et al. 2009).

Similar to FaceCloak, NOYB (Guha et al. 2008), which is based on the use of obfuscation, is used with social networks. In this method, a trusted server is used to store shared data and focuses on protecting the confidentiality of the data against the non-friend users and the social network provider. At the time of data sharing, for each shared data item, a symmetric key is generated by the user and divided into several parts. For each part, a dictionary provides possible values. Then, the dictionary stores the data on the trusted server. When a friend wants to access shared data, initially, he/she receives fake values that are stored on the server of the social network. Then, using the keys received from the user and through access to his/her dictionary, it is possible to obtain the real user data. In addition, in the NOYB scheme for preventing attacks on personal profiles, user information from different sites is combined, and to achieve privacy, this method is equipped with several mechanisms, such as the marginal distribution of the cipher text, atom compartmentalization, public dictionary, random nonce, steganography, standard ciphers, and communication across different channels (Guha et al. 2008).

Defining different social relationships for friends is one of the needs of a user. To improve the implementation of changes in the social relations of users in a social network, Lockr (Tootoonchian et al. 2008, 2009) was proposed. In Lockr, the user is able to define different relations and, for each friend, consider a social certification, which represents the social relationship of the user with the friend. There is also the ability to define an access control list that includes friend IDs or user–social relationships. When a user shares data, he/she also assigns an access control list to the shared data. The user can prove his/her authorization to access friend data in two ways: (1) by showing his/her social certification to the social network service provider, and (2) using Challenge–Response Operations to prove that his/her ID is on the access control list. If the user can prove his/her identity with one of these two methods, a session key is created between the friend and social network provider, and the social network provider uses this key to encrypt user data and send it to the friend. In Lockr, data in plaintext format are stored by the social network provider and there is complete confidence in the social network provider (Tootoonchian et al. 2008, 2009). This method does not focus on the confidentiality of data but rather the social network provider and the user relation confidentiality. Since the access control list can contain users' IDs and their social relationships with each other, the social network provider can easily discover the type of interaction with any of the user's friends. Although the access control list specifies the type of shared data access for authorized friends, the capability of dynamic access control is not included. Moreover, to revoke a friendship or delete a friend from the friendship set, a new social certification should be created for friends who have a similar relationship with this friend. Hence, the issue of high computational overhead comes to light.

DEFF (Raji et al. 2013), using a semi-trusted proxy server, is focused on completely access control such as dynamic, efficient, flexible, and fine-grained on OSNs. In the DEFF system, users are allowed to cryptographically categorize their friends into different relations and to share data with arbitrary groups of them. DEFF employs a simplified broadcast encryption (BE) scheme to provide full access control system for OSN users. Proxy maintains a tree of keys. The proxy key tree (PKT) is for the universe of users. PKT is created gradually, and is used to encrypt and exchange confidential data between the user and Proxy over public channels. Proxy shares some secret key to each user's social network. When updating their relationship, they do not have to change privacy settings, so dynamic access control of relationship is provided for OSN users. In DEFF, a random identifier is assigned to each friend. Since user information is not used in the generation of ID, confidentiality of user friends and relations is protected. Moreover, removing/revoking friends are done through this ID and there is no need for new settings in privacy and generating and sending new keys. DEFF provides the possibility of data audience determination based on different social relations. Therefore, DEFF guarantees the flexibility of access control for OSN users (Raji et al. 2013).

Patsakis et al. (2014) proposed a distributed scheme for privacy preserving in media content sharing on OSNs. This scheme focused to resolve issues related to identity theft, unauthorized content sharing, and distortion of malleable content and shared ownership. This is a distributed scheme independent from the third party. This means that there is no further trust dependence. For privacy preserving, this scheme use public encryption algorithms. Moreover, using public watermarking scheme provides another layer of security (Patsakis et al. 2014).

CommonFinder (Fu et al. 2014) distributed common-friend estimation scheme that proposed by FU et al. CommonFinder is a distributed estimation scheme that estimates the numbers of common friends between any pairs of users without disclosing the friends' information. For privacy preserving, this model use Bloom filters to collect a small number of common-friend samples. Moreover, CommonFinder is based on low-dimensional coordinates to estimate the numbers of common friends from each user to any other users. This model assumes that users are semi-honest. In addition, for privacy preserving against non-friends and service providers provide anonymous communication process (Fu et al. 2014).

Table 2 shows that each of the examined schemes in this section covers which of the privacy requirements includes aspects of confidentiality and access control on users' friends and users' relations. In addition, the type of architecture used in each design is also specified.

Although the proposed methods have tried to provide protection platforms for privacy and satisfy users' privacy requirements, no method that comprehensively satisfies all privacy requirements has been introduced. Each of the above studies focuses on one or more of the requirements of privacy.

2.3 The factors affecting on users privacy concerns due to privacy challenges

Social networks provides great advantages for users, including the ability to communicate and share data without limits of time and space, the possibility of sending messages in any format, and the reduced cost of sending messages. Despite these benefits, risks such as disclosure of confidential information, the possibility of information theft, and concerns about privacy violations are the challenges that social network users are facing. Therefore, identification of privacy risks associated with social networks and the factors that affect on privacy concern have long been considered by researchers.

Privacy concern refers to the users' concern about threats to their privacy online. This constructs reflects users' response to the perceived possibility of a privacy leak and the expected loss induced by the abuse of privacy (Xu et al. 2013). According to Paine et al. (2007), privacy concern is not only the reaction to the security of privacy but also a motivator for users to take care of their personal information (Paine et al. 2007). Milne and Culnan (2004) proved high levels of privacy concern provided the impetus for users to read, at least, the introduction of privacy policies online (Milne and Culnan 2004) and users with high levels of privacy concern may also be inclined to refuse to submit personal information to a social network site (Sheehan and Hoy 1999) or to submit false information (Gross and Acquisti 2005). Privacy concern has become one of the most important factors in studying online privacy issues.

So far, the impact of many factors on user privacy concerns has been proven. Privacy risk, information control, information sensitivity, subjective norm, and trust are some of them (Phelps et al. 2001; Malhotra et al. 2004; Milne and Culnan 2004; Chellappa and Sin 2005; Paine et al. 2007; Xu et al. 2013).

