Advantages of Having Users' Trust and Reputation Values on Data Sharing Process in Online Social Networks*

1st Gulsum Akkuzu
School of Computing
University of Portsmouth
Portsmouth, United Kingdom
gulsum.akkuzu@port.ac.uk

2rd Benjamin Aziz
School of Computing
University of Portsmouth
Portsmouth, United Kingdom
benjamin.aziz@port.ac.uk

3rd Mo Adda
School of Computing
University of Portsmouth
Portsmouth, United Kingdom
mo.adda@port.ac.uk

***Abstract*—Online Social Networks (OSNs) are quite popular platforms that have an environment where a person can contact to another person without restricting their locations. Users get in contact with each other via sharing contents of data such as videos, photos, messages, and events. Shared contents do not include always only the user's information, who uploads the content to OSNs, but also include other users' information. This type of data sharing might cause serious problems on other people's lives, the type of content is called co-owned data. Current OSNs do not have systems in which there is an enforcement system to make a balance between co-owned data sharing and protection of users' privacy. One way to make the balance is to use reputation systems on co-owned data sharing process in which OSNs' users could be punished or awarded based on their own actions on the co-owned data sharing process. In this work, we propose a reputation system where trust values, which exist between OSNs' users, are used as feedback values. The beta reputation system is used as a groundwork to develop the proposed work's models.**

***Index Terms*—the beta system, reputation, data sharing, co-owned contents, trust, online social networks.**

I. Introduction

Online social networks (OSNs) provide a digital environment for people to interact each other regardless of their locations. The communication in OSNs is based on data sharing, users post data and other users give like, dislike, or share the shared contents to express their opinions. Users sometimes share contents of data, which include not only their own information on but also have other users' information on. That type of data sharing may cause privacy leakage, in such a case, users either become unfriend with the user who leaks their information or they quit in OSNs. Being unfriend might be considered as a way to punish other user since there is no punishment that is provided by current OSNs. There is also no way to reward users if they do not leak others' information. One way to provide that needs is to have reputation values in OSNs.

The reputation is an important information that might be used to decide whether interact or not to interact with a user in OSNs [1]. The idea behind developing reputation systems in OSNs is basically to help OSNs' users to decide whom to trust, whom to be friend, whom to make their data available, and encourage OSNs users to respect other users' decisions on data sharing process. Why is important to build a reputation system for OSNs' users? To answer this question, it helps first to understand how users behave if the contents of their data are shared by other users without their permissions in OSNs. There are two way users behave, one is users quit from OSNs and the other is users become unfriend with the user, who misbehaves in OSNs, as a way to punish them. In order to encourage users keep their account in OSNs and persist friendship with other users, reputation systems are needed. Since, reputation systems seek to establish the shadow of the future to each interaction on data sharing process by creating an expectation that other people will look back on it. At an OSN, for instance, a user may have millions of friends and interact with them via data. User's friends might become unfriend with him if he misbehaves on their data, but his friends should be able to express their furiousness. Also, if the user behaves in a good way on others' data, then other users should be able to express their appreciativeness. In both ways, users behaviours will affect his future friendship actions, because, others users can decide to be/ not to be his friend or interact/ not interact with him by looking his reputation in the future. Our reputation model is grounded on the beta reputation system, which is defined in [2]. Our work aims to provide a way not to be quit from OSNs by punishing and rewarding a user based on the user's behaviours on data sharing process that includes their information on. In order to do that, the main questions of this work are as follows;

- How do users build their own reputation via sharing co-owned data in OSNs?
- What are the advantages of having reputation systems in OSNs?

II. Related Work:Reputation in Online Social Networks

Trust and reputation have been studied in different disciplines, such as psychology, sociology, philosophy and economy [3], [4]. Trust is defined in sociology and psychology as *a*

belief that appears between entities in which entities' honesty and reliability are built with their own direct experiences [5]. Reputation is measured with the collection of trustworthiness that is rated by other entities [6]. The common and simple examples to differentiate trust and reputation are *"I trust you because of your good reputation"/ "I trust you despite your bad reputation"* [6]. In real life, people make friends or business based on the trustworthiness. However, trust is not a subjective expression and it is difficult to be personalised in OSNs as it is in real life [7]. In other words, it is not easy task to quantify trust in OSNs.

