Towards Secure Data Sharing Processes in Online Social Networks: *Trusty*

Gulsum Akkuzu, Benjamin Aziz and Mo Adda

School of Computing, University of Portsmouth, PO1 3HE, Portsmouth, U.K.

Keywords: Web 2.0 Application, Online Social Networks, Sharing Data.

Abstract: The development of Web 2.0 has remarkably increased in today's world. These development has also been a reason for the increment of online social networks (OSNs). Web 2.0 is the roof of the online social networks since online social networks are built on Web 2.0. Users are given an environment in which they can communicate with others without considering other users locations. The way of communication in OSNs is done via sharing various contents of data, such as photos, texts, and videos. Sharing data sometimes cause privacy problems in OSNs, especially in the case that the content involves different users information on itself. Users are notified after the content is shared and they are allowed to remove tags. The content is still available in OSNs platforms, users, therefore, find a way to punish other users with being unfriend, or they quit from OSNs. However, both cases are contradictory with the main of OSNs. By considering the above issues, we develop a framework in which users' opinions are taken on data sharing process and based on the final decision, which is taken by the user who posts the content, punishing or rewarding technique is used. We also evaluate the proposed work with users interactions.

1 INTRODUCTION

The use of Web 2.0 applications have become remarkably common in our era, Web 2.0 concepts have increased the development of Web-based services, applications, and social networking sites (Harris and Rea, 2019). Online social networks (OSNs) are well-known Web 2.0 applications, since OSNs are free social networking sites with the development of the Internet (Mata and Quesada, 2014). OSNs are one of the main communication channels for people, because, OSNs provide an environment to people connect to each other regardless of their locations (Akkuzu et al., 2019c). The way of communication in OSNs environments is done via sharing contents of data, such as, photo, text, video, or event (Keijzer et al., 2018). Sharing data sometimes causes privacy issues in OSNs, this is because of the fact that people like sharing data which involves others users' information on it (Xu et al., 2018). OSNs users choose two ways to protect themselves for such privacy issues, one way to be unfriend with user, who leaks his/her privacy, the other way quit from OSNs platforms (Akkuzu et al., 2019a).

In some of the current OSNs platforms such as Facebook, users are let to remove their ids from the shared contents (Au, 2019). However, the shared content is still available which shows that removing the tag is not a solution in OSNs. Removing the tag is only available when the data is shared because people are allowed to see the content they are related when it is shared. There is no chance for people to give their opinions in data sharing process in current OSNs. In OSNs, it is a need to have a data sharing process in which users, who are related to data, are given chance to give their opinion when data is being shared. With respect to this need in OSNs, we propose a framework in this work. In the developed framework, users reputation values are used to reward or punish the user who shares the data based on his behaviours in the sharing process. In order to show the applicability of the proposed work, we implemented the proposed work with a Web 2.0 application.

The rest of the paper is structured as follows; In Section 2, we give similar works done in the web application area. We then introduce the proposed work in Section 3. In Section 4, the implementation of the proposed work with its details and the analysis on the implemented Web application are given. Finally, we conclude the paper in Section 5.

Akkuzu, G., Aziz, B. and Adda, M.
Towards Secure Data Sharing Processes in Online Social Networks: Trusty.
DOI: 10.5220/0009806304180425
In *Proceedings of the 15th International Conference on Software Technologies (ICSOFT 2020)*, pages 418-425
ISBN: 978-989-758-443-5

2 RELATED WORKS

Web 2.0 applications provide users an environment where people can produce contents and disseminate the produced content with others efficiently (Constantinides and Fountain, 2008). Web 2.0 applications are used for social networking and commercial purposes (Mata and Quesada, 2014). Social networks applications and Web 2.0 terms are frequently considered together because the Web 2.0 is a baseline for social networks (Cooke and Buckley, 2008). In the last decade, the usage of OSNs has become one of daily activities for people (Grabner-Kräuter, 2009). People have been using the OSNs platforms in order to continue their interactions with others. These communication or interaction is mostly done via sharing contents of data (Krasnova et al., 2010). Sharing data sometimes cause privacy issues in OSNs because the shared content might include other users information on itself (Akkuzu et al., 2019b).