Privacy risk refers to users' expectation of losses associated with privacy disclosure online, which is caused by opportunistic behavior and the misuse of personal information. The greater the losses caused by the disclosure of personal information, the greater the risk users would perceive. Chellappa and Sin (2005) proved a positive relationship between privacy concern and privacy risk, but did not mention the causation relation. In their model presented, the level of privacy concern of Internet users was proved to have a positive effect on privacy risk (Chellappa and Sin 2005). Xu et al. (2008) and Dinev and Hart (2004) proved that perceived risk had a positive effect on privacy concern (Xu et al. 2008; Dinev and Hart 2004).

Information control refers to the capacity that people have to control information released online. Factors that determine the perception people have of information control relate to manners in which web sites collect, store, and utilize user personal information (Xu et al. 2013). We could postulate that if a privacy policy of a given website made users feel they could maintain their privacy, it would significantly decrease the level of user privacy concern. In researching online shopping, Phelps et al. (2001) thought that the lack of control over personal information explained 42.5% of the change in people's level of privacy concern (Phelps et al. 2001). Dinev and Hart (2004) considered that it was the control that people perceived over their personal information that governed the extent of self-disclosure online (Dinev and Hart 2004).

Information sensitivity represents people's attitudes toward revealing differing levels of personal information during the online shopping experience (Xu et al. 2013). Phelps et al. (2001) divided personal information into three categories: (1) demographic information; (2) lifestyle and shopping information; (3) personal financial information. Malhotra et al. (2004) found that people are willing to provide less sensitive information online, but when they are faced with the dilemma of providing more sensitive information, they usually decline participation (Malhotra et al. 2004). To measure privacy sensitivity, Yang and Wang (2009) set matched groups in their experiment: (1) users that were asked demographic information only; (2) users that were asked both demographic information and personal financial information (Yang and Wang 2009).

As a notion deriving from psychology and sociology, subjective norm has been well used in studies exploring factors acting on people's attitude about certain behaviors. Lehikoinen et al. (2008) found that social culture had a significant effect on people's information disclosure in social networks (Lehikoinen et al. 2008). Kaufman et al. (2008) found that students were more likely to take part in social

Table 2 Classification of proposed methods based on confidentiality mechanisms (including protect against service provider, non- friends, confidentiality of relations), access control (including fine-grain, flexible, and dynamic), and accessibility in centralized and decentralized online social networks

Method	Parameters												
	Confidentiality			Access control							Availability	Architecture	
	Protect the confidentiality against the service provider	Protect the confidentiality against the non-friends	Confidentiality of relations	Coarse grain	Fine-grain		Flexible		Dynamic			Centralized	Decentralized
					Single membership	Multi membership	Relation	Friends	Add	Remove/ Revoke			
									Relation	Friends			
Safebook (2009)	✓	✓	–	✓	–	–	–	–	–	–	–	–	✓
Vis-`a-Vis (2011)	✓	✓	–	-	–	–	–	–	–	–	–	–	✓
LifeSocial-KOM (2011)	✓	✓	–	✓	–	–	–	–	–	–	–	–	✓
LotusNet (2012)	✓	✓	–	✓	–	–	–	–	–	–	–	–	✓
DECENT (2012)	✓	✓	–	✓	✓	✓	✓	–	–	✓	–	–	✓
PeerSON Buchegger and Datta 2009	✓	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	✓
Porkut (2010)	✓	✓	–	–	–	–	–	–	–	–	✓	–	✓
PESCA (2014)	✓	✓	✓	✓	✓	–	✓	✓	*	✓	✓	–	✓
Mistrustful P2P (2017)	✓	✓	✓	–	–	–	–	–	–	–	✓	–	✓
BE-PEKS (2010)	–	✓	–	✓	✓	–	–	–	✓	✓	–	✓	–
GCC (2010)	*	–	–	✓	✓	✓	–	–	✓	✓	–	✓	–
FlyByNight Lucas and Borisov 2008	*	✓	–	✓	✓	✓	–	–	–	–	–	–	✓
FaceCloak (Luo et al. 2009)	✓	✓	–	–	–	–	–	–	–	-	–	–	✓
NOYB (Guha et al. 2008)	✓	✓	–	–	–	–	–	–	–	–	–	–	✓

Table 2 (continued)

Method	Parameters												
	Confidentiality			Access control							Availability	Architecture	
	Protect the confidentiality against the service provider	Protect the confidentiality against the non-friends	Confidentiality of relations	Coarse grain	Fine-grain		Flexible		Dynamic			Centralized	Decentralized
					Single membership	Multi membership	Relation	Friends	Add	Remove/ Revoke			
									Relation	Friends			
Persona (2009)	✓	✓	–	✓	✓	✓	✓	–	–	✓	–	–	✓
Lockr (Tootoonchian et al., 2008, 2009)	–	✓	–	✓	✓	✓	✓	✓	–	–	–	–	✓
EASiER (2011)	✓	✓	–	✓	✓	✓	✓	–	–	✓	–	–	✓
DEFF (Raji et al., 2013)	✓	✓	✓	✓	✓	–	✓	✓	✓	✓	–	–	✓
CommonFinder (Fu et al. 2014)	✓	✓	✓	–	–	–	–	–	–	–	–	–	✓

"✓" if the scheme satisfies the property; "–" if not and "*" if the scheme satisfies the property partially network sites where their classmates had already gained membership (Kaufman et al. 2008). Xu et al. (2013) demonstrated subjective norm acted on the degree that people regard privacy online. All of these studies have proved that subjective norm has influenced people's privacy disclosure online.

Trust means users' sense of trust about certain websites. Trust factors about privacy online were influenced by the user experience and familiarity to an online website. Usually, but not always how personal information (e.g., age and gender) characteristics are used by an online organization is set out in their privacy policy (Culnan and Armstrong 1999; Dwyer et al. 2007).

