Fuzzy Logic Decision Based Collaborative Privacy Management Framework For Online Social Networks

Gulsum Akkuzu[1], Benjamin Aziz[2] and Mo Adda[3]
[1 2 3] *School of Computing, University of Portsmouth, Portsmouth, United Kingdom*
gulsum.akkuzu@port.ac.uk, benjamin.aziz@port.ac.uk, mo.adda@port.ac.uk

Keywords: privacy management, online social networks, data security features, fuzzy logic

Abstract: Online Social Networks (OSNs) have become one of the most popular implement for interacting with people all over the world and sharing data with them. These data sometimes may be a co-owned data which involves multiple users, sharing co-owned data can cause privacy violation if co-owners are not happy with the owner's sharing privacy settings. To tackle privacy issues on co-owned data, collaborative privacy management has become a popular research area in recent years. In this work, we provide a fuzzy logic decision based collaborative privacy management framework for OSNs. We use data sensitivity value and confidence value in targeted group as input variables of fuzzy system. We also use trust values between users since our framework needs to calculate trust loss and gains for reputation value.

1 INTRODUCTION

Online Social Networks (OSN) are popular all over the world, since they offer information sharing, social communications, and attractive interactions among people. There are various social networking sites in the Internet such as Facebook, Google+, Twitter, WeChat, Linked-In, etc. Facebook is one of the social network sites in which people are allowed to share different types of context such as video, photo, message, event, etc. These contents may include their personal life information, private information and the content may be disclosed to wider audience than they actually intended for. Sensitive information of users are stored in OSNs, however, most users are unaware of shared contents' features. Protecting information is one of crucial concerns, therefore OSNs need to provide mechanisms for protecting users' data.

Users can upload content to their own space and other users' spaces also. They are allowed to tag users, which may cause privacy leakage. Current OSNs allow users to regulate access to the data that is on their own space, however, they can not control or take precaution for contents that are shared by other users and include their information. It is most likely to see the leakage of sensitive information while data is being publicised (Hu et al., 2015). Beside the service providers of OSNs take precaution to prevent data breach, users can also adjust their data access control by using the privacy setting function implemented in OSNs (Xu et al., 2011). Facebook has provided users different levels of privacy protection countermeasure that users can decide who is allowed to contact them, see their stuff, and search them. A privacy policy determines which users are allowed to access to other user's data. OSNs use user relationships and group membership to distinguish trusted and untrusted users (Hu and Ahn, 2011). OSNs provide simple access control that allows users to control information on their own spaces, however, users cannot control or in other words have no rights to control data, that is related to them, outside of their space.

Current Online Social Networks have provided restrictions on users who can access data, however, there is no restrictions who posts data. There is one side data restriction on data even if data is co-owned data which involves more than one user. However, privacy management of co-owned data requires collaborative privacy management. Even though some online social networks provide chances to co-owners, who have rights to manage permissions of a co-owned data, which is related to them, either with tagging or face-recognition techniques we do not see any benefit for those who are not tagged or notified.

In this work, we provide a collaborative privacy management on the shared data from multiple associated users. Different from previous studies ,which assume all users are tagged by owner or use identification technique, we assume the owner who intends to share co-owned data notifies co-owners and allows

fuzzy decision system to make a decision based on co-owners' privacy requirements on the data. We use fuzzy logic on decision making process in which decision is not restricted with the Boolean decision **'Yes' or 'No'**. We define multi-value set in decision making with Fuzzy Logic Decision Making System **'Yes', 'Maybe', 'No'**. Based on the owner's final decision on data co-owners' trust in owner either increases or decreases, end of the sharing process our framework updates the owner's reputation. In short, the main contributions of this work as follows:

- A fuzzy decision making system is proposed for making decision in OSNs. The result of fuzzy decision making system affects the privacy loss calculation and changes on owner's reputation value.
- Exploring the connection between data sensitivity and trust in targeted group for sharing sensitive data. The sensitivity value of data and confidence value in targeted group are gathered together for making decision of fuzzy system .

2 Related Works

Collaborative Privacy Management is a challenge for OSNs since all users have different privacy requirements. Hence, it is very possible to see conflicts on shared contexts in OSNs. Although privacy management mechanism has restrictions on users who want to access data, there is no restriction on users who post data. However, users who post data may violate other users' privacy. Recent works have focused on conflicts among users' privacy policies, they first have aimed to detect the conflicts, then generate an aggregation policy that resolves the conflicts. The aggregated policies are not the solution since there are still privacy loss issues in OSNs.

Researchers have worked on the problem of collective privacy management of co-owned data even though OSNs do not yet set restrictions on the co-owned data. This problem was addressed by Squicciarini et al.(Squicciarini et al., 2009), they proposed a solution for privacy management for photo sharing in OSNs, this means that each co-owner can specify their own privacy preference for the shared content. They adopt the Clarke-Tax mechanism to provide collective enforcement in shared content, they evaluate their work with Game Theory. The usability is an issue for this work, they do not take all stockholders' privacy preferences.