Most of the current OSNs platforms provide the tagging feature. Tagging is specifically classified in to the multimedia content threats in (Rathore et al., 2017). Users are allowed to tag other users on OSNs' contents such as videos, and texts. This tagging feature unfortunately may cause privacy issues for other users (Rathore et al., 2017). In OSNs platforms, Although there are users who do not want to like being tagged on any contents, which is nor uploaded by themselves, some of their friends can tag them and visualise not only their photos but also display their profiles (Squicciarini et al., 2010). Another issue is that tagging may link someone who is not member of the concerned OSN platform and does not want his information being appeared in OSNs platforms (González-Manzano et al., 2014). There is also another possible scenario in which a spammer or malicious user can tag large number of users in a single post, such as a picture or video, in order to spread the malicious content to a large audience with little effort (Ahmed and Abulaish, 2013).

Recently, Facebook, which is one of the most common OSNs give users flexibility of removing the tag on the shared content. It might be considered as a solution for removing users' names on the context, however, the content is still available on other users' personal pages. Above problems and solutions are provided by research papers do not focus on having users opinions on the co-owned content data sharing process. Also they do not taken having the reputation systems into the consideration if users leak each others' privacy on co-owned data sharing processes in OSNs platforms. In order to fill this gap in the literature, this work proposes a framework which is applied on Web 2.0.

3 PROPOSED WORK

In current OSNs, each content of data has an owner who produces, uploads, or creates the content. The owner specifies the targeted group tags people and takes the decision for sharing the data. If the tagged users do not want their ids being seen on the content, then they find ways to punish the user. The punishment is either remove the tag, be unfriend with the user, or quit from OSNs platforms. The current OSNs do not have such systems which can award or punish a user when the users behaves in a certain ways. Also in the current OSNs, tagged users do not have chance to express their opinions when data is being shared. Users do not know which content of data is being shared until it is appeared in OSNs. Many OSNs users have serious problems in their lives because of the privacy leakage which is originated from tagging or sharing co-owned data (Yu et al., 2018). Quitting from OSNs is a contradictory action to OSNs platforms main aim, because OSNs are created to bring people together, connect to each other (*i.e. friendship*), and make to share contents of data (Heidemann et al., 2012). Therefore, it is important to have OSNs environments in which users should be able to express their opinions in data sharing processes when they are related to data (*this type of data called co-owned data*) and also the OSNs platforms should use a punishment and awarding system when a user behaves in a certain way in the co-owned data sharing processes. With regards to those needs in OSNs platforms, we have developed a framework which uses group decision making and users reputation values. The group decision making technique is used to allow users to express their opinions on data, which includes their ids on data (*in current OSNs it is tagging*). The reputation values are used to punish or award a user when the user takes a decision on co-owned data.

Figure 1 represents the difference between the proposed work structure and the current OSNs structure in a content of co-owned data sharing process. As it is seen in the figure, the proposed framework structure uses tagged users opinions before data is being shared while the current OSNs do not allow tagged users to give their opinions in the sharing process. The proposed framework does not allow the owner to share the content until tagged users give their opinions, it is shown in the figure with dashed lines. There are new actions which are assigned to the OSNs platforms with the proposed work, one is *"Notify the owner with the taken decision"* which refers that the system is responsible to notify the owner. The other one is *"Punish OR Award"* which refers that the system should take the responsibility for punishing or rewarding the owner based on his final decision on co-owned data. The proposed framework does not remove any of the current actions in OSNs platforms but adds new actions for the OSNs platforms in order to decrease *"Removing tags, Quitting, and Being Unfriend"*.

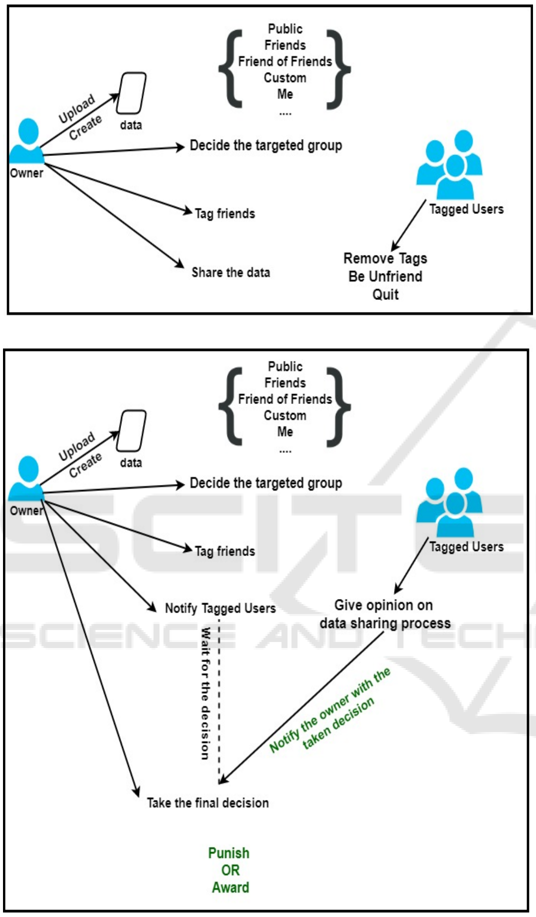


Figure 1: Current Online Social Network Structure vice versa the Proposed Social Network Structure.