Some research specifically focuses on the demographic characteristics of the user and its relationship with privacy concerns. Based on Gross and Acquisti (2005), the use of social networks in which user privacy requirements and security issues are not considered has highlighted risks such as stalking, identity theft, price discrimination, and blackmailing (Gross and Acquisti 2005). The severity of risk associated with the use of social networks depends on their culture and social structures. Damaged reputations, unwanted contacts, and surveillance-like structures due to backtracking functions, harassment, and the use of personal data by third parties are some of the known dangers in the use of social networks (Boyd and Ellison 2007).

Social network users usually share different data. Depending on the type of data, there are different levels of risk. In other words, according to the type and significance of data, users will have different concerns. Social networks sites, as potential locations for user data, include various types of data, such as personal, sensitive, and professional information. Skeels and Grudin (2009) studied social networks sites that are used in the workplace. In their study, tensions caused by mixing professional and personal circles were examined (for example, the crossing of hierarchy and/or power boundaries). Regrettably, due to the lack of limitations when sharing personal and professional information, the excessive social network penetration in users' lives and the financial risks due to the disclosure of professional information of the organization are some negative consequences of improper (uncontrolled) use of social networks (Skeels and Grudin 2009).

Studies have shown that concerns caused by the possible risks of using social networks are different among users. It seems that users' reactions to these risks depend on their sensitivity to, as well as their awareness of, different aspects of the social network service. Most studies that have focused on user concerns about the use of social networks have discussed negative consequences of this communication infrastructure, as well as regretful experiences of users. In addition, some parts of social networks that are related to users' privacy, such as privacy settings, are of interest to researchers. This section is one of the most important parts of the security and privacy issues of users, which is provided by the service provider for customization of the privacy settings by users. Users' awareness and knowledge of how to use it can reduce users' concerns to a certain extent. It should be noted that changes in the privacy settings do not fully guarantee privacy protection, because privacy is a multidimensional concept and different elements are involved in the formation of the concept of privacy and its protection (Gross and Acquisti 2005; Skeels and Grudin 2009; Acquist and Gross 2006; Ellison et al. 2007; Lampe et al. 2008; Fogel and Nehmad 2009; Gilbert et al. 2008; Besmer and Lipford 2009; Kaufman et al. 2008; Nov and Wattal 2009; Wang et al. 2011; Tufekci 2008).

The findings of the previous studies on students who were Facebook members in the United States of America have shown behavioral inconsistencies related to privacy concerns, too much sharing of personal information and rare changes to the default privacy settings. In a study conducted on Facebook users at the Carnegie Mellon University, Gross and Acquist (2005) found that the majority of users share large amounts of personal data with others, even though only a small percentage of them change their privacy settings (Gross and Acquisti 2005). In the same vein, in another study, Gross and Acquist found that even users who claim that they have concerns about privacy tend to reveal much of their personal information. In fact, it seems that there is a mismatch between their attitude toward privacy and their actual behavior (Acquist and Gross 2006). Ellison et al. (2007) found that only 13% of registered Facebook user profiles at the University of Michigan are restricted to friends (Ellison et al. 2007). Another study of the same population in different geographical areas confirmed this finding (Lampe et al. 2008). Since these studies were conducted on American college students, the results cannot be generalized to other populations. For example, Joinson conducted a study into Facebook users who were not primarily students in the UK in 2008 and found that the majority of respondents (57.5%) changed their default privacy settings (Joinson 2008). In this study, which was an online survey, and involved private interviews, a wider range of the population (the population was composed only of students) was considered. Recent studies have indicated that the users have many privacy concerns and tend to apply changes to their default privacy settings (Boyd and Hargittai 2010; Madden and Smith 2009). For example, according to a report, which the Pew Internet and American Life Project released, 71% of social networks websites users, who were in the age range of 18–29 years, announced changes in their privacy settings. Demographic characteristics in the user behavior analysis on social networks were another aspect of the research. Age and gender are two important user demographic features that affect the type and amount of user concerns about violations of their privacy on social networks. Fogel and Nehmad found that, in general, men are less concerned about privacy than their female counterparts and even tend to share more personal information such as phone numbers and physical addresses on the social networks websites (Fogel and Nehmad 2009). Statzman and Kramer-Duffeld (2010) found that female users and users who have more friends on social networks (Facebook's case) only prefer their friends to have access to their profiles. In fact, they feel concerned when the data are to be seen by unwanted audiences (Statzman and Kramer-Duffeld 2010). In a study conducted on MySpace users, Gilbert et al. (2008) found that rural users have fewer friends and make fewer comments than urban users. In addition, rural users, particularly women, have higher levels of concern about their privacy. Rural women apply more settings than urban users in their privacy settings (Gilbert et al. 2008). Boyd and Hargittai (2010) also found that individual characteristics such as Internet skill, frequency, and type of Facebook use are correlated with making modifications to privacy settings (Boyd and Hargittai 2010). Levels of user engagement and user friendliness with each other are effective in a sharing data format. Users display more concerns about sharing with their weak-tie friends than with outsiders or their colleagues in the workplace. In a study carried out on Facebook, Statzman and Kramer-Duffeld found that, in their profile settings, users are more sensitive to deal with unwanted disclosure of their information to a Weak-tie friend. Their study showed that the profile settings with the option friend-only to deal with unwanted disclosure by Weak-tie were more than those with outsiders (Stutzman and Kramer Duffield 2010). It should be noted, however, that a user's close friends have a higher confidence level, but there have a concern about data to be shared between them, especially when the relationship is terminated. User identification based on their profile represents inferred valuable information on social networks. The more the information that can be deduced from the shared data, the more the concerns about its disclosure. Besmar and Lipford found that there are more worries about photo privacy, which can be used for identification purposes and for impression management in a user's social circle. These photoprivacy concerns revolve around revelation of incriminating evidence (e.g., underage drinking), unflattering photos, and unwanted associates (e.g., ex-significant others) (Besmer and Lipford 2009). In 2008, a study was carried out on Facebook at Harvard University in which Lewis et al. found that students tend to have private profiles, so that only friends and roommates are able to access it (Kaufman et al. 2008). In another study conducted on the privacy settings on Flickr, Nov, and Wattal found that the sense of trust and sharing feel of a community positively affect community members' privacy concerns and information sharing behavior (Nov and Wattal 2009). Wang et al. (2011) examined the regrettable experiences related to posts made by users on Facebook. In their study which was based on a series of interviews, user diaries, and online surveys on American users, it was shown that, in most cases, users may regret after posting on Facebook.Some of the reasons for their regrets were: posts made in hot state of high emotion, the possibility of their posts being seen by an unintended audience, various interpretations about users' posts and creating inconvenience for the audience or user, revealing secrets with friends or family members, and misunderstanding or misusing the Facebook platform. Some significant results in this study were reflecting reports about breaking up of relationships or job losses.

