A Multi-Agent Model to Support Privacy Preserving Co-Owned Image Sharing on Social Media

Farzad N. Motlagh, Anne V.D.M. Kayem, Christoph Meinel

Abstract Privacy on online social networks is a concern, specifically in relation to sharing co-owned images. Co-owned images raise a privacy conundrum, in that enforcing privacy policies impacts negatively on performance and usability. In most existing work, this issue is addressed by requiring users from the same or overlapping friendship networks to contribute privacy opinions vis-a-vis posting the co-owned image. This poses two issues: (1) privacy posting decisions cannot be made, resulting in delay; and (2) ineffective user opinion computation necessitates large amounts of image distortion, resulting in low levels of user satisfaction. In this paper, we present a multi-agent system in which an opinion formulation algorithm computes offline user opinions based on user personality and behaviour information. Our results indicate that posting decisions take 3.81 seconds on average for offline users vis-a-vis co-owned images.

1 Introduction

Social media offers a feature-rich platform for co-owned image sharing [1, 2]. Co-owned images are ones that may have been taken by an individual, but include images of other individuals. In certain cases, however, users involved may not be aware that the picture was taken and would typically not have been consulted before the image is shared publicly. For users wanting to keep their information private, this raises a privacy a conflict [3, 4].

Farzad N. Motlagh
Hasso-Plattner-Institute, University of Potsdam, Germany, e-mail: farzad.motlagh@hpi.de

Anne V.D.M. Kayem
Hasso-Plattner-Institute, University of Potsdam, Germany, e-mail: anne.kayem@hpi.de

Christoph Meinel
Hasso-Plattner-Institute, University of Potsdam, Germany, e-mail: meinel@hpi.de

For instance, consider a scenario in which Alice wishes to upload co-owned graduation party images to her social media account. Using her privacy settings, she controls the exposure of the uploaded co-owned images so that the images are visible only to her close friends. However, one of her friends, say Bob, would have preferred to keep his presence at the graduation party secret from his employer, say John, who also happens to be in Alice's friendship network. By sharing the image without Bob's consent, Alice inadvertently puts Bob's privacy vis-a-vis his employer at risk.

Problem Statement. Most existing approaches [5, 6, 7, 8, 9, 1, 10, 11, 12] consider mainly cases in which the users involved are online and can actively provide privacy opinions vis-a-vis posting the co-owned image. What has received less attention, is the case in which the users involved may be offline for extended periods. This, however, poses two issues in terms of privacy preservation and usability, namely: (1) When users are offline, a privacy decision regarding whether or not to post the image cannot be reached, thereby resulting in delay. (2) Ineffective user opinion computation necessitates large amounts of image distortion, resulting in a low level of user satisfaction.

Contributions. In this paper, we present a multi-agent model to address both problems by handling opinions from both offline and online users. Our multi-agent model maps each user profile to an agent. An **uploader agent** acting on behalf of the user wishing to post the co-owned image, contacts the **user agents** acting on behalf of the other users who appear in the image, to reach a privacy agreement with respect to posting the image. Users who are online submit their opinions directly to the **uploader agent**. For users who are offline and/or users who fail to provide an opinion before a pre-defined response time threshold, opinions must be computed to determine the associated users' privacy preferences with respect to the co-owned image. To formulate the offline user opinions, we employ an opinion computation algorithm that infers the user's privacy preferences based on personality profile and behaviour history information. Finally, based on the user privacy opinions, the **uploader agent** invokes a **filtering agent** to blur out (enforce privacy by concealing) the images belonging to the users who declined to have their image displayed. Our empirical results demonstrate that we can reach a privacy-preserving decision regarding posting a co-owned image in a time-efficient manner, even when most of the users involved are offline.

The rest of the paper is organized as follows. Section 2 presents the related work. Our proposed agent-based model is presented in Section 3. In Section 4, we discuss results from our empirical model. We offer conclusions and suggestions for future work in Section 5.