Wishart et al.(Wishart et al., 2010) provided a collaborative privacy policy authoring in the context of social networking, they allowed the originator of the data to specify policies for the content, however, their work does not consider co-owners' privacy policy specifications.

Hu (Hu et al., 2015) proposed a collaborative management of shared data in OSNs, it is a simple but flexible mechanism. The mechanism provides conflict resolution that considers both the privacy risk and data sharing loss.

Suvitha (Suvitha.D, 2014) formulated a multi-party access control and policies, he used voting mechanism for making decision on co-owned data. Collaborative privacy management issue might be described mother of the privacy conflicts. Therefore, it is an inevitable point to be involved while the co-privacy management of shared data is considered.

Joseph (Joseph, 2014) proposed a solution for privacy risk and sharing loss for collaborative data sharing in online social network. The work proposes an algorithm to identify conflict segments in accessor space.

A framework was developed for protecting and securing co-owned data for public OSN by Shaukat et al. (Ali et al., 2017). They pointed that the privacy risk is seen not only from unauthorized users but also from the OSNs service providers, they used cartographic-based technique in their framework to overcome privacy concerns.

Recently, a work has been proposed to address collaborative privacy management with an agent-model (Ulusoy, 2018). He has proposed to modify Clarke-Tax mechanism that was used in (Squicciarini et al., 2009). Du et al, proposed an evolutionary game model that analyses how a user's data privacy protection is affected by other users' privacy decisions (Du et al., 2018).

All given above studies generally assume that there is a service provider (mediator) that knows each users' privacy policies for data items. However, there are studies that consider mediator is unnecessary and not taking trust into consideration. In the literature there are also studies which exclude service provider from the scope, and they use involved users feedbacks for making final decision of owner (Xu et al., 2019; Rathore and Tripathy, 2017). We use the same approach with those studies which consider mediator is unneeded, however, we use fuzzy logic decision making system to help co-owners (in other words stakeholders who are involved to data). In the previous studies, owner of data asks co-owners opinion on the data whether they want to share data with decision=1 or they do not want to share the data with decision=0. The decision does not have just Boolean value, decision would be between 0=no and 1=yes which can be named maybe. We take this point into

consideration, also in the previous work data sensitivity has been decided by owner, however, data sensitivity would be different for each co-owners, therefore, we develop a system which asks to each co-owners the sensitivity value of data. We think such a system is more realistic and practical, considering collaborative privacy management in Online Social Networks.

3 System Model

A social network structure involves a set of actors and a set of connection between these actors. An OSN is represented as a directed-graph $G = V, E$, where V is the set of nodes (actors, users) and E is the set of relationships among actors. A simple online social network has nodes and edges, where nodes represent users and edges present a relationship between users in the graph representation of online social networks. User relationships are divided into two groups, namely symmetric and asymmetric (Rathore and Tripathy, 2017). In our case, we use both symmetric and asymmetric discrimination for trust value adjustment, i.e., we use $t_{u(ij)} \in [0,1]$, which shows u_i's trust in u_j. For instance, if u_i has the symmetric relation to u_j, then $t_{u(ij)}$ could have a high value, most possibly full trust.

3.1 Overview of Fuzzy-decision based framework

We provide our proposed algorithm and its explanations in this section.

- **1.** An owner starts the process by uploading data. Then choose the trust threshold and the priority criteria. The priority choice is either Co-owner Trust Preferential, in which co-owners' trust value in owner is in priority, or Owner Trust Preferential in which owner trust values in co-owners is preferred for data sharing process and trust-reputation calculations.
- **2.** Once the owner chooses requirements for the first step then s/he needs to notify co-owners by giving them details for which data s/he intends to share and the group of people (targeted group) who will access the data.
- **3.** Fuzzy Decision Making Step: It allows co-owners to rate on data CIA properties for the sensitivity value, and confidence value for targeted group which is calculated based on relations that are between co-owners and members of the targeted group people.

Result: Updated Reputation value of owner
while *Owner upload the data, adjust the privacy settings,notify co − owners* **do**
  if *Co-owners:rate CIAPP features ;* **then**
    activate the fuzzy decision mechanism;
    Result of Fuzzy decision making system;
  else
    Wait till CIAPP ratings are completed
  end
end
if *preference: co-owner trust* **then**
  $Pl \rightarrow$ equation11;
  $Trustlossand Trustgain \rightarrow$ Equations 13 and 12;
  if $valueofequation12 \leq valueofequation13$ **then**
    share data with full permission
  else
    if $Th_{tr} \leq Avg_{tr}$ **then**
      share data with like and view permission
    else
      Do not share
    end
  end
else
  if *fuzzy decision Yes or Maybe* **then**
    if $0.7 \leq dec_{deg}$ **then**
      share data with full permission
    else
      share data with like and view permission
    end
  else
    Do not share
  end
end

Algorithm 1: Algorithm of FuLoBaF

- **4.** After a fuzzy system gives the decision value on co-owned data, the second part of framework works through.