In this study, negative experiences associated with social networks posts on Facebook are depicted (Wang et al. 2011).

In some cases, it appears that users, based on their needs and experiences, take administrative measures to deal with privacy risks. For example, Lampe et al. showed that some users have taken action to manage their profiles, for example, to create a constraint and who can see their profiles or sensitive content. Tufekci (2008) analyzed college students' information disclosure behaviors on social networks and found that "students manage unwanted audience concerns by adjusting profile visibility and using nicknames but not by restricting the information within the profile" (Tufekci 2008). In a year-long ethnographic study of Facebook users in their 20 s, Raynes-Goldie found various strategies including using aliases, deleting wall posts, un-tagging photos, and creating multiple accounts to circumvent Facebook's default privacy settings (Goldie 2010). According to a study conducted on users in America's Carnegie Mellon University, 90.8% of users had uploaded their photos in their profiles on Facebook, 87.8%, their date of birth, and 39.9% of them, their current location (Ellison et al. 2007). Based on the research conducted, Table 3 classifies the factors contributing to privacy concerns.

As shown in the research presented in this section, various factors affect the privacy concerns of users and users have different reactions toward protecting their privacy. This research focuses specifically on the types of privacy settings that users can change. Table 3 shows the classification of research based on the factors studied in each of the above studies.

3 Discussion

Privacy preservation is one of the major challenges in social networks. Many researchers have considered privacy preservation and have tried to provide different architectures in these networks for improving the privacy of users. In most proposed schemes, meeting the requirements of user privacy is the main goal; these requirements include confidentiality of data and social relationships; access control mechanisms

Table 3 Classification of research which focused on the factors affecting of users' privacy concerns (including privacy risk, information control subjective norm, privacy concern, trust, demographic characteristics, and type of data) in social networks

	Privacy risk	Information control	Information sensitivity	Subjective Norm	Privacy concern	Trust	Privacy policy	Demographic characteristics					Type of shared data
								Gender	Age	Life style	Internet skills	Time and type of social network used	
Gross and Acquisti (2005, 2006)	–	–	–	–	–	–	–	–	✓	–	–	–	–
Ellison et al. (2007)	–	–	–	–	–	–	–	–	✓	–	–	–	–
Lampe et al. (2008)	–	–	–	–	–	–	–	–	✓	–	–	–	–
Boyd and Hargittai (2010)	–	–	–	–	–	–	–	–	✓	–	✓	✓	–
Fogel and Nehmad (2009)	✓	–	–	–	✓	✓	-	✓	✓	–	–	–	–
Stutzman and Duffield (2010)	–	–	–	–	–	–	–	✓	–	–	–	–	✓
Kaufman et al. (2008)	–	–	–	–	–	–	–	✓	–	–	–	–	✓
Gilbert et al. (2008)	–	–	–	–	–	–	–	✓	-	✓	–	–	✓
Wang et al. (2011)	–	–	–	–	–	–	–	✓	✓	–	–	–	✓
Culnan and Armstron (1999)	✓	–	–	–	–	✓	✓	–	–	–	–	–	–
Phelps et al. (2000)	–	✓	✓	–	✓	–	–	–	–	–	–	–	–
Sheehan and Hoy 1999	–	-	✓	–	✓	✓	✓	–	–	–	–	–	–
Phelps et al. (2001)	–	✓	–	–	✓		–	–	–	–	–	–	–
Dinev and Hart (2004)	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
Malhotra et al. (2004)	✓	✓	✓	–	✓	✓	✓	–	–	–	–	–	-
Chellappa and Sin (2005)	–	–	–	-	✓	✓	-	–	–	–	–	–	–
Dwyer et al. (2007)	–	–	–	✓	✓	✓	–	–	–	–	–	–	–
Hui et al. (2007)	–	–	–	✓	✓	✓	–	–	–	–	–	–	–
Xu et al. (2008)	✓	✓	–	✓	✓		–	–	–	–	–	–	–
Xu (2009)	–	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
Xu et al. (2013)	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–

"✓" if the research investigates the factor; "–" if not including fine-grained, dynamic and flexible; and fairness in message exchange.

Studies in the field of MSNs platforms have focused on three aspects of privacy: location privacy, relation privacy, and privacy of sensitive data. In the case of users' sensitive data, given the development of information search and retrieval tools, the collection of user profile information by malicious and curious people has become very easy. Thus, users' sensitive and personal data on social networks sites are at risk. Moreover, the use of mobile phones in social networks platforms poses great risks to users' privacy, because they may incorporate valuable spatial and temporal data into the data network. Discovering the patterns of mobility of users from time and space–time series and using re-identification algorithms are another open issue that results from the constant proximity of smartphones to users. The use of anonymization methods, if the uniqueness of the data is minimized, can partly overcome this problem.

Regarding the methods that are provided to ensure location privacy, it should also be noted that hiding or removing location updates is not adequate for meeting the requirements of privacy protection. This is especially serious when friendship relationships are known among users.

Consideration of relation privacy in the research on MSNs is important, because user–social relations are different with different friends. It could even be the case that a user has multiple social relations with a given friend. Therefore, preserving the privacy of social relationships and preventing the disclosure of social information are very important. Thus, the mere existence of a relationship between users on social networks is not sufficient to reveal the user account information. Moreover, based on the complex nature of social relations, users may want to share their data in more complex social relationships. These relations can be obtained by combining the existing social relations. Under current conditions and with existing models, since fine-grained, flexible, and dynamic access control has not been fully implemented, it is not possible to build and manage complex user relationships with friends; we still need a model that can seamlessly guarantee access control capabilities.

