International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 3767~3776
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp3767-3776

Policy resolution of shared data in online social networks

Nisha P. Shetty, Balachandra Muniyal, Saleh Mowla
Department of Information and Communication Technology, Manipal Institute of Technology,
Manipal Academy of Higher Education, India

Article Info

Article history:

Received Oct 4, 2019
Revised Jan 13, 2020
Accepted Feb 2, 2020

Keywords:

Fuzzy logic
OSN
Privacy
Shared data

ABSTRACT

Online social networks have practically a go-to source for information divulging, social exchanges and finding new friends. The popularity of such sites is so profound that they are widely used by people belonging to different age groups and various regions. Widespread use of such sites has given rise to privacy and security issues. This paper proposes a set of rules to be incorporated to safeguard the privacy policies of related users while sharing information and other forms of media online. The proposed access control network takes into account the content sensitivity and confidence level of the accessor to resolve the conflicting privacy policies of the co-owners.

Corresponding Author:

Balachandra Muniyal,
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal Academy of Higher Education,
Manipal- 576104, Karnataka, India.
Email: bala.chandra@manipal.edu

1. INTRODUCTION

Online Social Networks (OSNs) have become one of the most popular means of communication and information sharing in the modern era. Platforms such as Facebook, Instagram, Twitter, etc. encourage users to spend time on the respective platform through engaging content, advertisements, etc. However, as time passed by, the leakage of confidential information to the unintended audience became prevalent and a cause for concern for the users. Every social media platform has its own set of policies which they implement to protect the privacy of their users, but the goal of absolute privacy has still not yet been achieved [1]. The evolution, accessibility and improved usability of OSNs this past decade has resulted in the sharing and upload of vast amount of data and media. Consequently, it has become physically impossible to keep track of the data being stored and retrieved through these social platforms [2]. In addition, there has been an increase in the number of attacks which affect users in OSNs ranging from privacy breaches to network structural attacks [3] and even viral marketing [4]. Privacy related attacks have been further compounded due to the increased visibility of user's contents promoted through likes, shares, comments and other forms of user interactions. The paper will briefly explain the disadvantages of the current system in place and illustrates the implementation of a security model to safeguard user's privacy preferences and resolve conflicts between different parties.

Privacy preferences of users in OSNs can be violated in different ways. In a hypothetical example on Facebook, if Alice shares a post and tags Bob, Bob can lower the visibility of the post to audiences belonging to his friend's list but has no control over those belonging to Alice's friend's list. Even though Bob can remove the associated tag himself, the post can still be visible on other parts of Facebook. This scenario does not account for those cases where the related users are not tagged but the content is shared nonetheless.

To tackle issues related to privacy, policies have been enforced by OSNs giving the users flexibility to control who can view, react, comment or share the content they post on their profiles. Although these steps have lowered the visibility of users' contents to the unintended audience, users have limited flexibility in

controlling what other users post on their respective profiles. In such scenarios, the privacy policies of the owner of the data item may get enforced but it can lead to a conflict of interest or violate privacy preferences of users who may get affected by the respective data item related to them. Putting these challenges into perspective, it has become necessary to design a model or workflow which considers the preferences of every user and resolve any privacy conflicts which may arise due to the differing user opinion with respect to a shared data item.

Many authors have conducted research work and proposed models in order to achieve collaborative privacy management of shared data items in OSNs. Sindhu and Bhuvaneswari summarizes a survey they have conducted on various techniques and algorithms proposed by different researchers and concluded that there is a lack of multiparty privacy management support offered by the OSNs due to which users are unable to control which data items should be visible or shared to the targeted audience [5]. Rathore and Somanath proposes a collaborative access control for OSN (CACO) model that uses the degree of intimacy between the related parties viz. the stakeholders and the requesting users to determine the access decision [6]. Hu, Ahn and Jorgensan formulated a multiparty access control (MPAC) model as well as a multiparty policy specification scheme. They also implemented a proof-of-concept prototype called 'MController' which took into consideration the content sensitivity level assigned by the co-owners of the shared data item and the weights assigned to the multiple parties by the owner of the shared data item [7]. Such and Criado discuss the limited support for multiparty privacy offered by various OSNs and the strategies that users follow to overcome the limitations. As a result of their study, they outline a set of requirements to design and develop multiparty privacy management tools [8]. In another paper, they present a mechanism to detect privacy conflicts in OSNs and resolve them using a mediator. The mediator determines if a conflict exists based on the privacy policies associated with a shared data item and attempt to provide a solution if a conflict exists [9]. Ali et.al. proposes a framework which introduces an access management server. The server acts as a middleware between the users and the OSN server. Their framework emphasizes the protection of user privacy from unauthorized users as well as the OSN service provider using cryptographic based techniques [10].

