# Privacy Policy in Decentralized Online Social Networks: Cryptography

**Jyoti**

M.C. A. dept. M.D. University Rohtak

***Abstract:*** **Decentralized Online Social Networks (DOSNs) have recently captured the interest of users because of the more control given to them over their shared contents. Indeed, most of the user privacy issues related to the centralized Online Social Network (OSN) services (such as Facebook or Google+) do not apply in the case of DOSNs because of the absence of the centralized service provider. However, these new architectures have motivated researchers to investigate new privacy solutions that allow DOSN's users to protect their contents by taking into account the decentralized nature of the DOSNs platform. In this survey, we provide a comprehensive overview of the privacy solutions adopted by currently available DOSNs, and we compare them by exploiting several criteria. After presenting the differences that existing DOSNs present in terms of provided services and architecture, we identify, for each of them, the privacy model used to define the privacy policies and the mechanisms for their management (i.e., initialization and modification of the privacy policy). In addition, we evaluate the overhead introduced by the security mechanisms adopted for privacy policy management and enforcement by discussing their advantages and drawbacks.**

***Keywords:*** **Cryptography, Privacy Policy, Decentralized Online Social Networks:**

## I. INTRODUCTION

Recent years have seen unprecedented growth in the Online Social Network (OSN) services [1], with about 300 OSNs collecting information about more than half a billion registered users.1 An OSN enables its users to define their own profiles, a virtual repre- sentation of themselves, and to explicitly declare the relationships with (the profiles of) other users. Regardless of their purpose, the main service provided by the OSNs to their users is the sharing of information with a set of selected contacts. Users can publish on their profiles very heterogeneous contents, ranging from personal information, wall posts, photos, videos, comments to other posts, and they can send private messages.

Nowadays, the most popular OSNs are based on a centralized architecture where the service provider (e.g., Facebook) acts as central authority and takes control over users' information, by stor- ing a huge amount of private and possibly sensitive information on users and their interactions (such as the personal information and lifestyle behaviors).

Due to the centralized infrastructures, users of the current OSNs are exposed to several privacy risks. Indeed, users of centralized OSNs are forced to share the information directed to their friends by means of the OSN service providers, increasing the risk of censorship, surveillance and information revelation. Indeed, recent events have shown that, in addition to malicious users (internal or external to the OSN), also the centralized service provider [2,3] and third-party applications [4] introduce new privacy risks. The National Security Agency (NSA) documents clearly illustrate how the agencies collected users' information by exploiting the weaknesses of the Facebook's security platform [3].

To address the previous privacy issues and leave to the users the control on their data, researchers have proposed to decentralize the functionalities of OSNs by implementing them in a distributed way. The resulting platforms are known as Decentralized Online Social Networks (DOSNs) [5,6] and they are typically based on a P2P architecture, such as a network of trusted servers, an oppor- tunistic network, a Distributed Hash Table, or an unstructured P2P network. For this reason, in a DOSN there is no central control au- thority which manages and maintains available the users contents. Instead, DOSNs are based on a set of peers that store the contents and execute the tasks needed to provide a seamless service (such as, search for data [7], recommendation [8], etc.).

For instance, Diaspora [9] is one of the most popular DOSNs which currently has about 669,000 users, and it is based on a network of independent, federated servers that are managed by the users. A federated network is also used by Friendica [10], another popular DOSN based on an extensible plug-in architecture, which currently has more than 1100 users. RetroShare [11], instead, is a DOSN which exploits Friend-to-Friend network to manage and to store users' data.

Therefore, DOSNs allow to shift the control over data to the end users because contents generated by the users are not stored and managed by a single OSN provider but, instead, are the users who have the control over the management of data. However, the decentralization of the service introduces several issues related to the availability of users' contents and their privacy with respect the other users of the system.