$*$ if the co-owner trust was chosen by the owner in step 1, then the privacy loss is calculated with the given equation 9. Trust gain and trust loss are calculated with the privacy loss, according to equation 10 and equation 11. If the trust gain is higher than the trust loss, then the data can be shared with no access restriction on data. Otherwise, the average of co-owners' trust in owner is calculated and

compared with the threshold that needs to be decided by the owner in step 1. If the average trust value is greater than the threshold value, then the data is shared with some access restrictions on itself (i.e. viewers (targeted group of people) can view and like it but can not share it). The final need is to update owner reputation and gained or decreased trust values of co-owners in the owner.

* if the owner's trust was chosen in step 1 by the owner, then the system chooses at least half of the co-owners who have the highest trust values in owner. If choosing co-owners' rates on the sensitivity (CIA properties) without concerns, then the data are shared with a full permission. Otherwise, the framework checks the fuzzy membership degree, i.e., the intensity score of the decision.

3.2 Details of Fuzzy Decision Making Procedure

In the framework, co-owners' decisions are taken with the fuzzy system. The system has two inputs and one output, where the data sensitivity and confidence in the targeted group are defined as the inputs and the decision is defined as the output. A fuzzy decision is based on the fuzzy logic in which the decision values are ranged from 0 to 1 rather than binary values (0 or 1).

A fuzzy set is defined as (U,μ) in which U represents the universe set of elements and μ represents the membership function with the membership degrees of the elements to the set U, i.e., $x \in U \rightarrow \mu(x) \in [0,1]$. Based on the system and data, the shapes of the membership functions are chosen. There are various shapes of membership functions that can be chosen for a fuzzy set, such as triangle, trapezoid, and rectangle. It can be clearly seen that trapezoid functions can be viewed as a generalization of triangular and rectangular membership functions. As shown in Figure 1, if a=b and c=d, then the shape of the membership function would become rectangle. On the other hand, if b=c, then the shape would become triangle.

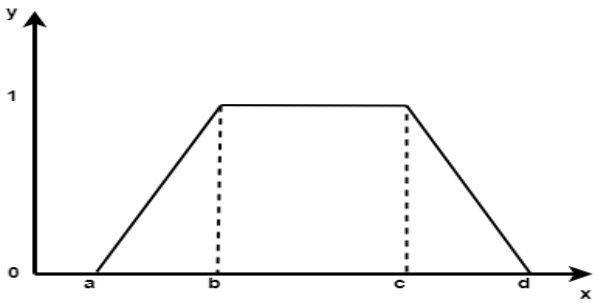

Figure 1: Trapezoid Membership Function

The membership function of the trapezoidal fuzzy set is defined by a function,f(x), and essentially depends on four parameters a,b,c,d as given below.

$$f_T(x) = \begin{cases} 0, & x \le a \text{ or } x \ge d \quad (1) \\ \dfrac{x-a}{b-a}, & a \le x \le b \quad (2) \\ 1, & b \le x \le c \quad (3) \\ \dfrac{d-x}{d-c}, & c \le x \le d \quad (4) \end{cases}$$

There are two ways to define membership functions, either expert knowledge can be used to define membership functions (Mamdani and Assilian, 1999) or data can be used to induce the membership functions using machine learning techniques (Hosseini et al., 2012), (Jamsandekar and Mudholkar, 2014).

A fuzzy rule based system mainly involves three operations, namely, fuzzification, inference, and defuzzification. In the fuzzification step, a numerical value is mapped into a membership degree according to a membership function. In the inference stage, rules are defined with the linguistic terms of input variables and the linguistic term of the output variable. For example,

· **x is A:** antecedent

· **Rule:** If x is A then y is B

· **y is B:** consequent

In a given fuzzy rule x is A and y is B can be true to a degree, instead of being entirely true or false (Koyuncu and Yazici, 2005), the antecedent may be composed of one condition or multiple conditions connected by the *AND* or *OR* logical operators. For example;

· **Rule 1:** If x_1 is A_{11} AND x_2 is A_{21} THEN decision= D_1

· **Rule 2:** If x_1 is A_{11} OR (x_1 is A_{12} AND x_2 is A_{22}) THEN decision=D_2

.

.

· **Rule m:** If x_1 is A_{1m} AND x_2 is A_{nm} THEN decision=D_k

A_{nm} is an indication of a linguistic term in which n represents A's input attribute and m represents the rule index. D_k represents a decision label, k is the decision index.