2 Related Work

Work on the problem of posting co-owned images in a privacy preserving manner is initiated by Squicciarini et al. [5]. The Squicciarini et al. approach was based on game theory and employed a collaborative private box based on inference to handle privacy concerns regarding posting co-owned images on platforms such as Facebook. However, a key drawback to this approach is that it lacks an efficient technique to obtain the opinions of the individuals appeared in the image, which may put the privacy of these individuals at risk.

Some approaches [6, 7, 14, 15, 13] consider the problem of co-owned image sharing as one of the multi-user privacy conflicts. For instance, Hu et al. [7] used decision and sensitivity voting for conflict resolution. To do this, each image was assigned a sensitivity level, and users were given a decision value as a vote, based on the perceived user sensitivity level in relation to the image. The final decision was made through a collaborative decision making process based on the number of total votes. However, the Hu et al. [7] approach does not handle time restricted scenarios where user satisfaction is conditional on posting speed.

Other solutions consider friends of friends from an adversarial stance [8, 16, 17, 18, 19]. In addition to the Hu et al. [7] multiparty access control concept, Suvitha [8] applied a flexible sensitivity level and a majority consent to share an online content on an OSN. The Suvitha's [8] approach, however, does not offer a time-efficient approach for dealing with delays in posting, when the sensitivity model cannot reach a privacy consensus.

Joseph [9] proposed a model to compute privacy risk and information loss to address multi-user privacy conflict. Using multiparty access approach, the algorithm separates publishers' sharing groups to mark them with trust and distrust labels. However, when there is a large group of individuals listed in the conflicting group, this strategy limits content uploaders.

Ali et al. [1] proposed a cryptographic technique to handle the data uploading problem raised by the Joseph solution. Each data owner creates a secret share for the data co-owner. Viewers can access published data if they get a certain threshold of secret shares. Similarly, some cryptographic models such as non-interactive public key exchange [20], saleable group key management [21], consensus encryption algorithm [22] have been focused on content sharing conflicts on OSNs. However, since the majority of viewers are unable to obtain secret shares, the posting delay increases.

To support collaborative privacy management, Ulusoy [10] used a tax-based approach to limit co-owner uploads. Users are expected to pay more tax if they collaborate more in the decision-making process. Nevertheless, this approach restricts former users actively engaging in the voting process and so puts privacy at risk as reduces usability.

Other approaches that build on the extended Squicciarini et al. [5] approach focus on user behavior [23, 24, 25, 26, 11]. A game theory algorithm was proposed by Du et al. [11] to influence clients' interactions and to encourage participation in configuring privacy settings. However, data publishers' opinions are not always taken into account which poses a privacy risk. Fuzzy group decision-making models [27, 28, 29, 12] have been used to support data publishing based on consensus. In this vein, Akkuzu et al. [12] proposed using dynamic trust values for weighting co-owner opinions. If co-owners are concerned about the potential security aspects of the co-owned online content and do not want the content to be shared, but the

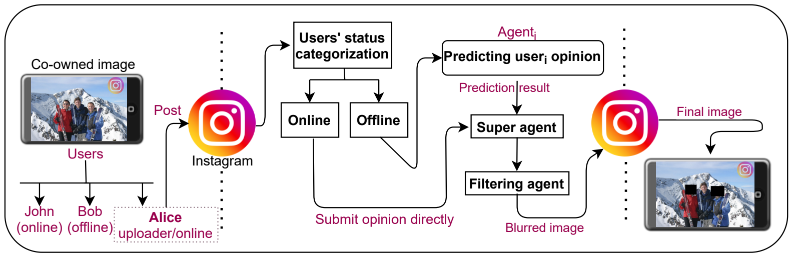

Fig. 1 Agent supported image transformation

owner agrees, then Akkuzu et al. [12] approach reduces the trust value in the owner side. But this approach requires the co-owners to share a lot of private data, which publishers considered undesirable.