Table 1 Comparison of the security mechanisms provided by current DOSNs

| Storage | DOSN | Enc | Rep | Schema | Privacy policy |
|---|---|---|---|---|---|
| Decentralized | DECENT | ✓ | ✓ | Asymmetric, Symmetric, ABE | selected contacts, attribute-based groups |
| | LotusNet | ✓ | ✓ | Asymmetric, Symmetric | selected contacts, regular expression on content type |
| | LifeSocial.KOM | ✓ | ✓ | Asymmetric, Symmetric | private, public, selected contacts |
| | Cachet | ✓ | ✓ | Asymmetric, Symmetric, ABE | identity or attribute-based policy |
| | eXO | – | ✓ | | public, private |
| | RetroShare | ✗ | ✗ | | circles, selected groups, selected contacts, n-degree contacts |
| | PeerSoN | ✓ | ✓ | Asymmetric, Symmetric | private, public, groups |
| Semi Decentralized | Gemstone | ✓ | ✓ | Symmetric, ABE | attribute-based policy |
| | Safebook | ✓ | ✓ | Asymmetric, Symmetric | private, group, attributes, trust level, depth |
| | SuperNova | ✓ | ✓ | Asymmetric, Symmetric | private, public, selected contacts |
| | ProofBook | ✓ | ✓ | Asymmetric, Symmetric | selected contacts, group |
| | Soup | ✓ | ✓ | ABE | attribute-based policy |
| | Prometheus | ✓ | ✓ | Asymmetric | relationship type, interactions, weights of the relationship, location |
| | DiDuSoNet | ✗ | ✓ | | selected contacts, all contacts, Dunbar circles |
| | My3 | ✗ | ✓ | | trusted contacts, all friends |
| | Diaspora | ✗ | ✗ | | private, public, selected contacts |
| | Friendica | ✗ | ✗ | | public, selected groups, selected contacts |
| Hybrid | Persona | ✓ | ✓ | Asymmetric, Symmetric, ABE | private, group, selected contacts, attribute-based group |
| | SocialGate | ✓ | ✗ | Symmetric, ABE | selected contacts, attribute-based groups |
| | Vegas | ✓ | ✗ | Asymmetric | selected contacts, all friends |
| | Contrail | ✓ | ✗ | Asymmetric, Symmetric | white-list (ACL),filter based on users' identities, location, tags or<br>keywords of contents |
| | Vis-a-Vis | ✗ | ✗ | | group admission based on friendship and credentials |

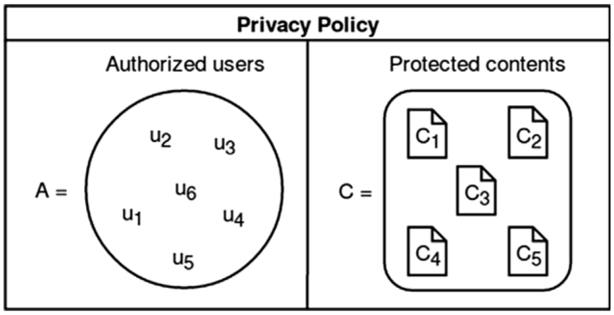

Fig. 1. The elements of a privacy policy.

## II. PRIVACY MODEL

Each DOSN enables its users to protect their contents by defin- ing privacy policies that determine the set of users authorized to access each of them. The majority of existing DOSNs, provide to the users a limited and predefined set of privacy policies based on the knowledge derived from the social network, e.g., relation- ships (friends, family, colleagues, etc.), groups, content or profile information. For instance, some DOSNs allow their users to define groups of friends, and to specify which groups are allowed to access each of the content they publish. Table 1 summarizes the access control options of current DOSNs by reporting the privacy policy type and (if the case) the encryption schemes used by each DOSN to enforce privacy policies. The most part of current DOSNs protect users' contents by employing both asymmetric and symmetric en- cryption. The details about the encryption schemes used to enforce privacy policies will be discussed in Section 5. In the following of this section, instead, we give a short description of the privacy model supported by each of the DOSNs introduced in Section 2.

Diaspora. In Diaspora [9], the users define privacy policies based on ''aspects'', i.e. groups of contacts which are part of one or more aspects of the users' life. Indeed, the ''aspects'' can be defined to reflect common features of friends (such as common interests, type of the relationships, etc.). The groups are visible only to their owners in their profiles, but the group owner can decide whether to make the identity of the group's members visible to each other.

### 4.1. Advanced privacy policy mechanisms

Besides the DOSNs previously described, there is a large collec- tion of works that propose extensions to the existing approaches.

Authors in [49] propose the D-FOAF system: a Friend of Friend ontology-based distributed identity management system for DOSNs, where access control management is provided as ad- ditional services. In D-FOAF, relationships are paired with a trust level, and users define their access control policies in terms of minimum trust level and maximum length of the paths (in terms of friendship relationships) connecting the applicant to the content owner. Authors in [50] extend the D-FOAF system by considering the case of multiple types of relationships.