In OSNs, confidentiality, access control, and data availability are among the issues that have been considered in the proposed methods. Users' needs to maintain data confidentiality against social networks service providers and non-friends and to maintain the confidentiality of social relations are the basic requirements of privacy. Great efforts have been made to protect such information. Nevertheless, this challenge remains as an unresolved problem among users of social networks.

Hence, considering different levels of user access control in privacy schemes is important. As in MSNs, users of OSNs need to have different levels of access control on their data and social relationships. However, providing a plan that can simultaneously cover various aspects of access control is difficult, especially considering time and computational complexity. It is also necessary to pay more attention to the availability of and confidence in the data storage site in the social network.

In both online and mobile social networks, schemes can be categorized into commercial and academic types. The commercial type focuses on the design of privacy settings and is more practical and realistic. However, the focus of academic research is on theory, rather than practical aspects.

Independent of social network type, using social networks services requires acceptance of the agreement by users. There are also challenges with the agreement and its contents. In some cases, the agreement itself can cause privacy violations. The agreement between the user and the service provider is unilateral and, in most cases, benefits the social network provider. In the face of this agreement, users have two options: 1—accepting it without any comments and becoming a member of a social network or 2—not entering the social networks space. In most cases, the first option is chosen and users accept the agreement. On most occasions, they accept the agreement without even reading it. Acceptance of the agreement by users, thereby granting ownership rights of user data to social network providers, can lead to the transfer of data access control from users to social network providers. The data control by the social network provider can violate users' privacy. Although ownership of user data, according to the agreement, is awarded to the social network provider, the responsibility of privacy preservation ultimately rests with the user. It seems that this duality can be controlled only by the existence of a reliable service provider. The issue of trust is another issue that has its own challenges. In addition, a lack of proper facilities for defining the authorized audience to access shared data can lead to privacy issues for social network users. This is because users cannot have full control over shared data in the flow of information on social networks. Although social network providers have tried to provide embedded privacy settings on social networks, these settings are not adequate for protecting users' privacy. Despite these settings, unauthorized users are still able to access much information.

Since privacy is a multidimensional concept and largely depends on the user, in social networks, it is necessary to add a section that considers user comments about the privatization of privacy. Although privacy settings on social networks sites are important for this requirement, in designing this section, it seems that factors affecting users' concerns about privacy breaches are not considered. Age, gender, social influence, occupation, religious beliefs, and social relations are among the parameters that affect the type and extent of changes to the privacy settings. In addition, a warning system in the case that default settings are not changed can encourage users to change their privacy settings. Informing users of any new policy by the social networks service provider is also effective in creating a sense of trust.

The concept of fairness in social networks is a new concept that needs more research. Since the need for collaboration between nodes in social network is inevitable, therefore, the creation of fairness is vital. Moreover, finding the point of trade-off between fairness and efficiency is essential.

4 Conclusion

Social networks have introduced new social communication methods. In terms of platform type, social networks can be divided into two categories: online and mobile. Each of these two categories, in terms of the type of architecture and service, may be centralized or decentralized. In centralized social networks, there are two major components: the server and the client. The social network service provider assumes the role of the server and the user assumes the role of the client. In these types of networks, the most important activities are the responsibility of the server and there is usually complete confidence in the server. In addition, full control over user data is an integral part of this kind of social network. In contrast, in decentralized social networks, the focus is transferred from the service provider to one or more other components. These components may be users or trusted third parties. In this way, the issue of trust in decentralized social networks seems to be less challenging than in centralized ones.

The increase in the number of mobile devices has enabled users to be ubiquitously connected through wireless and mobile communications technologies. On the other hand, easy access to online social networking sites has led to the growing popularity of social networks by users. Integrating social aspects of users in such networks has led to many challenges in terms of safety issues, in particular the privacy of users. Given that users have different sensitivity to the types of data that they share on these networks, and therefore, the classification of proposed schemes to protect user data with the purpose of privacy is one of the contributions of this paper. Specifically, schemes that focus on protecting sensitive data, user relationships, and users' location data are categorized. In addition, a clear classification of the types of architectures provided on any of the mobile and online social networks is another essential aspect of this research. Discussing about the proposed scheme on different architectures and the direction of future research which focusing on privacy challenges that are still open is also under consideration. In particular, this classification includes aspects of access control, confidentiality, and accessibility. In addition, one of the goals of this paper is to investigate the factors affecting on privacy concerns. Finding the most optimal trade-off between these factors and efficiency is vital in MSNs and OSNs, but unfortunately, not much has been done in this area.

To date, several models have been proposed for protecting users' privacy. Each of them focuses on one or more user needs. The basic needs of users for ensuring their privacy are confidentiality, access control, and fairness when exchanging information in the network environment.

For the preservation of confidentiality, there must be a guarantee that both user data and their social relationships are well protected. The components that may violate confidentiality include the social network service provider and non-friend users. The current models that focus on confidentiality are usually based on one of the following methods: obfuscation, encryption, anonymity, key management, and dynamic pseudonymity. Encryption methods, due to the need to use multiplication and exponentiation operations, usually have high computational overhead and high memory complexity; in some cases, there is a compromise between the degree of confidentiality and these parameters. In anonymity methods, the use of re-identification algorithms and discovery of the mobility patterns of users can place confidentiality at risk, because, according to time and place data series, one can discover sensitive user data and social relationships. Thus, anonymity should minimize the uniqueness of user data to complicate the discovery of the relationships and data of a particular user.

In term of access control, users as data owners must be able to control and manage access to their data. This means that only the data owner should have the ability to grant access to data to other audiences. In addition, given that the social relationships of users vary at different times, the user must be able to update and make changes to his relationships at any time. The models that support fine-grained, flexible, and dynamic access control can respond to this need. Computational overhead, time complexity, and the need for secure storage are issues that require compromise when meeting these requirements.