According to Golbeck the definition of trust in OSNs is a factor that gives information about with whom people should share their information and from whom they should accept information [8]. Trust is the unwillingness to be vulnerable on the actions of users towards to each others in OSNs [9]. It is used either to confirm a user's identity or to ensure protection of information in OSNs [10], [11]. Trust and reputation are used for evaluating an entity's trustworthiness, therefore trust and reputation systems provide a choice to select trusted services, entities, applications, users [**?**], [12]–[16].

Trust based research studies are categorised into three classes by Sherchan *et al.* [13], namely trust information collection, trust evaluation, and trust dissemination. In their work, users' interactions are the main criteria for evaluating the trust values between users, this sense implies that the more interactions they have with each other the more trust value they gain. Caverlee et al. [17] developed the SocialTrust to support tamper resilient trust establishment in OSNs with three social parameters which are the quality of the user relationships, user behaviour, and personalised feed-backs. They use the real life trust and reputation perception, meaning that if someone's reputation is bad, then they consider that user as untrusted user. Their claim is that users' bad behaviours affect their reputation, thereby malicious users can be realised by other users with their reputation.

A research study has been proposed recently in [18], they use quantified trust value as an incentive value in which users are encouraged to be more considerate of other users' privacy when they intend to share a co-owned data. Rathore and Tripathy [19] proposed a trust based access control method that evaluates the trust values to define access conditions. In their work, trust value is assigned to users with their relationship classes; for example, if a user member of the family social group, then its trust value is assigned between 0.75 and 1, and a user can specify minimum trust level that another user needs to have to access his/her data. Another recent work has been done by Takalkar and Mahalle [20], they extend Trustbook rules to make access control policies which are applicable for multi-role environment. The common point of those works is that trust values are assigned to the accessor.

Majority of works in the literature have not studied the trust in a quantified sense except Xu et al.' work [18]. The closest work to our proposed approach is done by Xu et al. [18]. The weak points of that work are, firstly they use Boolean decision values. Secondly, they do not consider co-owners when the data sensitivity is decided.

The aim of having the reputations systems is to have an opinion about a peer's future actions by looking at its past behaviours. It is basically collects peers' experiences about peers and brings the possibility of detecting improper peers [1], [21]–[24]. In order to build the reputation models feedback of other peers about a specific peer is used as an utility function, which reflects the satisfaction of a peer experiences after using a service or consuming a product [25]. There are few studies, which has pointed the usage of the reputation in different concepts for social networks [26], [27].

III. Preliminaries

- **Owner:** It represents the user who uploads the content that includes other users information on it.
- **Co-owner:** It represents users whose information is included on the content that was uploaded by a user in OSNs.
- **Trust:** It is a number that ranges in [0,1]. It is a bidirectional variable. Each user has a trust value in other users when he becomes friends with them, and vice versa. The value of the trust is not fixed value, it changes based on users's behaviours on the data sharing, which refers other users' information.
- **Feedback:** It is considered that trust loss and trust gain values are sort of feedback values, therefore, trust loss is used as a negative feedback and trust gain is used as a positive feedback value. This value can not be seen by users, it is stored by OSN system.
- **Reputation:** It is a general value that is visible by any user, who is member of OSN. It is calculated with trust loss and trust gain values.
- **Co-owned data:** If a content of data does not include only one user's information on itself, then it is called co-owned data. In other words, the content needs be controlled by multiple users.