This fuzzy rule based system can be seen in Figure 2. The system basically has three steps: fuzzification, inference process, and

- Fuzzification: Obtains membership degree values mapped from crisp values, i.e., it aims to map the

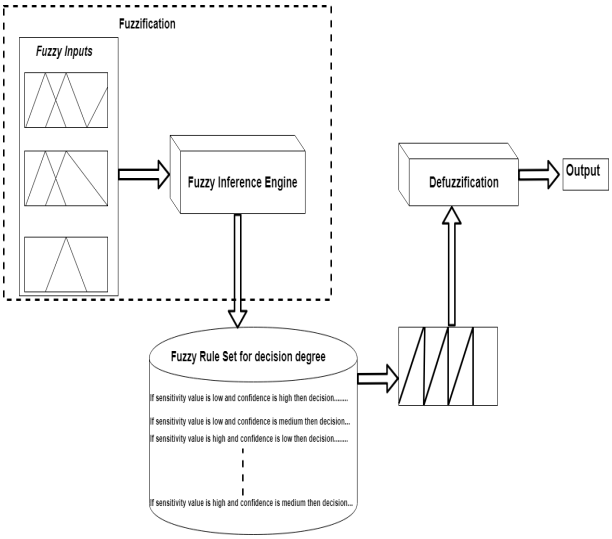

Figure 2: Fuzzy Expert System with proposed work sample rules

value of each continuous attribute to the membership degrees to the fuzzy sets defined for the continuous attribute.

- Inference Process: Obtains the membership degree to the consequent of each rule, i.e. a fuzzy output from each rule is derived, and then combines the fuzzy outputs of all the rules by using a fuzzy aggregation operator, in order to derive the overall membership degree.
- Defuzzification: Converts the derived overall membership degree into a crisp value as the output of the fuzzy system.

4 Data Generation

Dataset: We conduct our work on both real world data and synthetic data. We use the Facebook data from Stanford large network data set collection (snap Facebook Data, 2016). We also generate a network by using the network packages supported by Harberg et al. (Hagberg et al., 2008). The generated network has 1000 nodes and 20000 undirected edges.

To test our equations and proposed system usability, we have simulated data for sensitivity and confidence values. An owner decides the sensitivity value in all the previous work. However, the data sensitivity value may not be the same one for co-owners as owner's concern. In our work, co-owners decide how sensitive the co-owned data is for them. To do simulation, we formulate the sensitivity value with five features of Evolutionary Circles of Information Security (Cherdantseva and Hilton, 2012) which considers that data security is based on fourteen features. The Evolutionary Circles of Information Security model has five circles that are separated with regard to subject of protection and security goals. We choose five features that are related to information security in the network area. The equation of data sensitivity is as follows;

$$S_d = \frac{\sum_{i=1}^{m}(P_i * (w_i))}{\sum_{j=1}^{n}(f_j)} \tag{5}$$

S_d represents the data sensitivity, it ranges [0,1]. The numerator gives the summation of the data CIAPP probabilities, in which $P-i$ indicates the probability of CIAPP concerns that is voted by co-owners and w_i is the weight of the properties. The denominator indicates the total number of features.

We also formulate the confidence value based on the owner trust relation with targeted group members, co-owners' trust relations with targeted group members, and sensitivity value that is given in equation 1. We first show the calculation of the trust relation;

$$R_{oi}, f(r_{o1}, r_{o2}, r_{o3}, ..., r_{osi}) = \frac{\sum_{j=1}^{S_i}(r_{oj})}{S_i} \tag{6}$$

R_{oi} represents the owner's trust in each member of targeted group and S_i represents the size of the targeted group.

$$R_{ci}, f(r_{c1}, r_{c2}, r_{c3}, ..., r_{csi}) = \frac{\sum_{j=1}^{S_i}(r_{cj})}{S_i} \tag{7}$$

R_{ci} represents the co-owner's trust in each member of the targeted group and S_i represents the size of the targeted group.

From equations 2 and 3, we finalize the trust relation with the following formula;

$$R = R_{oi} * \prod_{k=1}^{c} R_{ki} \tag{8}$$

R is the trust in the targeted group with the owner's trust in the group i R_{oi}, also with the each co-owner's trust in group i.

With the equations 1,2 and 3, we can now calculate the Confidence value in targeted group as follows;

$$C_f = 1 - S_d * (1 - R) \tag{9}$$

Below figure shows the changes of Confidence value based on the sensitivity and relation values (see equation 9.

Our dataset (see Table 1) has sensitivity value and confidence value, these two variables values are obtained with the above equations (see 5 and 9). The dataset is used for fuzzy logic decision.