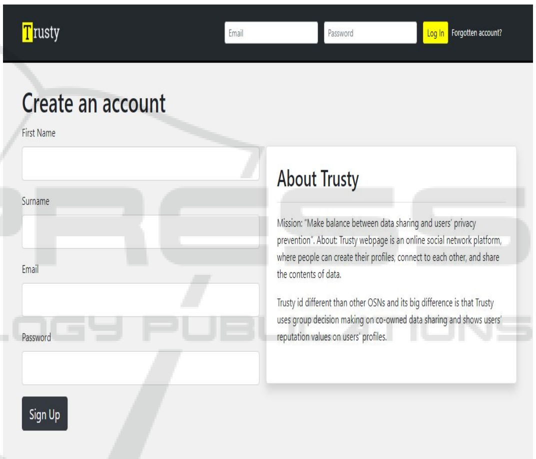
In order to show the applicability of the proposed work, we have developed an online social network named with *Trusty*. In the following section, we give the details of the *Trusty*.

4 *Trusty* SOCIAL NETWORK

Trusty is an online social network which has currently more than forty thousand users on it (visit http://www.trusty.gen.tr/). The *Trusty* aims to make a balance between data sharing and privacy protection in co-woned data sharing processes. It uses the proposed framework which is given in the previous section. The biggest difference between *Trusty* and the current OSNs is that *Trusty* assigns a reputation value to a user when a users become a member. We now give a co-owned data sharing process in *Trusty* step by step, the accounts which are used to show the steps are test accounts. That shows that there is no anonymity issue on the used accounts. The taken steps are follows;

- Create an account
- Make friends/ Search friends
- Share a co-owned content

Creating an Account: Figure 2 represent the *Trusty* main page, in order to create an account a user needs to provide his/her first name, surname, email address and password. Once the required information are provided by a users, *log-in* option is activated.



Create an account

First Name

Surname

Email

Password

About Trusty

Mission: "Make balance between data sharing and users' privacy prevention". About: Trusty webpage is an online social network platform, where people can create their profiles, connect to each other, and share the contents of data.

Trusty id different than other OSNs and its big difference is that Trusty uses group decision making on co-owned data sharing and shows users' reputation values on users' profiles.

Figure 2: *Trusty* online social network main page.

Searching Friends: Figure 3 shows the search engine in the *Trusty*. It is important to highlight that all accounts which are used in this work are test accounts.

Share a Co-woned Content: Figure 4 and Figure 5 show the process of sharing a co-owned data content. Taken steps are enumerated, first of all the owner needs to create/upload the content of data see the step *1*. Then decide who are related to the content, tag related users (co-owners) *step 2*. The number *3* shows the tagged users ids. The user should also decide the targeted group for the data. Until now, all steps are very similar to the current OSNs. The step *5* is the first difference in *Trusty* social network. In the current OSNs, after taking the previous steps users share the content of data while *Trusty* does not allow users to share the content without notifying its co-owners. In the current OSNs, there some techniques can be used

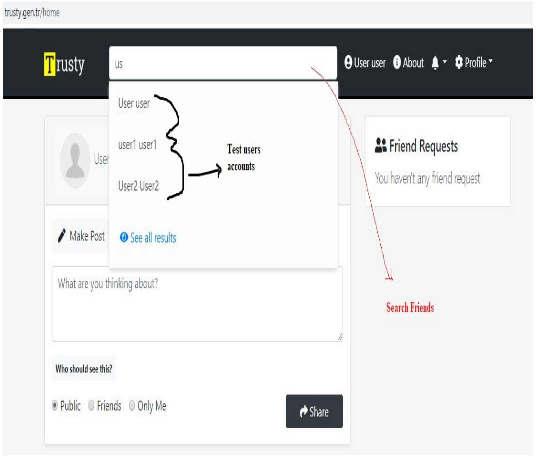


Figure 3: *Trusty* online social network search engine.

for this feature, for instance face recolonisation techniques can be used. The highlighted point in Figure 5 meets the dashed line part in Figure 1.