IV. The Proposed Model

Sharing information is an important part of life, the difficult part of the sharing process is to decide to share data with whom [28]. Because, sometimes shared information could cause profound impacts on other people's lives. In such a case people lose trust in other person who affects their life in a bad way. In this work, we assume that users have trust values in each other in OSNs and the trust values go up or down based on their actions on co-owned data sharing processes in OSNs. In other words, after each co-owned data sharing process is completed, each co-owner loses or gains trust in owner. Losing trust in a user points that the decision that was taken by the user was against to the co-owners' decisions on the data sharing process. On the other hand, gaining trust in a user shows the case that the user's decision was coherent to the co-owners' decision on the data sharing process. Therefore, trust values can be considered as feedback similar to work in [2]. The trust gain value is considered as a satisfaction, which is considered the representation of the positive feedback while

trust lose value is the representation of the dissatisfaction and thought as a negative feedback. The purpose of having trust values as a feedback value is to indicate the point that an owner's punishment or reward in a data sharing process for example the owner respects co-owners' group decision and it shows that the data sharing process is completed with the satisfaction.

Figure 1 gives a view to represent trust values among users in OSNs. When a user becomes friend with another user in ONSs, the relationship between these two users appears. In the figure, dashed lines between users represent the relationship. When users become friends with each other, trust values are automatically assigned by the system (OSNs). For instance, T_{C-A} is the presentation of User C's trust in User A and T_{A-C} shows User A's trust in User C.

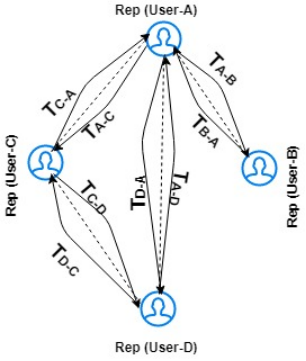

Fig. 1. A general representation of trust structure among members

Parameter *v* is the representation feedback in [2], in this work, co-owners' trust gain T_g and trust loss T_l in owner are feedback values. For instance, if co-owners lose trust in owner' then the value of *v* is trust loss T_l (negative), if not then it is trust gain T_g. The ranges of the variables' values of the model are given in Table I. The table represents the similarities of the reputation system's variables and the proposed work's variables on the reputation values [2].

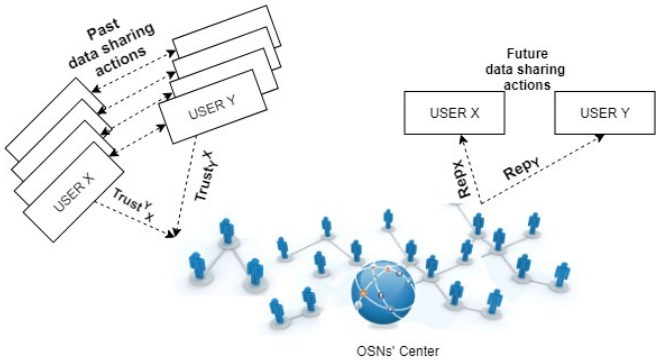

Fig. 2. Structure of feedback and reputation ratings for OSNs

A general model to calculate the reputation rating of a user in social networks area is defined by [2]. The reputation value of a user is calculated by collecting other users' feedback on

TABLE I
SIMILARITIES BETWEEN THE REPUTATION SYSTEM AND OSNS' VARIABLES

The reputation system	OSNs' Variables
feedback [-1,1]	Trust values [-1,1]
weights [0,1]	Data sensitivity [0,1]
n $\in \mathbb{N}$	n $\in \mathbb{N}$

the user, for instance, if a user was satisfied by another user's action on a buying and selling process, then hi gives a positive feedback about the user. While users express their unhappiness with negative feedback, which is defined dissatisfaction variable in [2].

Equation 1 is the model, in which the variables are adjusted with this work's scenario's variable, to calculate the reputation value of owner in OSNs.