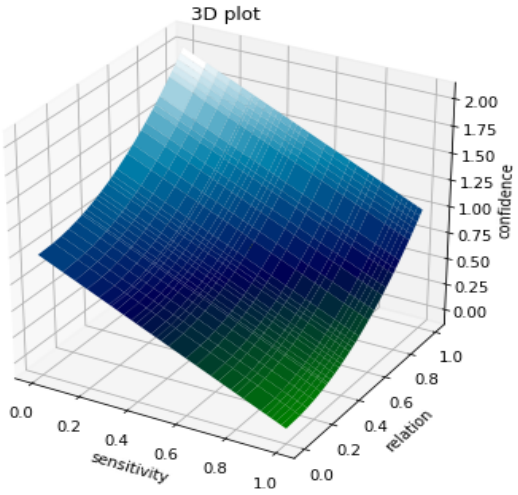

Figure 3: 3D graph of Confidence value with the Sensitivity and Confidence value

Table 1: Sample of Sensitivity and Confidence Input Values of Fuzzy System

sensitivity	confidence
0.5	0.5
0.1	0.9
0.2	0.9
0.3	0.9
0.4	0.8
0.9	0.5
0.9	0.1
0	1
0.12	1
0	0.98
1	0

Our Fuzzy Inference System has two inputs variables and one output variable. We used triangular and trapezoidal membership functions. To generate triangular membership functions of Figure 4 and 5, we used the fuzzy c-means clustering algorithm to generate clusters and to construct membership functions.

- Input variables' values and output variable values are formed into three clusters, and these three clusters' centers are used the centers of triangular fuzzy membership functions.
- The maximum and minimum values of each cluster are used as two vertexes values of each of triangular membership functions.
- The maximum and minimum values for the triangular membership functions are formed by increasing and decreasing b vertex values.
- In trapezoidal membership functions, the values of variables are calculated by increasing the minimum vertex value of the triangular membership function and decreasing the maximum vertex value of triangular membership function .

We have twelve rules for our fuzzy system, and the rules are given in Table 2.

As it is seen on the table, we use the 'AND' operator in which the minimum value among membership functions is picked up, while the 'OR' operator picks up the maximum value among the membership functions.

Figure 4 and 5 illustrate transformation of the linguistic variables x_1 and x_2 to numerical values.

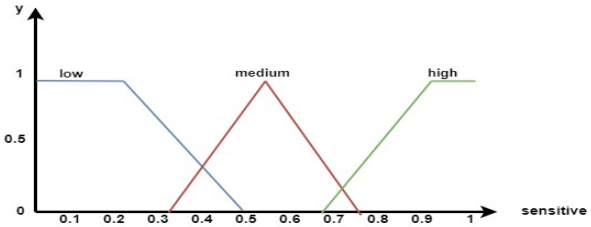

Figure 4: Linguistic terms' membership functions for sensitivity input

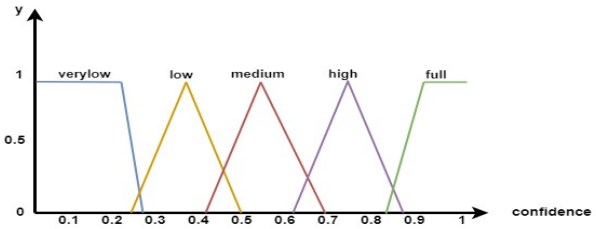

Figure 5: Linguistic terms' membership functions for confidence input

5 Experiments and results

In this section, we first give the experiments in the framework's fuzzy part. After getting the decision result from the fuzzy decision making part, we give use cases to show the applicability of the proposed framework.

Table 3 presents the decision output depending on two input values, which are sensitivity and confidence. The decision is given with its decision calculation.

Figure 6 and Figure 7 are the presentations of the decision making computation. Figure 6 indicates that the decision is 'maybe' if the sensitivity value is $low_{0.2}$ and the confidence value is $medium_{0.5}$. Similarly, Figure 7 shows the decision is 'no' if the sensitivity is $high_{0.8}$ and the confidence is $verylow_{0.1}$.

Table 2: The proposed work rules

Rule number	Rule
1	If x_1 is low AND x_2 is verylow then decision=maybe
2	If x_1 is low AND x_2 is low then decision=maybe
3	If x_1 is low AND x_2 is medium then decision=maybe
4	If x_1 is low AND x_2 is full then decision=yes
5	If x_1 is medium AND x_2 is verylow then decision=no
6	If x_1 is medium AND x_2 is low then decision=maybe
7	If x_1 is medium AND x_2 is medium then decision=maybe
8	If x_1 is medium AND x_2 is full then decision=yes
9	If x_1 is high AND x_2 is verylow then decision=no
10	If x_1 is high AND x_2 is low then decision=no
11	If x_1 is high **and** x_2 is medium then decision=maybe
12	If x_1 is high AND x_2 is full then decision=yes

Table 3: Decision Making Fuzzy System with Input and Output Variables' Values

Input 1 (sensitivity)	**Input 2 (confidence)**	**Output (decision)**
$medium_{0.66}$	$low_{0.33}$	$\mathbf{maybe}_{0.35}$
$high_{0.8}$	$verylow_{0.1}$	$\mathbf{no}_{0.12}$
$low_{0.2}$	$medium_{0.5}$	$\mathbf{maybe}_{0.64}$
$low_{0.2}$	$high_{0.8}$	$\mathbf{yes}_{0.84}$
$high_{0.9}$	$medium_{0.6}$	$\mathbf{maybe}_{0.45}$
$high_{0.9}$	$low_{0.3}$	$\mathbf{no}_{0.17}$
$high_1$	$medium_{0.5}$	$\mathbf{no}_{0.15}$