References

Abbas F, Rajput U, Wan J, Eun H, Oh H (2016) Say Hello Again: Privacy Preserving Matchmaking Using Cloud in Encounter Based Mobile Social Networks. In: Proceeding in: 16th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing

Acquisti A, Gross R (2006) Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: 6th Workshop on Privacy Enhancing Technologies, pp 36–58

Afifty Y (2008) Access control in a peer-to-peer social network. Master Thesis, EPFL, Lausanne, Switzerland

Aiello ML, Ruffo G (2012) LotusNet:Tunable privacy for distributed online social network services. Elsevier J Comput Commun 35(1):75–88

Ardagna CA, Jajodia S, Samarati P, Stavrou A (2013) Providing users' anonymity in mobile hybrid networks. ACM Trans Internet Technol 12(3):1–33

Baden R, Bender A, Spring N, Bhattacharjee B, Starin D (2009) Persona: an online social network with user defined privacy, and scholarship. In: proceeding of ACM Conference on Special Interest Group On Data Communications (ACM SIGCOMM), pp 135–146

Barnes J (1954) Class and Committees in a Norwegian Island Parish. Human Relations

Beach A, Gartrell M, Han R (2009) Solutions to security and privacy issues in mobile social networking. In: Proc. Int. Conf. CSE, pp 1036–1042

Besmer A, Lipford H (2009) Tagged photos: concerns, perceptions, and protections. In: Proceedings of CHI2009 extended abstract, pp 4585–4590

Blum M (1983) How to exchange (secret) keys. ACM Trans Comput Syst 1(2):175–193

Boyd D, Ellison N (2007) Social network sites: definition, history, and scholarship. J Comput Mediat Commun 13(1): 210–230

Boyd D, Hargittai E (2010) Facebook privacy settings: who cares? First Mond 15(8):479–500

Buchegger S, Datta A (2009) A case for P2P infrastructure for social networks- opportunities & challengers. In: Proceeding of the 6th International Conference on Wireless On-Demand Network Systems and Services (WONS), pp 161–168

Buchegger S, Vu Lh, Datta A (2009) PeerSoN: P2P Social Networking Early Experiences and Insights. In: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, pp 46–52

Challal Y (2005) Group key management protocols: a novel taxonomy. Int J Inf Theory 2(2):105–118

Chang W, Wu J, Tan C (2011) Friendship-based location privacy in mobile social networks. Int J Secur Netw 6(4):226–236

Chao S, Dongyu A (2013) Survey of location privacy. http://students.csci.unt.edu/da0097/

Chellappa RK, Sin R (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf Technol Manag 6(2):181–202

Cheng W, Aritsugi M (2014) A user sensitive privacy-preserving location sharing system in mobile social networks. Proc Proc Comput Sci 35:1692–1701

Chin A, Zhang D (eds) (2013) Mobile social networking an innovative approach. In: computational social sciences. Springer, New York, pp 112–113

Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ Sci 10(1):104–115

Cutillo LA, Molva R, Strufe T (2009) Safebook: feasibility of transitive cooperation for privacy on a decentralized social network. In: Proc. IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks and Workshops (WoWMoM), Kos, Greece, pp 94–101

da Silva PM, Dias J (2017) Manuel RicardoMistrustful P2P: deterministic privacy-preserving P2P file sharing model to hide user content interests in untrusted peer-to-peer networks. Comput Netw. https://doi.org/10.1016/j.comnet.2017.04.005

De Cristofaro E, Soriente C, Tsudik G, Williams A (2012) Hummingbird: privacy at the time of twitter. In: proceeding of IEEE Symposium on Security and Privacy, pp 285–299

De Capitani di vimercati S, Foresti S, Livraga G, Samarati P (2012) Data privacy: definitions and techniques. Int J Uncertain Fuzziness Knowl Based Syst 20(06): 793–817

De Montjoye YA, Hildalgo CA, Verleysen M, Blondel VD (2013) unique in the crowed: the privacy bounds of human mobility. Sci Rep. https://doi.org/10.1038/srep01376

DefrawyKEl,SolisJ, Tsudik G,"Leveraging social contacts for message confidentiality in delay tolerant networks. In: Proc. IEEECOMPSAC, 2009, pp. 271–279

Dinev T, Hart P (2004) Privacy concerns and Internet use—a model of trade-off factors. In: Paper read at Working Paper, Department of Information Technology and Operations Management at Florida Atlantic University

Ding X, Zhang L, Wan Zh, Gu M (2010) A brief survey on deanonmyzation attacks in online social networks: proceeding of International Conference on Computational Aspects Of Social Networks (CASoN), China 611–615

Dóra L, Holczer T (2010) Hide-and-Lie: Enhancing application-level privacy in opportunistic networks. In: Proc. MobiOpp, pp 135–142

Dramitinos M, Vannier R, Lassous IG 2009 A performance evaluation framework for fair solutions in ad hoc networks. In: Proc. ACM MSWiM, 2009, pp 46–53

Duckham M, Kulik L (2005) A formal model of obfuscation and negotiation for location privacy. In: Proc. Pervasive, pp 152–170

Dwyer C, Hiltz SR, Passerini K (2007).Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. In: Paper read at the Thirteenth Americas Conference on Information Systems, at Keystone, Colorado

Ellison N, Steinfield C, Lampe C (2007) The benefits of facebook "Friends": social capital and college students' use of online social network sites. J Comput Mediat Commun 12(4):1143–1168

European Commission (2012a) The Directive of the European Parliament and of the Council of 24 October 1995 review 2012 MEMO/12/41. http://europa.eu/rapid/press-releaseMEMO-12-41en.pdf

European Commission (2012b) The Directive of the European Parliament and of the Council of 24 October 1995 review 2012 Regulation Council of the European Parliament. document/review2012/com. http://ec.europa.eu/justice/data-protection/2012_11_en.pdf

European Council (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EuropeanCommunities, 23 November 1995, L 281/31, Available at. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Facebook Privacy Policy (2017) Facebook Privacy Policy (2017). April 2017 Available at http://facebook.com/policy.php. Accessed Apr 2017

Facebook statement of right and responsibilities (2017) acebook statement of right and responsibilities (2017) April 2017. Available athttp://facebook.com/terms.php. Accessed Apr 2017

Feng B, Deng RH, Wenbo M (1998) Efficient and practical fair exchange protocols with off-line TTP. In: Proc. IEEE Symp. Security Privacy, pp 77–85

Fogel J, Nehmad E (2009) Internet social network communities: Risk taking, trust, and privacy concerns. Comput Hum Behav 25(1):160–153