To tackle the issue of publishing private data, Mosca et al. [30] proposed ELVIRA algorithm as an agent-based collaborative sharing approach. ELVIRA supports users in enforcing privacy preferences with respect to co-owned images. While ELVIRA addresses the issues of consensus, one issue remains: dealing with offline users, belonging to overlapping friendship networks, whose privacy opinion is uncertain. In the following section, we present our approach to addressing both issues.

3 Co-Owned Image Sharing

We assume that images contain user tags that describe each user on an online social network. Moreover, tags are associated with a user account. So, a link between a tag and a user refers to an active (valid) account on the social network platform. We also assume that a user who wishes to post/share an image owns the image, in that he/she appears (has a tag) within the image. In the agent framework, the profile of this user is bound to a super agent called an **uploader agent**. Likewise, all tags belonging to the other users within the image to be posted are linked to user agents. In order to post an image, the uploader image must reach a consensus with these user agents. For instance, in Figure 1, Alice wishes to post an image containing tags associated with John and Bob. In this case, Alice's profile is linked to an *uploader agent*, while John and Bob's profiles are bound to **user agents**.

3.1 Multi-Agent Model

In our multi-agent model an *uploader agent* (agent bound to the profile of the user initiating the posting request) begins by broadcasting a message to the other user agents associated with the profiles of the users who appear in the co-owned image.

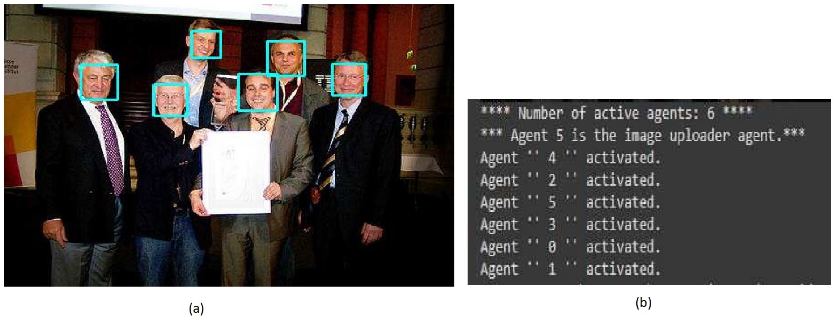

Fig. 2 Agent activation (a) Binding tags to associated user agents; (b) Uploader agent interaction with offline users' agents

As shown in Figure 2(a), to determine which user agents to invoke, the uploader agent analyses the co-owned image to identify the pinned tags within the image and binds these tags to the associated user agents on a per-user profile basis.

As shown in Figure 2(b), the *uploader agent* then broadcasts a message to all the user agents involved in the co-owned image requesting opinions on whether or not the associated users agree to have their image posted. Users who are online and actively using the social network platform, submit responses directly to the *uploader agent* during a pre-defined time window. If all the users are online and the *uploader agent* receives responses before a pre-defined delay threshold, a decision can be made on how to transform the image for posting. When users are offline, or online but fail to provide an opinion before the delay threshold expires, each corresponding *user agent* must determine what opinion its associated user is likely to have vis-a-vis the image to be posted. In order to decide, each *user agent* uses its **opinion computation algorithm** to formulate an opinion on behalf of the user. The opinion, once obtained, is submitted to the *uploader agent*. We now explain how the *user agent* computes an opinion on behalf of a user.

3.1.1 Opinion Computation

Each user agent maintains a case-base of previous opinions that the associated user submitted with respect to co-owned images. We use α to denote the minimum threshold of opinions in the case-base. This occurs when a user is new or has not previously participated in a co-owned image posting decision. The maximum number of opinions is denoted by F and F is such that $\alpha \leq F$.