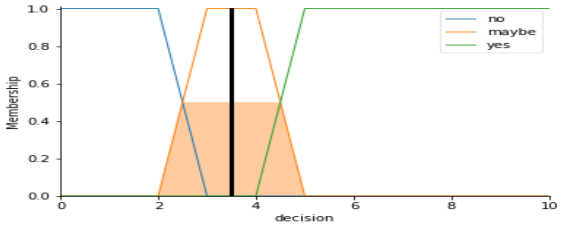

Figure 6: Maybe Decision Value

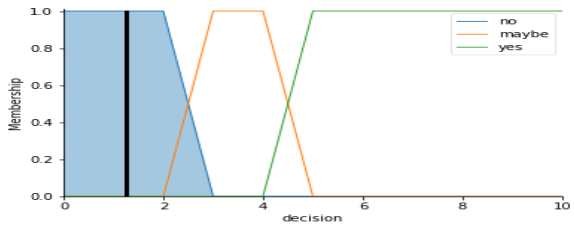

Figure 7: No Decision Value

5.1 Examples

In this section, we present the usability of our framework.

Let us assume Daniel has a photo with Alice, Bob, and Dan. Daniel notifies those people to solicit their ideas for sharing. She aims to share the photo with a group of her friends, which consists of five hundred people.

Example 1: Our framework continues with the co-owner trust preferential because Daniel chooses this option at the beginning.

We calculate the privacy loss with the data sensitivity and the number of authorised people by owner but unauthorised people by co-owners.

$$P_l(co) = S_d * |\frac{R_{co_i}^{'}}{R_{ci}}| \tag{10}$$

The privacy loss is calculated for co-owners who think their privacy is violated by the owner. Data security features choices show whether they worry about their privacy. If a co-owner chooses any of the data security features, then s/he shows her/his concern on the privacy. If there is no selection on the data security features, then we do not consider s/he worries about her privacy. We use the following rules for classifying users based on their concerns.

$full-worry : \forall i \in 1,2,.....,n : rate_i = 1$
$partly-worry : \exists i \in 1,2,.....,n : rate_i = 1$
$no-worry : \forall i \in 1,2,.....,n : rate_i = 0$

$$P_l(co) = S_d * |\frac{R_{coi}}{R_o}| \tag{11}$$

Equation 12 indicates the co-owners trust loss in owner if they are worried about any of the CIAPP data

Table 4: Co-owners' rates on data security features

Co-owner's id	Confidentiality	Integrity	Availability	Privacy	Possession
Alice	1	0	0	0	0
Bob	0	0	1	0	0
Dan	0	0	0	1	0
Alice	0	0	1	1	1
Bob	1	1	1	0	0
Dan	0	1	1	0	0

Table 5: Co-owners' relations with the targeted group's people

Co-owner's id	The number of known people in targeted group (NKP)
Alice	200
Bob	100
Dan	500

security features. It depends on the privacy loss if a co-owner does not have privacy loss, it means privacy loss means is 0, then we do not calculate the trust loss for them. If the privacy loss is not equal to 0, then trust loss is as follows;

$$Tl(pl) = \frac{1 - pl^n}{1 + pl^n} \tag{12}$$

In equation 12, n is the mood of co-owners, where n belongs to $\mathbb{N}$. The mood refers to states of co-owners' mind on the data sharing process.

Equation 13 is used for co-owners who do not consider that sharing the data cause the privacy violation (Xu et al., 2011). If someone is in the no-worry class and has the privacy loss value which is equal to 0, then the owner gains trust in them by sharing the data.

$$h(t_{co}) = t_{co}^{a}, (0 < a < 1)(Xu et\ al., 2011) \tag{13}$$

$$rep(u_i) = \frac{\sum_{u_j \neq u_i}(t_{ji})}{\sum_{i=1}^{i=n}(c_{oi})} \tag{14}$$

Equation 14 gives the calculation the owner's reputation. It is calculated with the summation of co-owners' trust in owner and the number of co-owners on the data. We can calculate the Daniel's reputation after he shared the data. The reputation value becomes rep(Daniel)= 0.33. Let us assume that his reputation value was 1 before he shared the data, and the new reputation value is calculated as follows;

$$Nrep(u_i) = |rep(u_i)' - rep(u_i)| \tag{15}$$

$Nrep(u_i)$ represents the new reputation value, $rep(u_i)'$ indicates the reputation value after sharing the data, and $rep(u_i)$ is the reputation value before the data was shared. $Nrep(Daniel) = 0.7$.

Case: Alice is owner of a data and chooses co-owner trust preferential: Let us assume Alice plans to have an event. She wants Daniel and Bob to participate for organizing it. Therefore, she notifies them and solicits their opinions to share event invitations. The targeted group for the event is Alice's friends, which consists of seven hundred people in it.

Table 11 shows the choices of Bob and Daniel on the data security features (CIAPP) .