Fu Y, Wang Y, Peng W (2014) Common Finder: a decentralized and privacy-preserving common-friend measurement method for the distributed online social networks. Comput Netw 64:369–389. https://doi.org/10.1016/j.comnet.2014.02.020

Gedik B, Ling L (2008) Protecting location privacy with personalized k-anonymity: architecture and algorithms. IEEE Trans Mobile Comput 7(1):1–18

Gilbert E, Karahalios K, Sandvig C (2008) The network in the garden: an empirical analysis of social media in rural life. In: Proceeding of CHI2008, pp 1603–1612

Goldie KR (2010) Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. First Mond 15(1):1–4

Gongjun Y, Olariu S, Weigle MC (2009) Providing location security in vehicular ad hoc networks. IEEE Wireless Commun 16(6):48–55

Google pluse (2017) Google pluse Pages Additional Terms of Service (2017). April 2017 Available at https://www.google.com/intl/en/+/policy/pagesterm.html. Accessed Apr 2017

Google Privacy Policy (2017) https://www.google.com/intl/en/+/policies/privacy/. Accessed Apr 2017

Graf K, Gross Ch, Stingl D, Hartung D, Kovacevic A, Steinmetz R (2011) Life Social. KOM: a Secure and P2P-based solution for online social networks. In: Proceeding of the IEEE Consumer Communications and Networking Conference (CCNC), pp 554–558

Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Paper read at the 2005 ACM Workshop on Privacy in the Electronic Society

Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. International Conference on Mobile Systems, Applications, and Services. 31–42

Guha S, Tang K, Francis PP (2008) NOYB: privacy in online social networks. In: First Workshop on Online Social Networks (WOSP'08), pp 210–230

Ho E, Lasch S, podolsky A, The Next Digital Divide: online Social Network Privacy. Center for study commercial Activities Research Report, 2008

Hui K-L, Teo HH, Lee S-YT (2007) The value of privacy assurance: an exploratory field experiment. Manag Inf Syst Q 31(1):19–33

Jahid S, Mittal P, Borisov N (2011) EASiER: encryption-based access control in social networks with efficient revocation. In: Proceeding of the 6th ACM Symposium on Information, Computer and Communications Security, China, 411–415

Jahid S, Nilizadeh Sh, Mittal P, Borisov N, Kapadia A (2012) DECENT: a decentralized architecture for enforcing privacy in online social networks. In: Proceeding of the 4th IEEE International Workshop on Security and Social Networking, (SESOC'12),326–332

Joinson AN (2008)Looking at, looking up or keeping up with people?: motives and use of Facebook. In: Proceeding of CHI 2008, pp 1027–1036

Kaufman J, Christakis N, Lewis K (2008) The taste for privacy: An analysis of college student privacy settings in an online social network. J Comput Mediat Commun 14(1):79–100

Kayastha N, Niyato D, Wang P, Hossain E (2011) Applications, architectures, and protocol design issues for mobile social networks: a survey. In: Proc. IEEE, 99(12) 2130–2158

Krishnamurithy B, Wills EC (2008) Characterectizing Privacy in Social Networks. In: Proceedings of the First Workshop on Online Social Networks, pp 37–42

Lampe C, Ellison NB, Steinfield C (2008) Changes in use and perception of Facebook. In: Proceedings of SCW2008, 721–730

Lehikoinen JT, Olsson T, Toivola H (2008). Privacy regulation in online social interaction. In: Paper read at ICT, Society and Human Beings 2008

Li M, Ning C, Shucheng Y, Wenjing L (2011) FindU: privacy-preserving personal profile matching in mobile social networks. In: Proc. IEEE INFOCOM, pp 2435–2443

Liang X, Li X, Luan TH, Lu R, Lin X, Shen X (2012) Morality-driven data forwarding with privacy preservation in mobile social networks. IEEE Trans Veh Technol 61(7):3209–3222

Lucas MM, Borisov N (2008) Flybynight: mitigating the privacy risks of social networking. In: WPES 2008: Proceedings of the 7th ACM workshop on Privacy in the electronic society, ACM, New York, pp 1–8

Luo B, Lee D (2009) On protecting private information in social networks: a proposal. In: Proceeding of IEEE International-Conference on Data Engineering, pp 1603–1606

Luo W, Xie Q, Hengartner U (2009) FaceCloak: architecture for user privacy on social networking sites. In: Proceeding of IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-09), Canada, pp 26–33

Madden M, Smith A (2009) Reputation management and social media. Technical report, Pew Internet & American Life Project

Magkos E, Kotzanikolaou P, Sioutas S, Oikonomou K (2010) A distributed privacy-preserving scheme for location-based queries. In: Proc. IEEE WoWMoM 1–6

Malhotra NK, Kim SS, Agarwal J (2004). Internet users' information privacy concerns (IUIPC): the construct, thescale, and a causal model. Inf Syst Res 15(4): 336–355

Mani M, Ngyuen AM, Crespi N (2009) What's up: P2P spontaneous social networking. In: IEEE International Conference on Pervasive Computing and Communications (pp 1–2). Galveston: TX, USA

Milne GR, Culnan MJ (2004) Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. J Interact Mark 18(3):15–29

Mtibaa A, Harras KA, (2011) FOG: fairness in mobile opportunistic networking. In: Proc. IEEE SECON, 2011, pp 260–268

Najaflou Y, Jedari B, Xia F (2013) Safety challenges and solutions in mobile social networks. IEEE Syst J 9(3):834–854. https://doi.org/10.1109/JSYST.2013.2284696

Narendula R (2010)The case of decentralized online social networks. School of Computer and Communication Sciences, EPFL, Switzerland. https://infoscience.epfl.ch/record/174927/files/report.pdf

Narendula R, Papaioannou TG, Aberer K (2010a) Privacyaware and highly-available OSN profiles. In: Proc. WETICE

Narendula R, Papaioannou TG, Aberer K (2010b) Privacy-Aware and Highly-Available OSN Profiles. In: Proceedings of the 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, pp 211–216

Narendula R, Papaioannou G, Aberer K (2011) My3: a highly-available P2P-based online social network. In: Proceeding of the IEEE International Conference on Peer-to-Peer Computing (IEEE P2P'11), (2011), pp. 166–167

