Analysis of Security and Privacy in Social Networks

Abstract—**The popularity of social networks has increased considerably over the past decade. According to most of the people, the ease of using these social networking web services are considered as more important than the privacy issues. On the other hand, some of the people pay attention to their personal privacy because the centralized social networking companies have a full control on these users' personal information. With the spread of this privacy concern around the world, decentralized social networking examples were beginning to emerge and they have received great support from the people who want to care about their security and privacy. The purpose of this paper is to discuss the comparison of how centralized social networks and decentralized social networks provide security and privacy properties.**

I. Introduction

With the beginning of the twenty-first century, social networks that began gaining a huge popularity, dominated the tools that people around the world use to communicate with each other. The most important point of social networks is that it enables this communication as well as the convenience it provides. According to a widely accepted definition, social networks are Internet-based services that make it possible for people to share information, by providing them with a profile to express themselves to their connections [1]. Because they serve these properties with the ease of use, the desire to use social media has begun to spread rapidly around the world in the last decade. The situation of most of these social networks that were able to reach millions in a short time proves the popularity.

On the other hand, the personal information that is being shared on such social networks is creating privacy issues. It is a fact that sharing of personal information is the responsibility of the individual itself. However, most of the users do not care about the privacy problems and continue to share their sensitive information like their home addresses without any hesitation [2]. The most important reason behind this situation is that they want others to know what is going on in their lives and most of these users cannot often realize the fact that someone outside of their connections can access this personal information with the spread of information through the circle of contacts [2]. Therefore, this issue might cause an unauthorized access to the sensitive information about the social network user. The purpose of this paper is to compare the centralized social networks with decentralized social networks according to their security and privacy properties. Based on the comparison, this paper aims to show that how centralized social networks and decentralized social networks approach personal privacy.

II. PRIVACY PROBLEMS OF SOCIAL NETWORKS

A. Centralized Social Networks

The majority of today's popularized social networks, such as Facebook, Twitter and LinkedIn, are defined as centralized social networks because they have unlimited authority at the point of reaching their users' information [1]. In a centralized social network, there is a central server that controls the whole data flow, which is consisted of sensitive personal information, and the organization stores each of the users' account in this central server [1][3]. The following figure shows the infrastructure that the centralized social networks have.

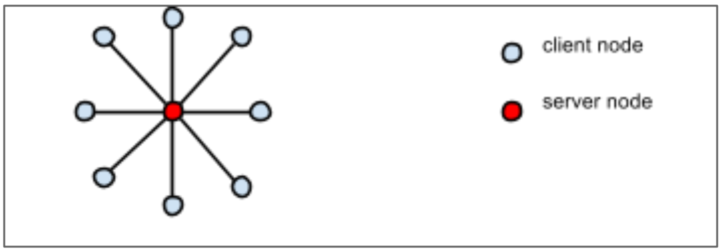

Figure 1 - Centralized Network

In centralized social networks, the right to have all this data flow causes the privacy problems for their users. People do not have much to say about how their sensitive information is used by these social network companies [1]. Most of these social networks have a business model that aims to have a large amount of personal data for using advertisement purposes, so users are rightly concerned about their personal information [4]. Because most of them achieved to get in demand and keep millions of people's personal information in their systems, they can make a good amount of money from advertising. Furthermore, besides common social media features, such as having a profile and sharing information with the connections, some of these social networks have various applications, such as music, videos and games, to attract the people and keep them inside their network [1]. As mentioned before, most of the users do not pay attention to the privacy issues on these centralized social networks and according to them it is much more important to be able to communicate easily with their connections. Social network companies such like Facebook are aware of this fact and they try to implement all of their services in this manner with an easily usable interface [1]. This attitude of the users makes these companies more popular.

B. Decentralized Social Networks

A few years after these centralized social network companies gained popularity, personal privacy concerns have begun to spread among some people who are not all the majority but sensitive to their own personal information. This has led to the emergence of decentralized social networks, such as Diaspora, GNU Social and Minds, because according to people these social networks were seen as a way to solve the privacy issues [1]. Centralized social network users have increased their confidence in these decentralized social networks and started to support them against the centralized ones, such as Facebook. In a decentralized social network, there is not any central server and it is possible that users can choose a specific server called pod for the storage of their personal data [5]. For instance, the Diaspora project is one of the most important decentralized social networking web service and they give their users the opportunity of choosing one of the pods for personal data storage. As seen in the following figure, a decentralized network consists of more than one central server nodes and they are connected to each other.

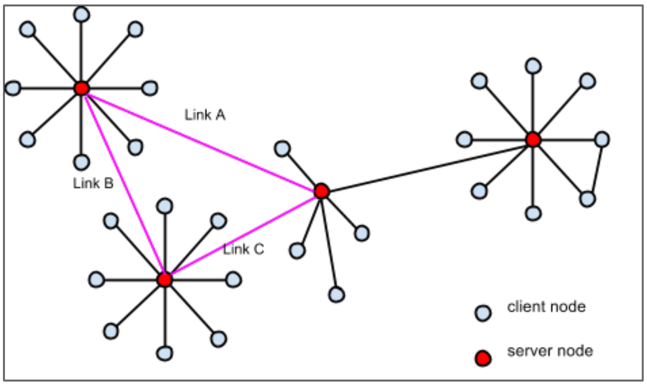

Figure 2 - Decentralized Network

The advantage of decentralized network against the centralized one is that anyone can host his own pod and each of these pods is physically located in different points [6]. Even though you have selected a specific pod, you can still communicate with users that use another pods in the network because all of these server nodes are connected to each other through the Diaspora network [6]. The right to host your own pod in the Diaspora network gives the opportunity of controlling your own data [6]. Therefore, when compared to the centralized social networking companies the decentralized ones such like Diaspora pay more attention to the privacy of their users and due to its advantages Diaspora is seen as the biggest competitor in decentralized social networking category by most of the people.