The following tables show values of S_d, R,Cf, P_l, T_l, ht_{co}. Based on the rates of the data security features, they are both in partly-worry and full-worry class. Therefore, the trust loss value needs to be calculated for both of co-owners.

Case: Alice is owner of a data and chooses owner trust preferential: In this case, Our framework goes through with owner's trust preferential. The degree of a fuzzy decision is important. The fuzzy system involve two inputs: s_d and C_f. Table 13 represents the values of s_d and C_f. With regard to our fuzzy rules, the decision degree becomes $no_{0,2}$. This means that the framework will not share the data, since the degree of a decision does not belong to *Yes* or *Maybe*. Alice will not loss values on her reputation.

Example 2: The framework checks the fuzzy decision whether is *maybe* or *yes*. If it is not, then the system ends the process without sharing the data. If the decision is *maybe* or *yes*, then the framework checks the degree of decision if it is greater than 0.7, which is the transition value between yes and maybe, then the co-owned data is shared with no restricted permissions on it. However, if it is less than 0.7, then the data is shared with the 'like' and 'view' permissions. The reputation value is an updated end of the sharing processes.

6 Discussion

The important point of the proposed framework is that it involves using a fuzzy system and trust values between the owner and their co-owners . It encourages users to solicit co-owners' opinions before sharing the data. It has a kind of punishment and re-

Table 6: The values of Sensitivity, Relation, and Confidence

Case id	Sensitivity (sd)	Relations (R)	confidence (cf)
Case1	0.2	0.533	0.906
Case2	0.53	0.533	0.47

Table 7: Trust values before sharing the data

Daniel's Trust in Co-i	Co-id	Co-i s Trust in Daniel
0.5	Alice	0.7
0.8	Bob	0.6
0.3	Dan	1

Table 8: Privacy loss for each co-owner who are in class full-worry or partly-worry and co-owners' trust loss in owner

Case 1	Co-owner-id	privacy-loss	Trust-loss
Case1	Alice	0.12	0.78
	Bob	0.16	0.72
	Dan	0	NA

Table 9: Co-owners' trust gain in owner

Case 1	Co-owner-id	Trust-gain
Case1	Dan	1

Table 10: Trust values after sharing the data

Daniel's Trust in Co-i	Co-id	Co-i s Trust in Daniel
0.5	Alice	0
0.8	Bob	0
0.3	Dan	1

ward system in which if the owner shares data with the decision which is against the co-owners' decision, then s/he losses value on her reputation, otherwise, she gains value for her reputation.

For the experimental study on the fuzzy decision making part, we use simulated data as mentioned in the data preparation section. The ranges of values are given in the same section. The data set includes data sensitivity S_d, which is simulated with the equation 8, the confidence value for the targeted group, and decision that is taken with the fuzzy system. The result of a fuzzy decision making system is shown in Table 3. Our data set is based on the subjective evaluations, i.e., the experts make the evaluations and the rules' definitions are based on experts' knowledge. While the decision making system was built upon trust and share rules, in this context, the phenomenon is that if you trust someone, then you share your data. However, you do not trust your data with untrusted people.

In comparison with the previous studies on collaborative privacy management in OSNs, our framework involves various approaches for collaborative privacy management in OSNs. Previous studies either allow owner to share co-owned data without asking co-owners' opinions , or they ask co-owners whether their decision is yes or no. However, a real decision is generally not, Fuzzy Logic allows an intensity score of the decision to be ranged from 0 to 1. In our case, we used the fuzzy logic context on the decision making part and use the outcome value in the data sharing process. In addition, co-owned data sensitivity is settled only by the owner in the previous studies. However, the sensitivity is also co-owners' concerns. Therefore, our framework allows co-owners to express their concerns on data sensitivity with CIAPP security features. Our framework encourages owners to solicit their co-owners opinions when the co-owned data is intent to share. At the end of the data process, if the owner makes a decision in favour of co-owners, then most possibly the reputation of the owner is not damaged. Otherwise, the owner looses the value on reputation.

This work proposes an effective fuzzy decision based collaborative privacy management framework for Online Social Networks. The fuzzy approach is used for making decision based on the data sensitivity and the confidence value in the targeted group in Online Social Networks. One of the aims is to use a fuzzy decision making system instead of asking co-owners' decision whether the data is shared, i.e., we ask co-owners which data security features (CIAPP) are in threat if the data is shared with people who will access the data. Another aim of this work is to encourage users to preserve co-owners privacy. The trust gain and the trust loss values are used for the benefit of owner and co-owners. In example 1 and example 2, we show the effects of trust gain and trust loss values on owner's reputation.