Nov O, Wattal S (2009) Social computing privacy concerns: antecedents and effects. In: Proceedings of CHI2009, pp 333–336

Paine C, Reips U-D, Stieger S, Joinson A, Buchanan T (2007) Internet users' perceptions of 'privacy concerns' and 'privacy actions'. Int J Hum Comput Stud 65:526–536

Patsakis C, Zigomitros A, Papageorgiou A, Galván-López E (2014) Distributing privacy policies over multimedia content across multiple online social networks. Comput Netw 75:531–543. https://doi.org/10.1016/j.comnet.2014.08.023

Phelps J, Nowak G, Ferrell E (2000) Privacy concerns and consumer willingness to provide personal information. J Public Policy Mark 19(1):27–41

Phelps JE, D'Souza G, Nowak GJ (2001) Antecedents and consequences of consumer privacy concerns: an empirical investigation. Journal of Interactive Marketing 15(4):2–17

Qi X, Hengartner U (2011) Privacy-preserving matchmaking for mobile social networking secure against malicious users. In: Proc. PST, pp 252–259

Raji F, Davarpanah Jazi M, Miri A (2013) DEFF: a new architecture for private online social networks. Int J Secur Commun Netw 6:1460–1470. https://doi.org/10.1002/sec.533

Raji F, Davarpanah Jazi M, Miri A (2014) PESCA: a peer-to-peer social network architecture with privacy-enabled social communication and data availability. Int J IET Inf Secur. https://doi.org/10.1049/iet-ifs.2013.0256

Schiberg D (2008) A peer-to-peer infrastructure for social networks. Disploma Thesis, Technical University Berlin, Germany

Schneier B (1996) Applied cryptography, 2nd edn. Wiley, New York

Shakimov A, Lim H, Caceress R, Cox P, Li K, Liu D, Varshavsky A (2011) Vis-vis: privacy-preserving online social networking via virtual individual servers. In: Proceeding of the 6th International Conference on Communication System and Networks (COMSNETS), pp 1–10

Sheehan KB, Hoy MG (1999) Flaming, complaining, abstaining: how online users respond to privacy concerns. J Advert 28(3):37–51

Skeels MM, Grudin J (2009) When social networks cross boundaries: a case study of workplace use of Facebook and LinkedIn. In: Proceedings of Group 2009, pp 95–104

Statista (2016) December 2016. Available at https://www.statista.com/topics/1164/socialnetworks/

Stutzman F, Kramer Duffield J (2010) Friends only: examining a privacy-enhancing behavior in facebook. In: Proceedings of CHI2010, pp 1553–1562

Sun J, Zhu X, Fang Y (2010) a privacy-preserving scheme for online social networks with efficient revocation. In: Procceding of the 29th of Information Communication (IEEE INFOCOM), pp 1–9

Tootoonchian A, Gollu K, Kiran S, Saroiu Y, Ganjali Y, Wolman A (2008) Lockr: Social Access Control for Web 2.0. In: Proceedings of the First ACM SIGCOMM Workshop on Online Social Networks (WOSN)

Tootoonchian A, Saroiu S, Ganjali Y, Wolman A (2009) Lockr: better privacy for social networks. In: Proceedings of the 5th international conference on Emerging networking experiments and technologies, Italy, pp 169–180

Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. Bull Sci Technol Soc 28(1):20–36

UN Global Pulse (2015) Mapping the risk-utility landscape: mobile data for sustainable development & humanitarian action. Global Pulse Project Series no. 18, 2015

Vastardis N, Yang K (2013) Mobile social networks: Architectures, social properties and key research challenges. IEEE Commun Surveys Tuts 15(3):1355–1371

Wang Y, Komanduri S, Giovanni Leon P (2011) I regretted the minute I pressed share: a Qualitative Study of Regrets on Facebook. In: Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA

Wang Y, Hou J, Xia Y, HZ (2015) efficient privacy preserving matchmaking for mobile social networking. Concurr Comput Pract Exp. https://doi.org/10.1002/cpe.3284

Wei C, Jie W, Tan CC (2011) Enhancing mobile social network privacy. In: IEEE GLOBECOM, pp 1–5

Wei W, Xu F, Li Q (2012) Mobishare: flexible privacy-preserving location sharing in mobile online social networks. In: IEEE INFOCOM, pp 2616–2620

Wu Y, Hui P, Xiaoying Z, Hong C, Cuiping L (2015) Publish me and protect me: personalized and flexible location privacy protection in mobile social networks. In: IEEE International Symposium on Quality of Service, IWQoS 2015, Portland, OR, USA, pp 147–152

Xiao X, Chen C, Sangaiah AK, Hu G, Ye R, Jiang Y (2017) CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2017.01.035

Xiaohui L, Xu L, Rongxing L, Xiaodong L, Xuemin S (2011) Fine-grained identification with real-time fairness in mobile social networks. In: Proc. IEEE ICC, 2011, pp. 1–5

Xu H (2009) Consumer responses to the introduction of privacy protection measures: an exploratory research framework. Int J E-Bus Res 5(2):21–47 (Special issue on the Protection of Privacy in E-Business)

Xu H, Dinev T, Smith HJ, Hart P (2008) Examining the formation of individual's information privacy concerns: toward an Integrative view. In: Paper read at 29th Annual International Conference on Information Systems (ICIS), at Paris, France

Xu F, Michael K, Chen X (2013) Factors affecting privacy disclosure on social network sites: an integrated model. Electron Commer Res 13:151–168. https://doi.org/10.1007/s10660-013-9111-6

Yang S, Wang K (2009) The influence of information sensitivity compensation on privacy concern and behavioral intention. Data Base Adv Inf Syst 40(1):38–51

Ye A, Chen Q, Xu L, Wu W (2016) The flexible and privacy-preserving proximity detection in mobile social network. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2016.12.012

Zhu Y, Hu Z, Wang H, Hu H, Ahn GJ (2010) A Collaborative framework for privacy protection in online social networks. In: Proceedings of the 6th International Conference on Collaborative Computing, USA, pp 40–45