Based on the opinions in the case-base, the *user agent* computes a Mean Score Opinion (MSO) using Equation (1) as follows:

$$MSO = \frac{\sum_{i=n}^{i=n-m} R_i}{m+1} \tag{1}$$

where n is the last opinion registered in the case-base, m is a list of opinions chosen from a case-base such that $n \geq m \geq \alpha$, and R_i is i*th* user opinion.

Once the MSO has been computed, the *user agent* must evaluate the computed score to determine if the value obtained is a satisfactory representation of the user's real opinion. If the case-base is empty - that is the user is new or has not previously participated in a co-owned image sharing scheme, then m $\leq \alpha$. In this case, the *user agent* submits the value of α to the *uploader agent* to indicate that the user's decision is "Disagree" and so his/her image should be blurred.

We now consider the case in which a user's opinion is unclear. That is, the uploader agent has not received a firm "Disagree" or "Agree" message from a user agent. In this case, the uploader agent qualifies the user opinion as being within an *Uncertain Range*. We formulate the *Uncertain Range* mathematically as follows:

We formulate the uncertain range mathematically as follows:

$$\frac{Z}{2} - \beta \leq UR \leq \frac{Z}{2} + \beta \tag{2}$$

where Z is the in range maximum value of submitting an opinion, and (β) as the maximum distance from $Z/2$.

When the MSO $\leq UR$, the *user agent* submits the MSO value to the *uploader agent* to indicate that the user has "Disagreed" to his/her image being posted. If the MSO $\geq UR$, the *user agent* submits the MSO value to the *uploader agent* to show that the user has "Agreed" to have his/her image posted.

We now consider what happens if a *user agent* submits an opinion but the *uploader agent* rejects it because it is an indecisive opinion, that is, it falls within the uncertain range. The *uploader agent* uses personality profile data to train a machine learning model to obtain a personality score (*PS*) that respects Equation (2). Our machine learning model employs the Random Forest and Support Vector Regression algorithms, as examples of regression-based algorithms that are useful in supporting continuous scoring schemes. Based on the results of the personality computation, the user's personality is then mapped onto a personality score scale (ranging from one to six) similar to that used in [31]. The *PS* is compared against Equation (2), and if the $PS \leq UR$, *user agent* concludes that the decision is "Disagree" and if the $PS \geq UR$, then the decision is "Agree". If a clear opinion has not been computed, the *uploader agent* considers that the user opinion is "Disagree". Figure 3(a) provides a visualisation of the agent opinion submission process. Once the user opinions have been computed, the **uploader agent** activates the **filtering agent**.

3.1.2 Filtering and Blurring

The filtering agent uses the python OpenCV library and the enhanced Haar-cascade based face detection algorithm [32], which is a functional object detection technique. Furthermore, to blur out images in OpenCV, the filtering agent uses a Gaussian smoothing kernel to have a bell-curve around the center pixel [33] instead of using a black box to blur the faces.

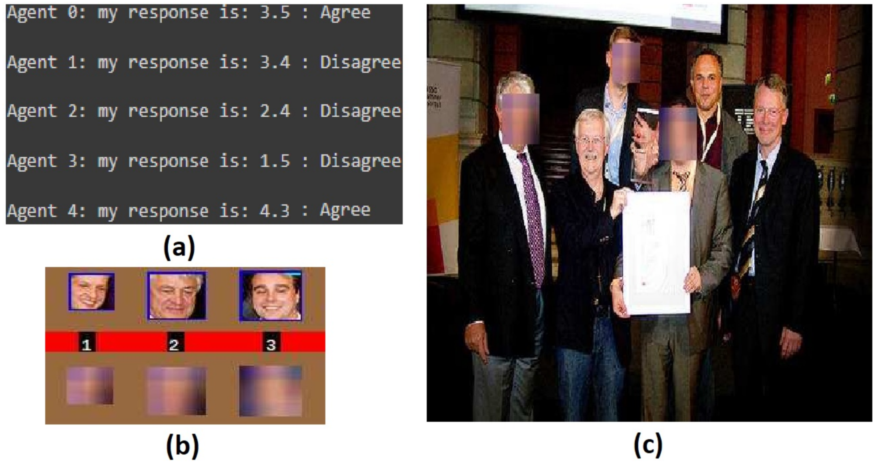

Fig. 3 Applying opinions on co-owned image (a) Agents' participation on behalf of offline users; (b) Detected faces; (c) Blurred faces

The faces of users who decline to share their images online are blended with the Gaussian blurred segments (see Figure 3(b)), and then inserted on an independent layer over the face positions, as shown in Figure 3(c).