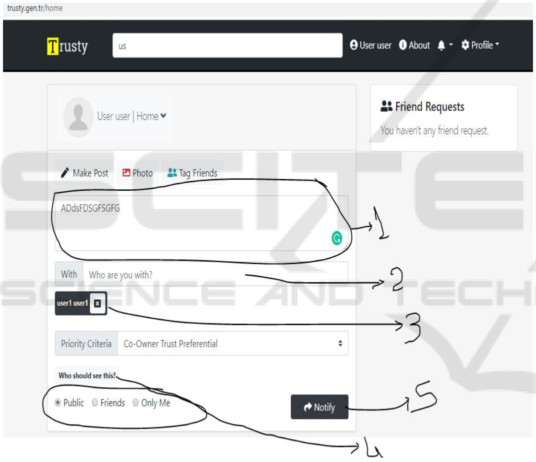


Figure 4: *Trusty* online social network co-owned data sharing steps.

After notifying the tagged users, the system is responsible to notify the co-owners. Figure 6 presents how the notification is shown on the co-owner page. Figure 7 represents the page on the owners' sides in order to take co-owners' opinions on co-owned data sharing process.

Figure 8 shows the page which gives the notification on the owner's page in order to show that co-owners take the decision. Figure 9 presents the co-owners' decision to the owner.

As it is aforementioned, every user has a reputation value on users' profiles. The reputation value is visible by any user in *Trusty* network. Figure 10 shows the user's profile with user's reputation value. The reputation value is increased by the system if the

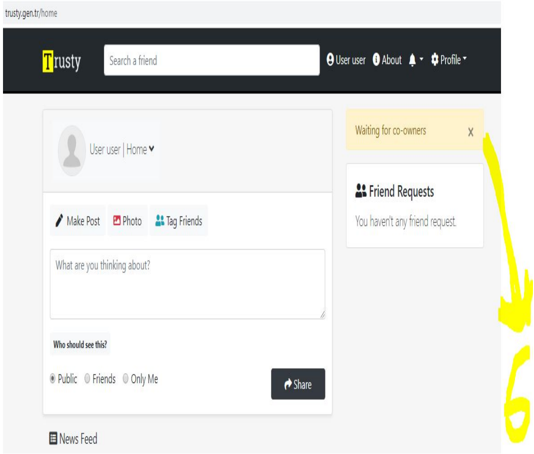
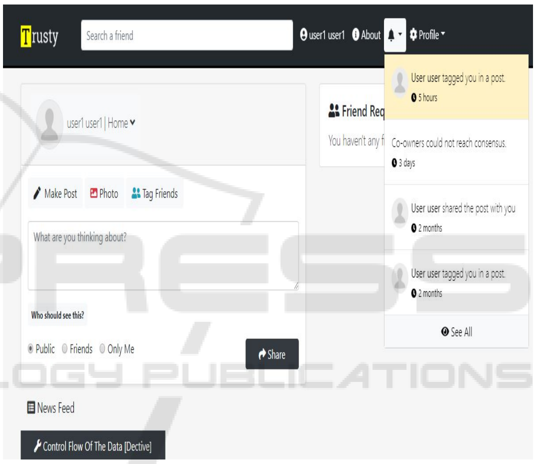


Figure 5: *Trusty* online social network waiting for co-owners opinion.



User user tagged you in a post.
5 hours

Co-owners could not reach consensus.
3 days

User user shared the post with you
2 months

User user tagged you in a post.
2 months

Figure 6: *Trusty* online social network notification on co-owners page.

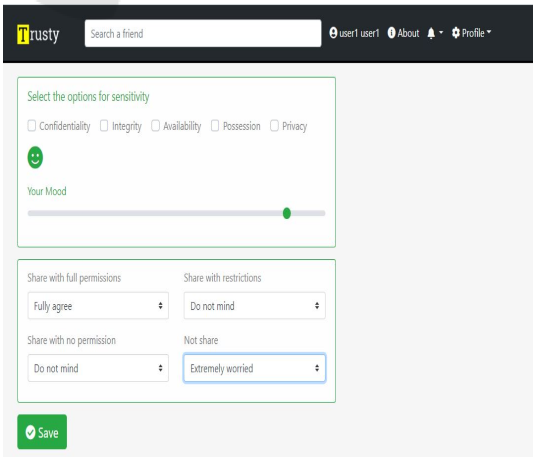
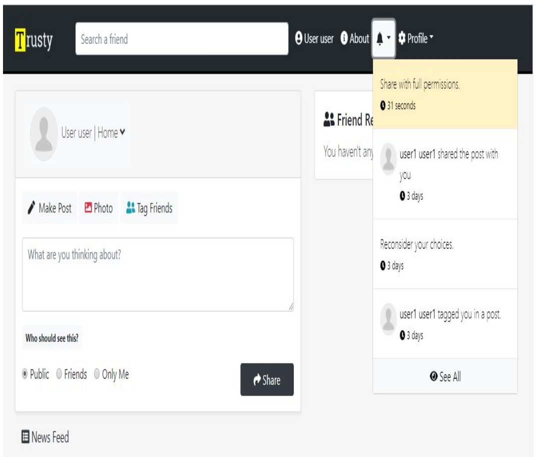


Figure 7: *Trusty* online social network asking for co-owners opinions.