On the same line of research, the authors of [51] propose Lockr: a system exploiting relationships among users within the DOSN to specify privacy policy.

Authors in [52] propose a privacy mechanism based on trust where each user has a reputation value computed by considering the ratings specified by other users in the system. In particular, each user is paired to an operating trust level that is used to de- termined contents that can be accessed by the user. The operating trust level is obtained by combining an input parameter provided by the user and the reputation value of the user. The content cre- ated by a user is paired to numeric confidence level which ranges from 0 (for contents with higher exposure) to the operating trust level of the content owner (for contents with limited exposure). Each content created by a user is encrypted with a key Kc and published on a set of trusted peers. Threshold based cryptography is used as sharing scheme between the trusted peers. The user operating at trust level τ can access the content c to the trusted peers only if the confidence level of the contents is equal or less than the operating trust level τ of the applicant.

Authors of [53,54] focused on a rule-based access control mech- anism for OSNs where authorized users are denoted in terms of the type of the relationship, the depth of the paths between two users in term of friendship relations and the trust level of the existing relationship.

Recently, Carminati et al. [55] proposed an access control model based on semantic web technologies where semantic web ontolo- gies are used to model different aspects of the online social net- work (relationship, properties of the users, relationship between users and resources, etc.).

Authors of [56,30] proposed to exploit XACML [57] (a language based on XML defined by the OASIS consortium) for defining com- plex privacy policies that leverage the knowledge provided by the DOSN (e.g., time, type of relationship, location, etc.). In addition, authors of [30] propose to exploit such privacy policies to produce smart contents allocation that meets the privacy preferences defined by users.

Typically, the systems reviewed above, exploit privacy policy languages for representing their policies. Privacy policy languages are designed to define the privacy controls that both organizations and users want to express. Privacy policy languages are expected to be fairly simple.

Instead, the authors of [58] focused on the resolution of the privacy conflicts arising from the process of data sharing. In par- ticular, users are able to specify their privacy policies to grant data access to the other users, based on their friendship relation, group membership and identity. Each user is paired to a trust level while each privacy policy for a content is paired to a sensity level, which are both of numerical values defined by the user who specifies the policy. The trust level indicates how much user trust another member while the sensity level specifies the degree of protection of the data, respectively.

The resolution of a privacy conflict aims to find an authorization decision (permit, deny) which ensure lower privacy risk and lower sharing looseness. In particular, authoriza- tion decision is computed as a function of the trust le{vel and the }sensity level of the data, and the trust level of the { ap}plicant.

## III. PRIVACY POLICY MANAGEMENT

In order to enforce privacy policies, the majority of the solutions proposed by current DOSNs are based on encryption mechanisms. Other DOSNs [42,59,29], instead, exploit alternative approaches in order to avoid the use of cryptography. In the case of cryptography-based DOSNs, encryption mech- anisms perform a data transformation in such a way that only authorized users can understand the contents. For instance, to achieve fine-grained access control, each content should be en- crypted before being stored on the peers of the DOSN. In turn, the secret key used to secure this content should be securely distributed to the users who are authorized to access the contents (see Sections 5.1 and 5.2). Consequently, even though a generic user can retrieve the encrypted content stored on a peer, only users who have the permission of the owner (i.e. the secret key) can understand it. As a result, cryptographic mechanisms used for privacy policy management introduce some overhead in terms of: number of keys created and number of encryption operations. Every time a user defines a privacy policy P (A, C ) to protect the contents in C , the DOSN must initialize it by generating the encryption data structure, e.g., the cryptographic keys, required to protect these contents, by distribute it among the proper set of user, and by encrypting these contents before being stored on the peers of the system. In addition, every time a user changes a privacy policy, the related encryption structures meant to enforce such policy must be properly updated as well to reflect the new access rights, i.e., to update the set of users allowed to access the related contents. For instance, if the privacy policy model is based on the definition of groups of users, the initialization of a policy concerns the creation of the group key and the distribution of this key to the group members. Every time the privacy policy is changed by adding a new member to the group, the DOSN must properly update the group key and redistribute it to the group members in order to ensure that both the new member and the previously authorized users can access future contents that will be published on this group. This is clearly a performance issue, especially when the set of authorized users specified in a privacy policy is large and it is frequently updated.