Algorithm (1) summarizes the operation of the multi-agent model in terms of reaching a decision in a time efficient manner on transforming an image for utility (minimal blurring) and privacy (adhering to user privacy opinions). There are two procedures in Algorithm (1). The first procedure computes and checks offline users' opinions; the second procedure blurs faces of disagreed users and returns the modified image to the uploader agent.

4 Experimental Setup and Results

Our multi-agent model was implemented on a machine with an Intel CPU 2.3 GHz core i7, 16GB of RAM, and run over a Windows 10 operating system using Google Colab. For the personality score scheme, we used the Big Five Personality Test (BFPT) dataset [31] containing 1,015,342 questionnaire answers. In our experiments, we only used the first 300K records and the first ten items ('EXT1' to 'EXT10') as users' recent online opinions about sharing images on social networks and we attempted to predict 'EXT9' feature in the dataset. Furthermore, we used Mesa project [34] to construct a multi-agent system since it provides foundations for running agent-based models operating on python.

Algorithm 1 Opinion Computation Algorithm (OCA)

```
Input ← a co-owned image
Output → a filtered image considering users opinions
procedure OCA (CO-OWNERS, IMAGE)
    UA ← activate a super agent
    for all co-owners do UA → request user(i) to submit opinion end for
    WAIT (Time_window); % receiving co-owners opinions
    %Status check:
    for all co-owners do
        if UA did not receive opinion from user_i then
        status ← offline else status ← online end if
    end for
    for all offline co-owners do
        activate user_i agent; agent_i checks database_i;
        top:
        if database_i is not empty then
            compute_i ← compute user_i opinion; % run opinion computation algorithm
            if opinion_i located within uncertain range then goto top end if
            FilteringAgent ← collected opinions;
        end if
    end for
end procedure
procedure FILTERINGAGENT (Face_Positions, OPINIONS, IMAGE)
    faces ← Face_Positions;
    if opinion_i == disagree then Blur (face_i); % Gaussian filter end if
    Return filtered image
end procedure
```

Table 1 Inputs into multi-agent model based on BFPT dataset

	α	β	Z	UR	F	Disapproval	Approval	Neutral
Values	3	0.5	6	2.5 - 3.5	10	0	6	3

4.1 Results

Table 1 shows our inputs into multi-agent model based on BFPT dataset [31]. Briefly, in Table 1, α denotes the least number of opinions to activate an agent, Z is the highest opinion value in the dataset, and F is the number of opinions submitted directly by user$_i$. Because the neutral opinion on the BFPT dataset equals three, we consider $beta$ to be 0.5 as the maximum distance in the uncertain range.

Figure 4(a) shows the number of agents whose opinions fall in UR (infected agents) during the opinion formulation process. For 30 co-owned images, we put six agents to the test to compute users' opinions. Based on the results, a maximum of two agents were infected agents. Accordingly, Figure 4(b) depicts the effectiveness of the multi-agent model in terms of time complexity. Bonding users to agents and considering infected agents take about 3.81 seconds to compute offline users' opinions.