Sd is the data sensitivity value, it is used as weight, since, the data sensitivity value is the expression of co-owners' opinion on the data security features. ${c_{co}}^o$ shows satisfaction value of a co-owner's in owner, ${d_{co}}^o$ similarly indicates dissatisfaction value of a co-owner's in owner.

$$Rep({c_{co}}^o, {d_{co}}^o) = \frac{{c_{co}}^o - {d_{co}}^o}{{c_{co}}^o + {d_{co}}^o + 2} \tag{1}$$

Model 2 is representation of a normalised form of Model 1 with satisfaction *c* and dissatisfaction *d*, respectively. $c \in [0,1]$ and $d \in [-1,0]$. The trust value can have the highest value T_g 1 when all data security features are selected by co-owners as worrisome properties, while it carries the minimum value T_l -1 when none of the data security features are selected by co-owners.

$$\begin{aligned} c &= \frac{Sd * (1 + T_g)}{2} \\ d &= \frac{Sd * (1 - T_l)}{2} \end{aligned} \tag{2}$$

We also present the behaviour of Equation 1 with changing and fixing its variables on the following figures.

$$\begin{aligned} &\boxed{\begin{aligned} c : \mathbb{R}, d : \mathbb{R} \\ Rep : cXd; \\ Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \end{aligned}} \\ &c = \frac{Sd * (1 + T_g)}{2}, \\ &d = 0, \\ &Rep(c, 0) = \frac{(n * \frac{Sd*(1+T_g)}{2})}{(n * \frac{Sd*(1+T_g)}{2}) + 2} \end{aligned} \tag{3}$$

Figure 3 indicates the changes on the reputation model with Equation 3, it is a function of the number of co-owners *n* for the data sensitivity value S_d=0, S_d=0.1, S_d=0.2, S_d=0.3,..., S_d=0.9. The data sensitivity value 1 is out of the calculation in the case, this is because if S_d is 1, then the trust gain value can not be taken into the consideration. Because it is the case

that shows all co-owners are worried about their data's all security features.

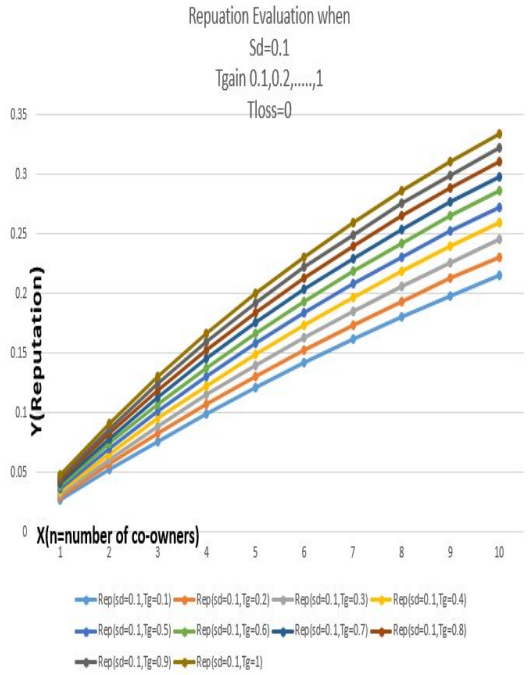

Fig. 3. Reputation evaluation with varying the data sensitivity value when there is no trust loss value

It can be clearly seen that the reputation value remains 0 when the data sensitivity value is 0, whereas, it increases rapidly when the data sensitivity value gets higher value.

$$\boxed{\begin{aligned} c : \mathbb{R}, d : \mathbb{R} \\ Rep : cXd; \\ Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \end{aligned}}$$

$$\begin{aligned} c &= 0, \\ d &= \frac{Sd * (1 + T_l)}{2}, \\ Rep(0, d) &= \frac{(-n * \frac{Sd*(1-T_l)}{2})}{(n * \frac{Sd*(1+T_l)}{2}) + 2} \end{aligned} \tag{4}$$

Figure 4 indicates the changes on the reputation model with Equation 4, it is a function of the number of co-owners n for the data sensitivity value S_d=0.1, S_d=0.2, S_d=0.3,..., S_d=0.9, S_d=1. The data sensitivity value 0 is out of the calculation in the case, this is because if S_d is 0, then the trust loss value is out since all co-owners are not worried about all the data security features. What is striking in Figure 4 is the rapid decrease on the reputation value when the data sensitivity value approaches 1.