The cryptographic systems used by the existing DOSNs are typ- ically based on the combination of symmetric/asymmetric cryp- tography or their variations (such as Attribute Based Encryption or ABE [60]). In contrast to traditional public–private schemes, in ABE, a set of descriptive attributes is used as an identity to generate a secret key and to encrypt the data. Only the users who holds a secret key with the specified attributes are able to decrypt the data. Table 2 summarizes the general notation used to represent the key factors affecting the performance and the complexity of a secure DOSNs. In particular, we consider the overhead intro- duced by each DOSN for the enforcement of a general privacy policy P (A, C ) which grants to the set of authorized users A a1, . . . , an the permission to access the set of protected contents C c1, . . . , cm . Based on the previous analysis, we identified two different operations that can occur during the life time of privacy policies: Initialization and Update. In the following, we analyze in more detail the overhead introduced by these operations.

**Initialization**

Privacy policies P (A, C ) are defined by the content owner o in order to allow users in set A to access the contents in set C . To protect the confidentiality of the published contents, each privacy policy needs an initialization phase before being properly enforced. In general, the initialization phase concerns the creation of proper cryptographic data structures, as detailed in the following for each DOSN.

Diaspora. In Diaspora, initialization of a privacy policy does not require any additional costs because storage of data on pods is not encrypted [61]. Consequently, the pod administrator can access all the profile data hosted by the pod and all the data published by users.

## IV. EVALUATION

The previous sections surveyed some crucial aspects of current DOSNs, and this section presents a comparison among them with respect to those aspects. In particular, we analyze the privacy models provided by DOSNs and evaluate the overhead introduced for privacy policy management.

Evaluation of the privacy modelsTo help the reader in understanding the different types of privacy models provided by current DOSNs, previously described in Section 4, we propose to classify them by using the taxonomy shown in Fig. 2. In particular, we identified 4 different privacy models:

Relationship-based: where the relationships (such as friendship) established by users, as well as the features of these relation- ships, are directly exploited by the DOSN users in order to define their privacy policies.

Group-based: where users are able to organize their contacts in a set of groups, and they define their privacy policies by granting the right to access their contents to these groups.

Profile-based: where each user exploits the profile information of the other users to define their privacy policies.

Content-based: where users organize their contents in distinct groups (or types) and they exploit these groups (or types) to define privacy policies that permit access only to the specified set of contents.

As shown in Table 3, all the considered DOSNs except Diaspora, allow their users to define relationship-based privacy policies. Most of DOSNs, such as Safebook, Cachet, SocialGate, DECENT, Persona, Soup, eXO, Vegas, DiDuSoNet, Prometheus, Gemstone, allow users to organize their contacts in homogeneous groups by specifying the type of relationship (such as family, acquaintances, close friend, colleague, etc.). Then, users can state privacy policies which exploit the type of relationships. In particular, Safebook allows users to assign labels to each relationship in order to define badges, i.e., sets of contacts having the same labels.

Besides relationships type, some DOSNs enable users to provide attributes for their relationship. Such attributes are features which can be either automatically derived from the DOSN knowledge or explicitly provided by a user for each of their contacts. For example, the depth of a relationship (such as friend, friend of friend, etc.) is used by Safebook, RetroShare, Soup, and Cachet as attribute of privacy policies. The identity of a user involved in a friendship relationship (friend's identity) is another attribute of the relationships which can be easily obtained from the DOSN knowledge and it is used by PeerSoN, LotusNet, SuperNova, LifeSocial.KOM, Vis-a-Vis, Cachet, DECENT, SocialGate, Soup, Friendica, ProofBook and Vegas to de- fine privacy policies.

## V. CONCLUSION

In this paper we investigated the privacy mechanisms provided by the existing DOSNs in order to protect the privacy of the con- tents published by their users.

We selected a relevant number of DOSNs and we investigated the mechanisms they provide to allow users to express their privacy preferences, i.e., to decide which of the contents they published should be disclosed to the other users. In particular, we classified and compared the different types of supports for expressing privacy policies provided to the users to specify access rights to the contents of their profiles.