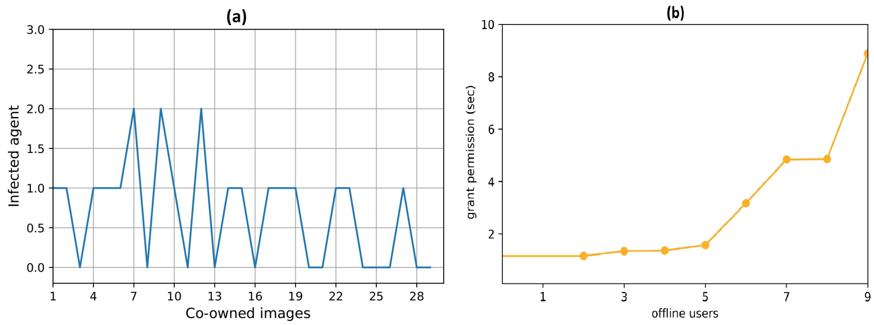

Fig. 4 (a) the number of agents in the UR; (b) effectiveness of the multi-agent model in terms of time complexity considering infected agents.

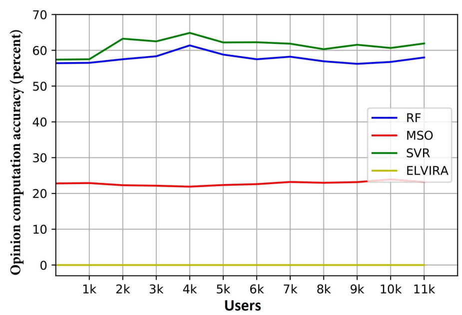

Fig. 5 User opinion computation accuracy for middle-sized test dataset with $11k$ users

We use a variety of opinion computation algorithms to compute user opinions, including MSO, Random Forest (RF), and Support Vector Regression (SVR). Furthermore, We split the BFPT data into two sets: 80 percent for training and 20 percent for testing opinions accuracy in comparison to Personality Score. Figure 5 shows the performance of opinion computation accuracy for middle-sized dataset (1K to 11K user previous opinions in BFPT dataset). On average, the RF algorithm computed the users opinions with 57.82 percent accuracy, while the results for SVR and MSO were 61.71 and 22.79 percent, respectively. Moreover, the opinion computation results for large-sized dataset with 300K users were 58.73, 24.02, 63.82 and zero percent for RF, MSO, SVR and ELVIRA [30] algorithms, respectively. Generally, SVR provides the best-performing model in terms of computing users' opinions based on their recent opinions.

Moreover, Figure 6(a) delineates the performance of our agent-based model in the direction of blurring accuracy for multiple offline users. The results achieved from 60 co-owned images present that that the SVR and RF perform more effectively in terms of face blurring accuracy than the MSO algorithm. Based on the results, however, the RF algorithm is suitable for co-owned images with at least

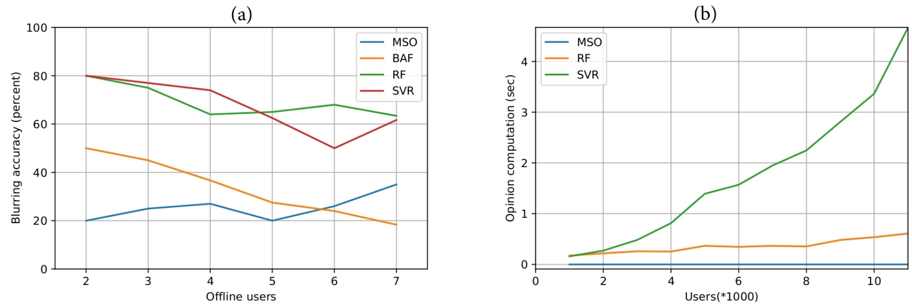

Fig. 6 (a) Face blurring accuracy for multiple offline users based on various opinion computation algorithms (BAF: Blur all Faces, SVR: Support Vector Regression, MSO: Mean Score Opinion, RF: Random Forest); (b) Training time to formulate users' opinions

four offline users. On the other hand, the SVR algorithm performs well when the co-owned images contain between one to three offline users. Figure 6(b) indicates the training time required to compute users' opinions. According to the results, the training time for SVR algorithm surges when faced with online behaviours of more than 3k user profiles. Based on the results, we can conclude that the training time for the SVR algorithm can be reduced by training a middle-sized dataset since the SVR algorithm performance for 4k users is close to the large-sized dataset (300K).