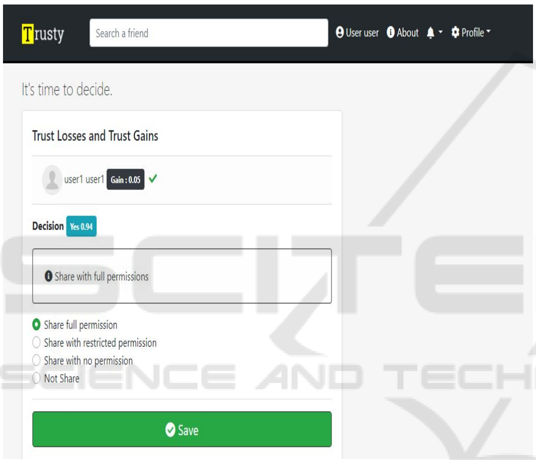
Share with full permissions.
31 seconds

user1 user1 shared the post with you
3 days

Reconsider your choices.
3 days

user1 user1 tagged you in a post.
3 days

Figure 8: *Trusty* online social network notification on the owner page.



It's time to decide.

Trust Losses and Trust Gains

user1 user1 Gain : 0.05 ✓

Decision Yes 0.94

Share with full permissions

● Share full permission
○ Share with restricted permission
○ Share with no permission
○ Not Share

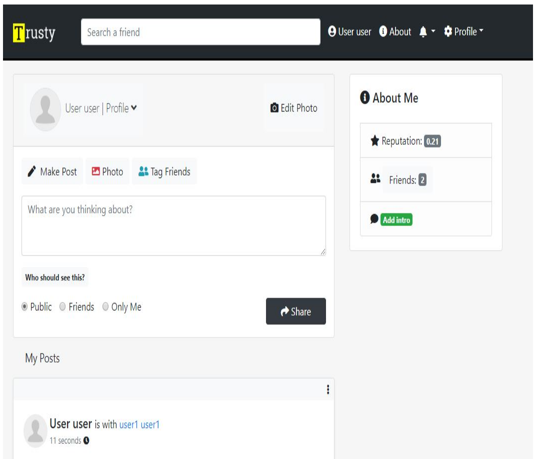
Figure 9: *Trusty* online social network notification which shows co-owners opinions.

user respects the co-owners' decision. It is decreased otherwise.

4.1 Analysis on the *Trusty*

In order to analyse the usability and the interoperability of the *Trusty* online social network, we conducted two questionnaires one for the users, who take the owner role in a co-owned data sharing process, the other one for the users, who take the co-owners role in a co-owned data sharing process. The analysis of each questionnaires are as follows; The results obtained from owner respondents are given on Figure 11, Figure 12, Figure 13, Figure 14, and Figure 15. Detailed explanations on each figure result are given below.

Figure 11 provides the results obtained from the analysis of the first question on the questionnaire



Reputation: 0.21

Friends: 2

User user is with user1 user1
11 seconds

Figure 10: *Trusty* online social network user profile with reputation.

which was completed by owners. From the results in the figure, it is apparent that *knowing co-owners' group decision* was found very useful by the majority of owners in their co-owned data sharing process.

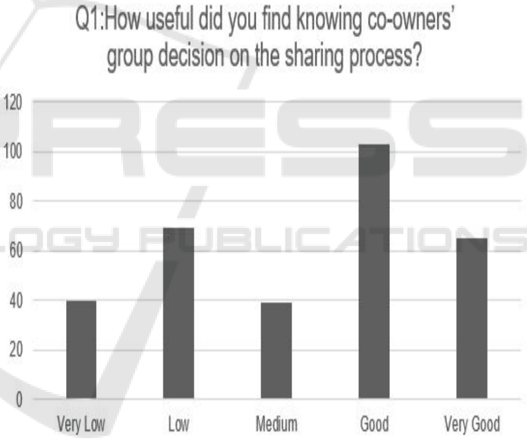


Figure 11: Evaluation on knowing group decision in co-owned data sharing process.