Furthermore, although the Diaspora project does not serve the property of switching to another pod, there are some decentralized social network example that users can switch to a different server provider and moving to different hosting does not prevent the system from working in a proper way, so this gives people the right to have more say on their personal privacy [5]. Even though it is not possible to talk from a system that can have complete privacy, the decentralized social networks are far ahead of centralized social networks on personal privacy.

III. SECURITY AND PRIVACY PROPERTIES OF SOCIAL NETWORKS

Due to the existence of privacy issues, both of the centralized and decentralized social network companies are trying to improve their current systems and implementing different security and privacy mechanisms to protect their users' sensitive information. Although it can be assumed that decentralized social networks are safer, as mentioned before it is not possible to talk about a completely secure web service, so these companies are also working to improve themselves. One of the most essential techniques to improve the security is cryptography. In cryptography, encryption is the operation that encodes the data and helps on preventing this data from being accessed by unwanted people, so it improves the security [7]. For instance, in order to improve the security, both of the Diaspora and Facebook use encryption technique to secure their traffics [1]. In addition to this, in Messenger, the chat application of Facebook, encryption is used to protect the data transfer [7]. Facebook also uses Hyper Text Transfer Protocol Secure (HTTS) to protect the user from malicious attacks because in case of connecting to Facebook from a public Internet network might be dangerous for users due to the possibility of adversary attack [7]. Furthermore, in case of detecting some suspicious situations, such as connecting to Facebook from different locations that are far away to each other in a short time, Facebook protects the user by showing a CAPTCHA, which aims to check whether the user is human or not [7]. Despite such security mechanisms being taken by Facebook, there is still a possible risk related with personal privacy if the user shares his physical location by using the check-in property or shares a personal photo that might have sensitive information [2]. As mentioned before, the personal information might spread to non-connected users and this might cause a dangerous situation. Additionally, although these centralized social networking companies try to improve their security properties for protection of their users' information, they have full control on their users' personal data due to the infrastructure of their system that consists of just a central server [4]. On the other hand, according to the Diaspora project community, they guarantee that they do not use any personal data of their user for any objective [6]. As discussed the details of how Diaspora works before, only the hosting provider can access to this personal information, but it is obvious that you can host your own pod or you can choose one of the pods that you want to join [6]. This leads to having more control on your own data when compared to the centralized social networking web services. Furthermore, in Diaspora project it is possible that users do not have to specify their true identity and they have a right to say on how much information they want to share, so this improves the personal privacy [6]. Moreover, as seen in the figure 2, it is more difficult to break the whole network of a decentralized social network due to the existence of many server nodes but when considering the situation of centralized social networks, the collapse of the network is entirely on the central node, which is a more risky situation [8].

IV. CONCLUSION

As discussed before, although most of the social network users prefer the ease of using the web service rather than focusing on his or her personal privacy, there are some people who care about their privacy and want to have more control on the usage of their personal data by the social networking company. After commonly hearing of the names of many centralized social networking companies, such as Facebook, Twitter and LinkedIn, by personal privacy problems, this privacy concern spread to more people over the time and this situation led to the support of decentralized social networks, such as Diaspora, GNU Social and Minds. When all the comparisons that discussed in the previous parts are evaluated, providing confidence that the social networking company will not use users' personal information is an important need for the personal privacy.

V. REFERENCES

[1] An Analysis Grid for Privacy-related Properties of Social Network Systems. (n.d.). Retrieved May 13, 2017, from http://guillaume.piolle.fr/doc/Marin13.pdf

[2] Lack of Privacy Awareness in Social Networks. (n.d.). Retrieved May 13, 2017, from https://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Lack-of-Privacy-Awareness-in-Social-Networks.aspx

[3] Introduction to Network Centralization and Decentralization. (n.d.). Retrieved May 14, 2017, from http://searchitchannel.techtarget.com/tip/Introduction-to-network-centralization-and-decentralization

[4] Social Networks and Privacy. (n.d.). Retrieved May 14, 2017, from https://www.diva-portal.org/smash/get/diva2:812449/FULLTEXT02.pdf

[5] Decentralized Social Networking, Why It Could Work. (n.d.). Retrieved May 14, 2017, from https://tech.slashdot.org/story/12/10/05/1215249/decentralized-social-networking-why-it-could-work

[6] The Diaspora Project Community. (n.d.). Retrieved May 14, 2017, from https://wiki.diasporafoundation.org/Choosing_a_pod

[7] A Review On Data Encryption Techniques Used For Social Media On Internet. (n.d.). Retrieved 14 May, 2017, from http://www.iraj.in/journal/journal_file/journal_pdf/3-299-147800265464-68.pdf

[8] Distributed versus Decentralized Networks. (n.d.). Retrieved May 14, 2017, from http://blog.cryptoiq.ca/?p=26

Figure 1 - Figure 2) Distributed versus Decentralized Networks. (n.d.). Retrieved May 14, 2017, from http://blog.cryptoiq.ca/?p=26