5 Conclusion

Enforcing privacy on co-owned images raises a conflict in terms of usability and privacy when some or most of the users involved are offline. Two key issues arise: (1) when users are not online, a privacy decision regarding whether or not to post the image cannot be reached, thereby resulting in delay; and (2) ineffective user opinion computation necessitates large amounts of image distortion, resulting in low levels of user satisfaction. We employed a multi-agent model to address both issues in a time-efficient manner. To formulate offline user opinions, we employ an opinion computation algorithm that infers the users' privacy preferences based on the users' historical online usage behaviours. Our empirical results demonstrate that by supporting predictions with machine learning algorithms, agents can reliably reach a consensus on posting the image in 3.81 seconds on average without negatively impacting performance, which is beneficial in terms of usability.

References

1. Ali S, Rauf A, Islam N, Farman H (2019) A framework for secure and privacy protected collaborative contents sharing using public OSN. Journal of Cluster Computing 22(3):7275-7286
2. Severo M,Feredj A, Romele A (2016) Soft data and public policy: Can social media offer alternatives to official statistics in urban policymaking?. Journal of Policy & Internet 8(3):354-372
3. Xu L, Jiang C, He N, Han Z, Benslimane A (2018) Trust-based collaborative privacy management in online social networks. Journal of IEEE Transactions on Information Forensics and Security 14(1):48-60
4. Giovannetti E, Hamoudia M (2018) Understanding the different pre and post peak adoption drivers in the process of Mobile Social Networking diffusion. In: Seoul: International Telecommunications Society (ITS) (pp. 1-4)
5. Squicciarini AC, Shehab M, Paci F (2009) Collective privacy management in social networks. In: Proceedings of the 18th international conference on World wide web (pp. 521-530)
6. Wishart R, Corapi D, Marinovic S, Sloman M (2010) Collaborative privacy policy authoring in a social networking context. In: IEEE International Symposium on Policies for Distributed Systems and Networks (pp. 1-8)
7. Hu H, Ahn G (2011) Multiparty authorization framework for data sharing in online social networks. In: IFIP Annual Conference on Data and Applications Security and Privacy (pp. 29-43)
8. Suvitha D (2014) Mechanisms of Multiparty Access Control in Online Social Network. Journal of Recent Development in Engineering and Technology 2(3):8-13
9. Joseph NS (2014)Collaborative data sharing in online social network resolving privacy risk and sharing loss. IOSR Journal of Computer Engineering 16(5):55-61
10. Ulusoy O (2018) Collaborative privacy management in online social networks. In: Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (pp. 1788-1790)
11. Du J, Jiang C, Chen KC, Ren Y, Poor HV (2018) Community-structured evolutionary game for privacy protection in social networks. Journal of IEEE Transactions on Information Forensics and Security 13(3):574-589
12. Akkuzu G, Aziz B, Adda M (2020) Towards consensus-based group decision making for co-owned data sharing in online social networks. Journal of IEEE Access 8:91311-91325
13. Wishart R, Corapi D, Marinovic S, Sloman M (2010) Collaborative privacy policy authoring in a social networking context. In: IEEE International Symposium on Policies for Distributed Systems and Networks (pp. 1-8)
14. Kumar A, Bezawada R, Rishika R, Janakiraman R, Kannan PK (2016) From social to sale: The effects of firm-generated content in social media on customer behavior. Journal of Marketing 80(1):7-25
15. Thomas K, Grier C, Nicol DM (2010) Unfriendly: Multi-party privacy risks in social networks. In: International Symposium on Privacy Enhancing Technologies Symposium (pp. 236-252)
16. Baden R, Bender A, Spring N, Bhattacharjee B, Starin D (2009) Persona: an online social network with user-defined privacy. In: Proceedings of the ACM SIGCOMM 2009 conference on Data communication (pp. 135-146)
17. Dürr M, Maier M, Dorfmeister F (2012) Vegas–A Secure and Privacy-Preserving Peer-to-Peer Online Social Network. In: International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing (pp. 868-874)
18. Jahid S, Nilizadeh S, Mittal P, Borisov N, Kapadia A (2012) Vegas–A Secure and Privacy-Preserving Peer-to-Peer Online Social Network. In: IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 326-332)