Owners were asked to rate *how useful did they find knowing data sensitivity value in data sharing process*, Figure 12 indicates the results of respondents on the question. There was a significant number of owners found knowing the sensitivity value useful. However, it is important to mention that there was people who did not find to know the data sensitivity value in the sharing process.

Figure 13 provides the results obtained from analysis of results on question *"How useful did you find knowing knowing the trust loss and trust gain values in each co-owner in the sharing process?"*. In the figure, the correlation between the number of choices on *Good* and the number of choices on *Low* is interesting

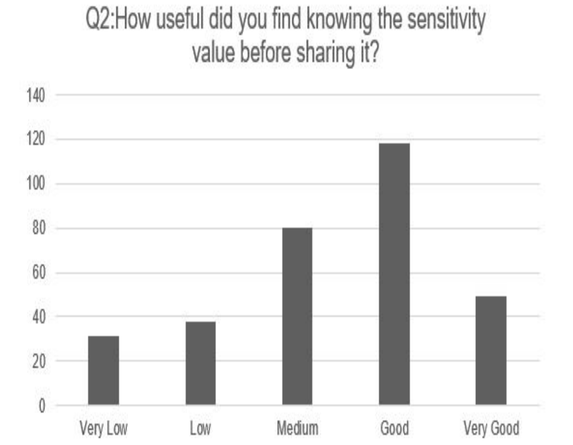


Figure 12: Evaluation on knowing co-owned data sensitivity value in sharing process.

because the difference between two choices is twenty respondents.

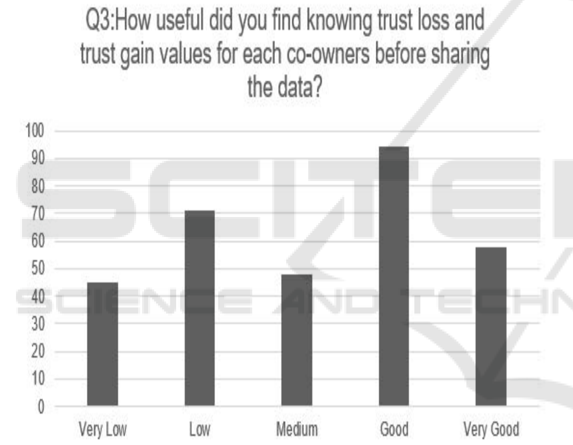


Figure 13: Evaluation on knowing trust loss and trust gain values in each co-owner.

From the result in Figure 14, it is apparent that having reputation values in online social network was found advantageous by respondents. The number of respondents, who chose *Low* option, from this figure were compared with the number of respondents in Figure 13 which shows the result for *Low* option, the comparison analysis showed that people who chose *Low* for both question were same. It can therefore be assumed that those respondents do not want to know they are punished for sharing the data.

The implementation of the developed models have been done with *Trusty* online social network, therefore, it is important to have a question which can be used to evaluate the network. Respondents were asked to evaluate *Trusty* with question *"How useful did you find the Trusty?*", of the 316 respondents who completed the questionnaire, just thirty percent of them rated the *Trusty* with *Good* option.

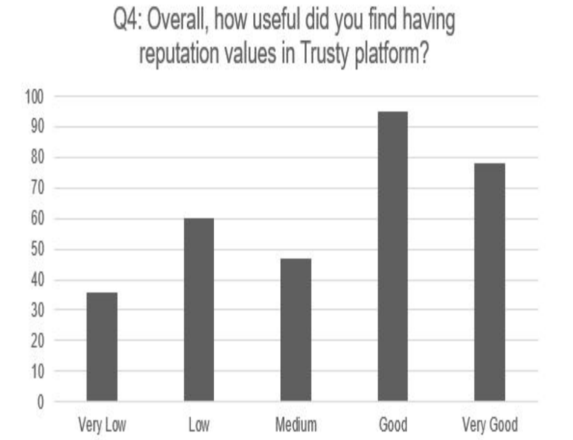


Figure 14: Evaluation on having reputation values in online social networks.

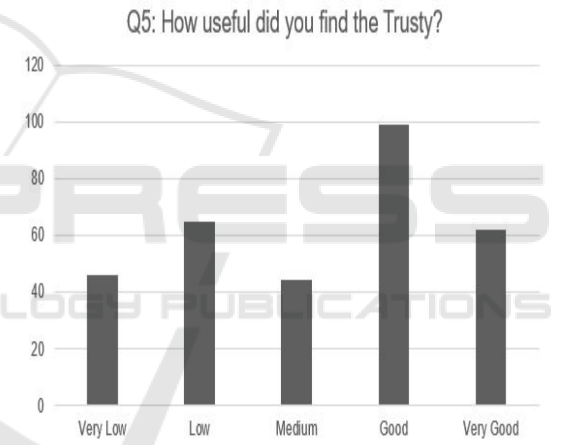


Figure 15: Overall evaluation on Trusty social network.