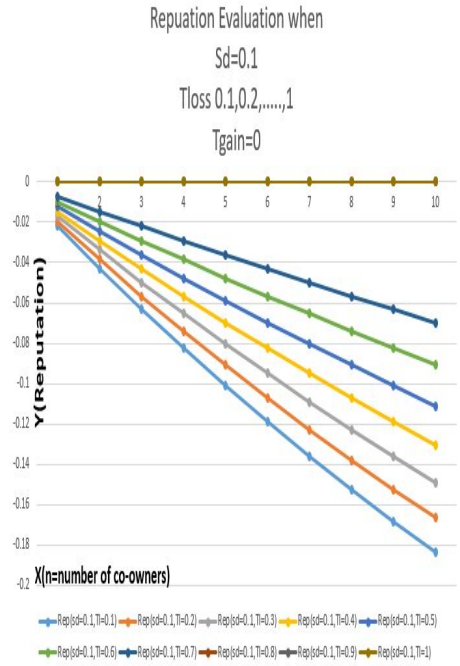

Fig. 4. Reputation evaluation with varying the data sensitivity value when there is no trust gain value

$$\boxed{\begin{aligned} c : \mathbb{R}, d : \mathbb{R} \\ Rep : cXd; \\ Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \end{aligned}}$$

$$\begin{aligned} c &= \frac{Sd * (1 + T_g)}{2}, \\ d &= \frac{Sd * (1 - T_l)}{2}, \\ Rep(c, d) &= \frac{n * (c - d)}{(n * (c + d)) + 2} \end{aligned} \tag{5}$$

Figure 5 shows the changes behaviour on the reputation with varying the trust values and fixing the data sensitivity value to 0.. The figure is generated with Equation 1 and Equation 5. It is explicitly seen that the changes on the reputation value is more stable when the data sensitivity value is fixed rather than the trust values.

Figure 3, Figure 4, and Figure 5 are just representations of the evaluations of the models. The most important feature of those figures is that if the number of co-owners increases, then the changes on the figure go up.

Figure 6 shows the fluctuations on the reputation when the data sensitivity has the high value and there is no trust gain value. In such a case, the reputation rating is decreased. Figure 7 indicates the changes on the reputation evaluation when the data sensitivity ranges in [0,1] and there is only trust gain value. In this case, the reputation rating is increased.

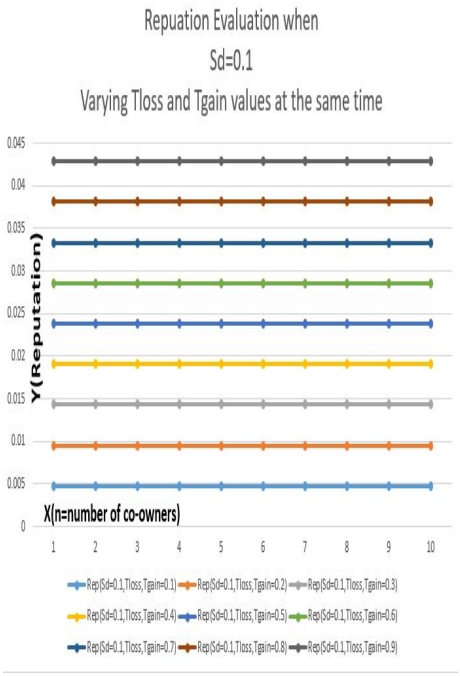

Fig. 5. Reputation evaluation with varying the trust value when the data sensitivity value is fixed to 0.5

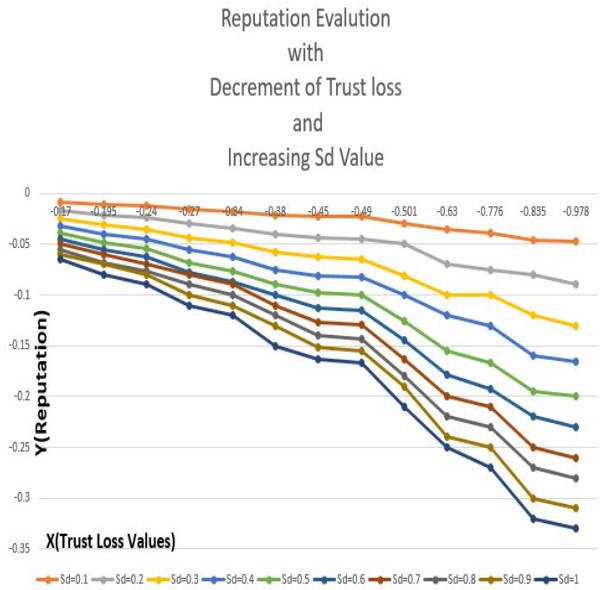

Fig. 6. Reputation evaluation with varying the trust loss and the data sensitivity value