19. Schwittmann L, Boelmann C, Wander M, Weis T (2013) SoNet–Privacy and replication in federated online social networks. In: IEEE 33rd International Conference on Distributed Computing Systems Workshops (pp. 51-57)
20. Lv X, Mu Y, Li H (2013) Non-interactive key establishment for bundle security protocol of space DTNs. Journal of IEEE transactions on information forensics and security 9(1):5-13
21. Ali S, Rauf A, Islam N, Farman H, Jan B, Khan M, Ahmad A (2018) SGKMP: A scalable group key management protocol. Journal of Sustainable cities and society 39:37-42
22. Srilakshmi P, Aaratee S, Subbalakshmi S (2016) Privacy My Decision: Control of Photo Sharing on Online Social Networks. International Journal of Computer Science and Information Technologies(IJCSIT) 7(2):780-782
23. Liu F, Pan L, Yao LH (2018) Evolutionary Game Based Analysis for User Privacy Protection Behaviors in Social Networks. In: IEEE Third International Conference on Data Science in Cyberspace (DSC) (pp. 274-279)
24. Tosh D, Sengupta S, Kamhoua C, Kwiat K, Martin A (2015) An evolutionary game-theoretic framework for cyber-threat information sharing. In: IEEE International Conference on Communications (ICC) (pp. 7341-7346)
25. Chen J, Kiremire AR, Brust MR, Phoha VV (2014) Modeling online social network users' profile attribute disclosure behavior from a game theoretic perspective. Journal of Computer Communications 49:18-32
26. Squicciarini AC, Griffin C (2012) An informed model of personal information release in social networking sites. In: International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing (ICC) (pp. 636-645)
27. Capuano N, Chiclana F, Fujita H, Herrera-Viedma E, Loia V (2017) Fuzzy group decision making with incomplete information guided by social influence. Journal of IEEE Transactions on Fuzzy Systems 26(3):1704-1718
28. Martinez-Cruz C, Porcel C, Bernabé-Moreno J, Herrera-Viedma E (2015) A model to represent users trust in recommender systems using ontologies and fuzzy linguistic modeling. Journal of Information Sciences 311:102-118
29. Akkuzu G, Aziz B, Adda MO (2019) Fuzzy logic decision based collaborative privacy management framework for online social networks. In: 3rd International Workshop on FORmal methods for Security Engineering (pp. 674-684)
30. Mosca F, Such J (2021) ELVIRA: an Explainable Agent for Value and Utility-driven Multiuser Privacy. In: International Conference on Autonomous Agents and Multiagent Systems (AAMAS) (pp. 916-924)
31. Tunguz B (2018) Big Five Personality Test Dataset. Retrieved September 16,2021 from https://www.kaggle.com/tunguz/big-five-personality-test/version/1
32. Gangopadhyay I, Chatterjee A, Das I (2019) Face detection and expression recognition using Haar cascade classifier and Fisherface algorithm. Journal of Recent Trends in Signal and Image Processing 922:1-11
33. Getreuer P (2013) A Survey of Gaussian Convolution Algorithms. Journal of Image Processing On Line 3:286-310
34. Masad D, Kazil J (2015) Effective Substances. In: 14th PYTHON in Science Conference (pp. 153-60)