As it is aforementioned, two questionnaires were conducted, one was filled by data owners and the other one was filled by data co-owners. Figure 16, Figure 17, Figure 18, and Figure 19 represent the results obtained from data co-owners' answers on the questionnaire given in Appendices.

Figure 16 presents the results on the question *"How useful did you find giving your opinion on the sharing process"*, this question was developed to understand the applicability of group decision making in online social networks. Of the data co-owners giving their opinions in the sharing process, 50% rated either good or very good.

Co-owners have been given chance to give their concerns on co-owned data security features in order to decide the data sensitivity value of a co-owned data. Figure 17 presents the results on the question related

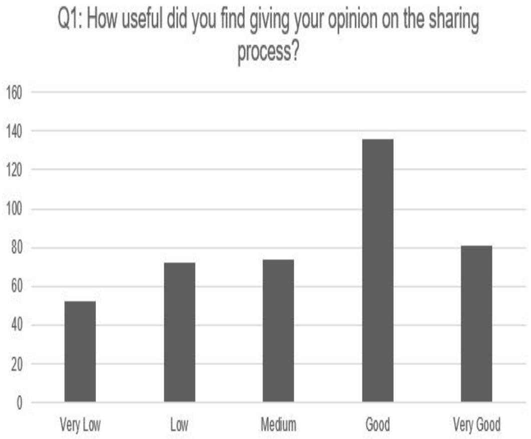


Figure 16: Evaluation of taking co-owners opinions on the sharing process.

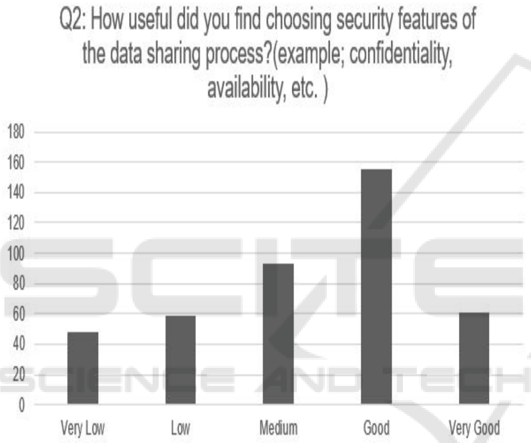


Figure 17: Evaluation on data security features.

to data security features, we can see that the majority of co-owners chose the option *Good*.

The next question was related to having reputation values in online social network platforms. This question and the next question were same on data owners' questionnaire. From Figure 18, it is apparent that having reputation values in online social networks, specifically on *Trusty*, was considerably good.

The last question on the questionnaire was about rating *Trusty* network. From the chart, it can be seen that by far the greatest choice is for *Good*.

The implementation and analysis of the proposed work have shown that it is a crucial need to use fuzzy decision systems and users reputation values in co-owned data sharing processes in OSNs. Users evaluation in the implemented work has shown that the proposed work users have positive views on the implemented models.

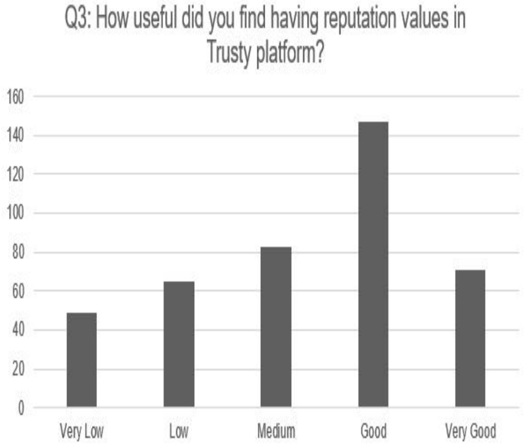


Figure 18: Evaluation of having reputation values in *Trusty*.