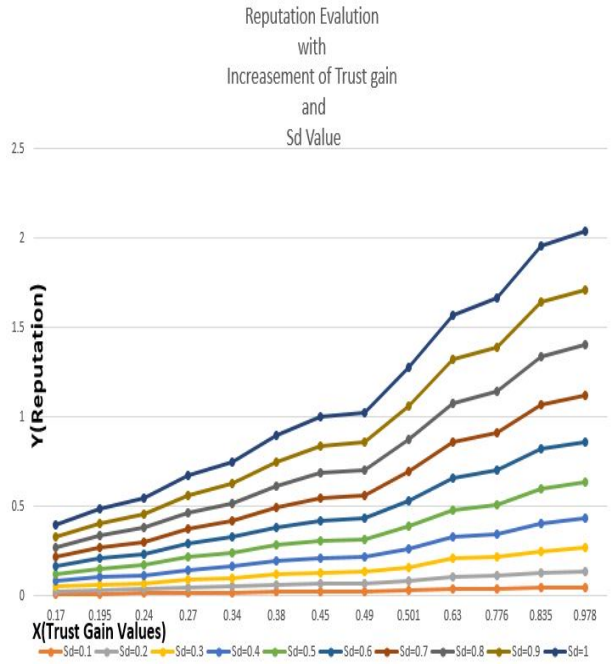

Fig. 7. Reputation evaluation with varying the trust gain and the data sensitivity value

V. Combining OSNs Decision Cases with Reputation Changes

This section shows the combination of the reputation update cases with the decision cases.

Table II indicates the conditions and cases for defining whether owner's reputation value is updated. As it can be seen on the table owner's reputation changes based on his action on the data sharing. If owner makes a decision to share the data that is congruent to co-owners' group decision, then the reputation value is increased. In contrast, if owner makes a decision to share the data that is against to co-owners' group decision, the the reputation value is decreased. In other cases and conditions, the reputation value remains.

Each OSNs' member has a reputation value that is defined in below boxes. Updating conditions for a member's reputation are given on Table II. In this work, we focus more the reputation changes when the content of data is co-owned, therefore, the member whose reputation is updated is owner of the content.

$$\boxed{Map : Member \mapsto Rep}$$

$$\boxed{Map[Member \mapsto [Map(member) + \delta(Rep_{ch}, c, d)]]}$$

$$\delta(Rep_{ch}, c, d) = \begin{cases} Rep(c, 0), & when \\ & Rep_{ch}{=}Rep_{ch1} \\ Rep(0, d), & when \\ & Rep_{ch}{=}Rep_{ch2} \\ Rep(c, d), & when \\ & Rep_{ch}{=}Rep_{ch3} \end{cases} \quad (6)$$

TABLE II
REPUTATION UPDATE RULES

Co-owners' Decision	**Owner's Action**	**Reputation Changes** Rep_{ch}
YES $\wedge$ Share with Full Permission	In any Action	Changes the Reputation Rep_{ch1}
YES $\wedge$ Share with Restricted Permission	Share with Full Permission	Changes the Reputation Rep_{ch2}
YES $\wedge$ Share with No permission	Share with Full Permission $\vee$ Share with Restricted Permission	Changes the Reputation Rep_{ch2}
Maybe $\wedge$ Share with Full Permission	In any Action	Changes the Reputation Rep_{ch1}
Maybe $\wedge$ Share with Restricted Permission	Share with Full Permission	Changes the Reputation Rep_{ch3}
Maybe $\wedge$ Share with No Permission	Share with Full Permission $\vee$ Share with Restricted Permission	Changes the Reputation Rep_{ch3}
No $\wedge$ Not Share	Share with Full Permission $\vee$ Share with Restricted Permission $\vee$ Share with No Permission	Changes the Reputation Rep_{ch2}
In all other cases	In all other cases	No changes