Moreover, we investigated the mechanisms adopted by these DOSNs in order to ensure that privacy policies defined by users are properly enforced. We found out that privacy policies are mainly enforced exploiting encryption, through a hybrid schema based on both symmetric and asymmetric cryptography. In addition, we observed that the security solutions exploited by DONS to enforce a privacy policy could be affected by the type of the privacy policy. As for instance, classical P2P security solutions could suffer from scalability issues if they are used for the enforcement of group- based privacy policies because the overhead introduced by encryp- tion operations in order manage very large groups.

We investigated better the above problem by measuring the overhead introduced by privacy policy management (i.e., initial- ization and modification of a privacy policy) and by comparing the performance of each approach in terms of number of crypto- graphic keys created (#Key), and number of encryption operations required (#Enc). These analyses reveal that the most expensive operations are initialization of a privacy policy and removal of a user from the set of authorized member (which mainly depends on the number of members of the group).

## References

[1]. N.B. Ellison, et al., Social network sites: Definition, history, and scholarship, J. Comput.-Mediat. Commun. 13 (1) (2007) 210–230.

[2]. M. O'Connor, Facebook Revealed Private Email Addresses Last Night, GAWKER, 2010.

[3]. G. Greenwald, E. MacAskill, NSA Prism program taps in to user data of Apple, Google and others, Guardian 7 (6) (2013) 1–43.

[4]. E. Steel, G. Fowler, Facebook in privacy breach, Wall Str. J. 18 (2010).

[5]. C.-m.A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, T. Berners-Lee, Decentraliza- tion: The future of online social networking, in: W3C Workshop on the

[6]. of Social Networking Position Papers, Vol. 2, 2009, pp. 2–7.Datta, S. Buchegger, L.-H. Vu, T. Strufe, K. Rzadca, Decentralized online social networks, in: Handbook of Social Network Technologies and Applications, Springer, 2010, pp. 349–378.

[7]. I.A. Klampanos, J.M. Jose, Searching in peer-to-peer networks, Comput. Sci. Rev. 6 (4) (2012) 161–183.

[8]. C. Selvaraj, S. Anand, A survey on security issues of reputation management systems for peer-to-peer networks, Comput. Sci. Rev. 6 (4) (2012) 145–160.

[9]. R.S.D. GRippi, M. Salzberg, I. Zhitomirskiy, DIASPORA*. https://joindiaspora. com/.

[10]. Friendica. http://friendi.ca/.

[11]. RetroShare. http://retroshare.sourceforge.net/.

[12]. B. Greschbach, G. Kreitz, S. Buchegger, The devil is in the metadata — new pri- vacy challenges in decentralised online social networks, in: 2012 IEEE Interna- tional Conference on Pervasive Computing and Communications Workshops, in: PERCOM Workshops, IEEE, 2012, pp. 333–339.

[13]. S. Rathore, P.K. Sharma, V. Loia, Y.-S. Jeong, J.H. Park, Social network security: Issues, challenges, threats, and solutions, Inform. Sci. 421 (2017) 43–69.

[14]. T. Paul, A. Famulari, T. Strufe, A survey on decentralized online social networks, Comput. Netw. 75 (2014) 437–452.

[15]. S. Taheri-Boshrooyeh, A. Küpçü, Ö. Özkasap, Security and privacy of distributed online social networks, in: 2015 IEEE 35th International Conference on Dis- tributed Computing Systems Workshops, ICDCSW, IEEE, 2015, pp. 112–119.

[16]. D. Koll, J. Li, X. Fu, The good left undone: Advances and challenges in decen- tralizing online social networks, Comput. Commun. (2017).

[17]. Sattikar, D.R. Kulkarni, A review of security and privacy issues in social networking, Int. J. Comput. Sci. Inf. Technol. 2 (6) (2011) 2784–2787.

[18]. L. Schwittmann, M. Wander, C. Boelmann, T. Weis, Privacy preservation in decentralized online social networks, IEEE Internet Comput. 18 (2) (2014) 16–23.

[19]. S.R. Chowdhury, A.R. Roy, M. Shaikh, K. Daudjee, A taxonomy of decentralized online social networks, Peer-to-Peer Netw. Appl. 8 (3) (2015) 367–383.

[20]. K. Graffi, C. Gross, D. Stingl, D. Hartung, A. Kovacevic, R. Steinmetz, LifeSocial. KOM: A secure and P2P-based solution for online social networks, in: 2011 IEEE Consumer Communications and Networking Conference, IEEE, 2011, pp. 554–558.