7 Conclusion

In this paper, we have proposed an effective framework which has a fuzzy logic based decision system and provides a collaborative privacy management on co-owned data in OSNs. To help the co-owners on decision of sharing co-owned data, we use related data security features (CIAPP) and ask co-owners concerns on CIAPP. In our work, co-owners are not forced to give their Boolean decision (0 or 1), all they need to do is to choose CIAPP features

Table 11: Co-owners' rates on data security features

Co-owner's id	Confidentiality	Integrity	Availability	Privacy	Possession	NKP
Bob	1	1	1	0	0	100
Daniel	1	1	1	1	1	0

Table 12: Trust values before sharing the data

Alice's Trust in Co-i	Co-id	Co-i s Trust in Alice	$p-loss$	$T-loss$	final-trust-in Alice
0.6	Bob	0.7	0.68	0.47	0.23
0	Daniel	0.5	0.8	0.21	0.29

Table 13: Co-owners' rates on data security features

S_d	R	Cf
0.8	0.07	0.256

that may be a reason for their information violation. When an owner wants to share data, it is needed to set the privacy policy on the data *i.e targeted group, co-owners of the data, owner trust or co-owner trust preferential*. Then the owner notifies co-owners and asks their opinions on the CIAPP features. Once co-owners choose which CIAPP features are their worries, then the fuzzy logic based decision system infers the decision. After getting the decision from the fuzzy logic based system, our system goes through the sharing process. If the owner choose the co-owner trust preferential when they set their privacy policy up on the data, then our system calculates the privacy loss, the trust loss, and the trust gain values. If the owner shares the data with targeted group without considering the co-owners' choices on the CIAPP features, the the owner looses the value on their reputation. However, if the owner chooses the owner trust preferential in the beginning, then they do not loss value on their reputation, since the fuzzy decision is based on the co-owners choices on CIAPP features. It is clearly seen that the fuzzy logic decision based system helps users to make trade-off sharing the data and getting benefits out of sharing data with increment on the reputation value.

REFERENCES

Ali, S., Rauf, A., Islam, N., and Farman, H. (2017). A framework for secure and privacy protected collaborative contents sharing using public osn. *Cluster Computing*.

Cherdantseva, Y. and Hilton, J. (2012). The evolution of information security goals from the 1960s to today. *Unpublished*.

Du, J., Jiang, C., Chen, K.-C., Ren, Y., and Poor, H. V. (2018). Community-structured evolutionary game for privacy protection in social networks. *IEEE Transactions on Information Forensics and Security*, 13(3):574–589.

Hagberg, A., Swart, P., and S Chult, D. (2008). Exploring network structure, dynamics, and function using networkx. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States).

Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., and Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung cad classification system. *IEEE Transactions on Fuzzy Systems*, 20(2):224–234.

Hu, H. and Ahn, G.-J. (2011). Multiparty authorization framework for data sharing in online social networks. In Li, Y., editor, *Data and Applications Security and Privacy XXV*, pages 29–43, Berlin, Heidelberg. Springer Berlin Heidelberg.

Hu, V. C., Kuhn, D. R., and Ferraiolo, D. F. (2015). Attribute based access control. *IEEE Computer Society*, 48(1):85–88.

Jamsandekar, S. S. and Mudholkar, R. R. (2014). Fuzzy classification system by self generated membership function using clustering technique. *BVICA M's International Journal of Information Technology*, 6(1):697.

Joseph, N. S. (2014). Collaborative data sharing in online social network resolving privacy risk and sharing loss. *IOSR-JCE) eISSN*, pages 2278–0661.

Koyuncu, M. and Yazici, A. (2005). A fuzzy knowledge-based system for intelligent retrieval. *IEEE Transactions on Fuzzy Systems*, 13(3):317–330.

Mamdani, E. and Assilian, S. (1999). An experiment in linguistic synthesis with a fuzzy logic controller. *International journal of human-computer studies*, 51(2):135–147.

Rathore, N. C. and Tripathy, S. (2017). A trust-based collaborative access control model with policy aggregation for online social networks. *Social Network Analysis and Mining*, 7(1):7.

snap Facebook Data, S. (2016). Stanford large network dataset collection. www.kaggle.com/lightcc/stanford-snap-facebook-data.

Squicciarini, A. C., Shehab, M., and Paci, F. (2009). Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*, pages 521–530. ACM.

Suvitha.D (2014). Mechanisms of multiparty access control in online social network. *International Journal of*

Recent Development in Engineering and Technology, 2, (3).

Ulusoy, O. (2018). Collaborative privacy management in online social networks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 1788–1790. International Foundation for Autonomous Agents and Multiagent Systems.

Wishart, R., Corapi, D., Marinovic, S., and Sloman, M. (2010). Collaborative privacy policy authoring in a social networking context. In *Policies for distributed systems and networks (POLICY), 2010 IEEE international symposium on*, pages 1–8. IEEE.

Xu, L., Jiang, C., He, N., Han, Z., and Benslimane, A. (2019). Trust-based collaborative privacy management in online social networks. *IEEE Transactions on Information Forensics and Security*, 14(1):48–60.

Xu, S., Li, X., Parker, T. P., and Wang, X. (2011). Exploiting trust-based social networks for distributed protection of sensitive data. *IEEE Transactions on Information Forensics and Security*, 6(1):39–52.