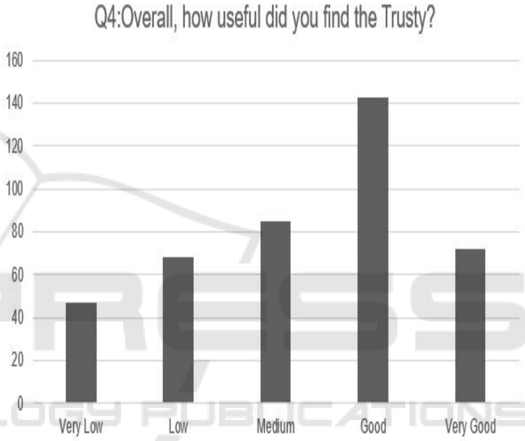


Figure 19: Overall evaluation on Trusty social network.

5 CONCLUSION

Web 2.0 applications have become remarkably common in today's world. The Web 2.0 applications and social networks terms are considered together because the Web 2.0 is a baseline for the social networks. The use of online social networks has been one of the daily activities for people. People use the online social networks for interacting others, the interaction or communication is done via sharing data in OSNs. Shared contents sometimes include more than one user id on, this type of data sharing might cause privacy problems in OSNs. In order to protect users privacy, current OSNs provide precautions such as removing tag on the shared content. However, removing tag sometimes is not enough for users. The problem here is that users are able to see the content, which includes their ids, after it is shared not in the process of sharing. In such cases, users choose either being unfriend with the user, who leaks their privacy, or quit from OSNs platforms. Both actions are contradicting with the main of OSNs because OSNs main purpose is to bring people into OSNs ans support them to be friend with others. By considering the above issues, we propose a framework which uses a punishment and rewarding system in order to encourage users to consider other users' opinions in a data sharing process. We implemented our proposed framework with a Web 2.0 application, named *Trusty* social network. We then analysed the implemented work with users evaluations. The result has shown that users want to give their opinions when the content is being shared not after it is shared. The result has also shown that using punishment and rewarding system give users satisfaction on data sharing process.

REFERENCES

Ahmed, F. and Abulaish, M. (2013). A generic statistical approach for spam detection in online social networks. *Computer Communications*, 36(10-11):1120–1129.

Akkuzu, G., Aziz, B., and Adda, M. (2019a). Advantages of having users' trust and reputation values on data sharing process in online social networks. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pages 189–195. IEEE.

Akkuzu, G., Aziz, B., and Adda, M. (2019b). Application of extended iowa operator for making group decision on co-owned contents in osns. In *10th IEEE International Conference on Intelligent Systems*. Institute of Electrical Engineers.

Akkuzu, G., Aziz, B., and Adda, M. (2019c). Fuzzy logic decision based collaborative privacy management framework for online social networks. In *3rd International Workshop on FORmal Methods for Security Engineering: ForSE*.

Au, M. Y. (2019). Removing sensitive parts of an image.

Constantinides, E. and Fountain, S. J. (2008). Web 2.0: Conceptual foundations and marketing issues. *Journal of direct, data and digital marketing practice*, 9(3):231–244.

Cooke, M. and Buckley, N. (2008). Web 2.0, social networks and the future of market research. *International Journal of Market Research*, 50(2):267–292.

González-Manzano, L., González-Tablas, A. I., de Fuentes, J. M., and Ribagorda, A. (2014). Cooped: Co-owned personal data management. *Computers & Security*, 47:41–65.

Grabner-Kräuter, S. (2009). Web 2.0 social networks: the role of trust. *Journal of business ethics*, 90(4):505–522.

Harris, A. L. and Rea, A. (2019). Web 2.0 and virtual world technologies: A growing impact on is education. *Journal of Information Systems Education*, 20(2):3.

Heidemann, J., Klier, M., and Probst, F. (2012). Online social networks: A survey of a global phenomenon. *Computer networks*, 56(18):3866–3878.

Keijzer, M. A., Mäs, M., and Flache, A. (2018). Communication in online social networks fosters cultural isolation. *Complexity*, 2018.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, 25(2):109–125.

Mata, F. J. and Quesada, A. (2014). Web 2.0, social networks and e-commerce as marketing tools. *Journal of theoretical and applied electronic commerce research*, 9(1):56–69.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., and Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information sciences*, 421:43–69.

Squicciarini, A. C., Shehab, M., and Wede, J. (2010). Privacy policies for shared content in social network sites. *The VLDB Journal*, 19(6):777–796.

Xu, L., Jiang, C., He, N., Han, Z., and Benslimane, A. (2018). Trust-based collaborative privacy management in online social networks. *IEEE Transactions on Information Forensics and Security*, 14(1):48–60.

Yu, L., Motipalli, S. M., Lee, D., Liu, P., Xu, H., Liu, Q., Tan, J., and Luo, B. (2018). My friend leaks my privacy: Modeling and analyzing privacy in social networks. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, pages 93–104.