VI. DISCUSSION: THE ADVANTAGES OF REPUTATION SYSTEMS IN OSNS

In this work, we aim to build and implement a reputation system by using the beta reputation system ground. In order to present the applicability of the proposed reputation system, we developed Trusty network. In this section, we now present a discussion of the advantages of having reputation systems in OSNs.

The main attractive point of many online platforms is that they provide an environment in which people can have social interactions via sharing data. Users sometimes act in a particular manner to insult other users [29], for instance, users may leak other users' privacy intentionally. These types of behaviours may cause inappropriate actions in OSNs, some users may quit their accounts because of the offensive behaviours. Therefore, it is a need to develop a system, which could use punishment when users behave offensively. It is not only about the bad behaviours but also good users, who do not treat other users inappropriately, do not have any reward systems. One way to reward and punish users based on their behaviours is to have reputation systems in OSNs. If a user behaves in a good way, then the user will be rewarded by the system. Otherwise, he will be punished by the system on his reputation.

One way to decide whether users' behaviours are good or bad is co-owned data sharing process in OSNs. For instance, a user has a content of data, which has other users' information on, and wants to share it by asking other users' opinions on data sharing. We call the user with owner who upload the content, and users whose information is included on the data, are co-owners. Owner asks co-owners opinions on the sharing process, then he finalises the decision by either respecting co-owners' decisions or ignoring their opinions on the sharing process. If the owner respects the co-owners' opinions, then his behaviour is considered as a good behaviour. If he does not respect the group's decision, which was made by co-owners, then his behaviour is considered as a bad behaviour.

With the developed reputation system in OSNs, users can see other users' reputation value, which might help users to decide to be friend, interact, or trust to other user.

Users sometimes may disable their posts and that might make other users to think that the person does not have any bad behaviours or offensive shared contents since there is no evidence. Another benefit of having reputation systems in OSNs could be in this possible scenario, because, even if the user hides his posts, his reputation value can show whether the user is bad or good user. The reputation value can be used as a convincing indicator in OSNs. In short, the reputation value of OSNs' members can reflect different type of users' behaviours not only in the case of making balance between co-owned data sharing and protecting other members' privacy.

VII. CONCLUSION

Online Social Networks have become part of people daily life, they are a way for users to show themselves, connect to others, and share information with each other. Users sometimes share contents of data, which does not have only their information on, this type of data sharing may cause serious problems in others lives, or they may not be happy to see that their content is accessible by unwanted viewers. People may quit their accounts from OSNs or become unfriend with the user, who shares the content. OSNs need to use a way to keep users' accounts and also keep the friendship that exist between users. The system needs to have penalty and reward approaches that can make users satisfied end of all data sharing process, which is not related to only one user. To do so, OSNs need reputation systems to protect users information on especially co-owned data sharing process.

This work reveals a reputation system in which users' trust loss and trust gain values are used as feedback values to calculate the reputation value of a user. A user's reputation is changed based on the user's actions on co-owned data sharing

processes. In other words, if a user shares a content, which has other users information on, then the users needs other users' expressions on the sharing process. Other users' trust in the user, who shares the content, either increase or decrease at the end of process. The trust values are used as negative or positive feedback values, if the trust value decreases the it is considered as negative feedback otherwise it is considered as positive feedback.

ACKNOWLEDGMENT

We gratefully thank to the Turkey Ministry of National Education for financial support.

REFERENCES

[1] C. Jensen, J. Davis, and S. Farnham, "Finding others online: reputation systems for social online spaces," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2002, pp. 447–454.

[2] A. Josang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, 2002, pp. 2502–2511.

[3] J. Hörner, "Reputation and competition," *American economic review*, vol. 92, no. 3, pp. 644–663, 2002.

[4] V. Buskens, "The social structure of trust," *Social networks*, vol. 20, no. 3, pp. 265–289, 1998.

[5] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *null*. IEEE, 2003, p. 150.

[6] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[7] G. A. L. B. A. Hamdi, S. and S. B. Yahia, "Tison: Trust inference in trust-oriented social networks," *ACM Transactions on Information Systems (TOIS)*, vol. 34, no. 3, p. 17, May 2016. [Online]. Available: https://dl.acm.org/citation.cfm?doid=2915200.2858791

[8] J. Golbeck, "Trust on the world wide web: A survey," *Foundations and Trends in Web Science*, vol. 1 (2), 2006.

[9] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," *AMCIS 2007 proceedings*, p. 339, 2007.

[10] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," *arXiv preprint arXiv:1402.2699*, 2014.

[11] M. N. Danny, O. P. Kogeda, and J. Mtsweni, "A context-sensitive trust model for online social networking," in *Advances in Computing and Communication Engineering (ICACCE), 2016 International Conference on*. IEEE, 2016, pp. 314–319.

[12] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in *Distributed computing systems workshops, 2007. ICDCSW'07. 27th International Conference on*. IEEE, 2007, pp. 25–25.

[13] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, p. 47, 2013.

[14] M. A. Azer, S. M. El-Kassas, A. W. F. Hassan, and M. S. El-Soudani, "A survey on trust and reputation schemes in ad hoc networks," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*. IEEE, 2008, pp. 881–886.

[15] X. Yu and Z. Wang, "A enhanced trust model based on social network and online behavior analysis for recommendation," in *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*. IEEE, 2010, pp. 1–4.

[16] A. N. Joinson, C. Paine, T. Buchanan, and U.-D. Reips, "Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys," *Computers in Human Behavior*, vol. 24, no. 5, pp. 2158–2171, 2008.

[17] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: Tamper-resilient trust establishment in online communities," in *Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries*, ser. JCDL '08. New York, NY, USA: ACM, 2008, pp. 104–114. [Online]. Available: http://doi.acm.org/10.1145/1378889.1378908

[18] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48–60, 2019.

[19] N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," *Social Network Analysis and Mining*, vol. 7, no. 1, p. 7, Feb 2017. [Online]. Available: https://doi.org/10.1007/s13278-017-0425-6

[20] V. Takalkar and P. N. Mahalle, "Trust-based access control in multi-role environment of online social networks," *Wireless Personal Communications*, vol. 100, no. 2, pp. 391–399, May 2018. [Online]. Available: https://doi.org/10.1007/s11277-017-5078-2

[21] T. Hogg and L. Adamic, "Enhancing reputation mechanisms via online social networks," *EC*, vol. 4, pp. 236–237, 2004.

[22] A. Mehra, A. L. Dixon, D. J. Brass, and B. Robertson, "The social network ties of group leaders: Implications for group performance and leader reputation," *Organization science*, vol. 17, no. 1, pp. 64–79, 2006.

[23] M. M. Wasko, S. Faraj *et al.*, "Why should i share? examining social capital and knowledge contribution in electronic networks of practice." *MIS quarterly*, vol. 29, no. 1, pp. 35–57, 2005.

[24] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, "Reputation management survey," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*. IEEE, 2007, pp. 103–111.

[25] A. E. Arenas, B. Aziz, and G. C. Silaghi, "Reputation management in collaborative computing systems," *Security and Communication Networks*, vol. 3, no. 6, pp. 546–564, 2010.

[26] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48–60, 2018.

[27] S. A. Paul, L. Hong, and E. H. Chi, "Who is authoritative? understanding reputation mechanisms in quora," *arXiv preprint arXiv:1204.3724*, 2012.

[28] S. Talja and P. Hansen, "Information sharing," in *New directions in human information behavior*. Springer, 2006, pp. 113–134.

[29] A. Bruckman, P. Curtis, C. Figallo, and B. Laurel, "Approaches to managing deviant behavior in virtual communities," in *CHI Conference Companion*, 1994, pp. 183–184.