Cheng, Park and Sandhu integrates attribute-based policies into relationship-based access control (ReBAC) in order to enhance access control capability and allow finer-grained control which are not available by simple using ReBAC [11]. The research by Shan et. al. proposes an attribute and relationship-based hybrid access control (HAC) model for OSNs based on policy language and path checking [12]. Carminati, Ferrari and Perego presented an access control model for web based social networks. In their model, the policies are formed as a result of constraints on the type of relationship which exist between users as well as the depth of the relationship [13]. In another paper, Carminati and Ferrari propose a solution which uses cryptographic and digital signature techniques to ensure that the privacy of the users is guaranteed during the collaboration process [14]. Nithya S. Joseph discusses a method for collaborative data sharing as well as a method to resolve privacy conflicts to ensure better protection against collusion attacks [15]. In their paper, Rathore and Tripathy propose a trust-based access control technique to allow or disallow the sharing of the resource taking into consideration the authorization requirements of all the multiple parties and analyzes the privacy risk of the model [16]. Wishart et.al. proposes a privacy-aware social networking service and then introduce a collaborative approach to authoring privacy policies for the service. Their approach considers the needs of all parties affected by content and information disclosed [17]. Xu et.al. proposes a trust-based mechanism to realize collaborative privacy management. In their model, the user makes the decision of whether or not to post a data item based on the aggregated responses of the users related to the data item. The weight factor which has been considered is the trust value between the users, and the values are updated according to users' privacy loss [18]. Akkuzu, Aziz and Adda uses fuzzy logic rules to determine access to a shared data item based on the content sensitivity of the data item and the confidence that the co-owners have on the owner of the data item [19].

In this paper, a collaborative model is proposed in which the fuzzy logic rules will be based on the mean content sensitivity level of the shared data item and the mean confidence that the co-owners have on the accessor of the data item. The model thus removes complete preference given to the owner of the shared data item [20] and allows co-owners a fair chance to enforce their privacy policies in spaces which in the present scenario, are out of their control. The privacy policies which have been taken into consideration are 'View Policy', 'React Policy', 'Comment Policy' and 'Sharing Policy' for a shared data item on Facebook. The model assumes that the users are notified of the shared data item either by 'tags' which were added by the owner or by Facebook's user identification system achieved through facial recognition techniques.

2. PROPOSED MODEL

This section describes the proposed model which has been based on the principles of fuzzy logic rules. The model will show how the privacy policies of a shared data item will be managed based on two aspects viz. content sensitivity level of the shared data item and the confidence level (or trust) that the co-owners have on the user trying to access the resource.

2.1. Definitions and assumptions

The following terms, definitions and assumptions [21, 22] will be used to describe the proposed model of the system.

a. Shared Data Item (D). A shared data item D can be a post, image, video or any content which is related to more than one user and which is jointly owned by the related users.
b. Co-owner (C_i). A co-owner of a shared data item D is a user who jointly owns D along with other users or has some authority to control the privacy policies concerning D. For a shared data item D, there can be *n* number of co-owners and C_i is the i^{th} co-owner of D where $i \in [1, 2, \ldots, n]$. C_1 is the *owner* of D i.e. the user who originally shares D.
c. Accessor (A). An accessor is any user who wishes to access the shared data item D or perform any action on D. An accessor can be friends, friends of friends, family members or anyone from the general public.
d. Mean Content Sensitivity Level ($CSL_{mean}(D)$): The mean content sensitivity level of a shared data item D is the average of the sensitivity level attributed to D by the related co-owners.

$$CSL_{mean}(D) = \Sigma CSL_i(D) / n \; ; \; i \in [1, 2, \ldots, n] \; , \; CSL_i(D) \in [0, 2, \ldots, 10]$$

The $CSL_i(D)$ values ranges from 0 (very low sensitivity) to 10 (very high sensitivity) which will be determined by the i^{th} co-owner for the shared data item D. These values will be normalized between 0 to 1 when the model will apply the fuzzification process.

e. Mean Confidence Level ($CONF_{mean}(D, A)$). The mean confidence level for an accessor A is the average of the quantifiable measure of trust attributed by the co-owners for accessor A for a given shared data item D.

$$CONF_{mean}(D, A) = \Sigma CONF_i(D, A) / n \; ; \; i \in [1, 2, \ldots, n] \; , \; CONF_i(D, A) \in [0, 0.05, 0.1 \ldots, 1]$$

The $CONF_i(D, A)$ values ranges from 0 (no confidence) to 10 (full confidence) which will be determined by the i^{th} co-owner for the shared data item D. These values will be normalized between 0 to 1 when the model will apply the fuzzification process.

f. Privacy Policies (PP(D, A)). The privacy policies for a shared data item D is a set of policies which determines the privilege granted to an accessor A. The model assumes these policies to be the 'View Policy', 'React Policy', 'Comment Policy' and 'Sharing Policy'. These policies are attributed Boolean values of 0 and 1 determined after applying the fuzzy logic rules. If a policy is attributed with the value of 0, the accessor A will be denied access or perform the privilege predetermined by the policy with respect to the data item D, otherwise the accessor A is given the required access. The model assumes that each privacy policy is a function of the mean content sensitivity level ($CSL_{mean}(D)$) and mean confidence level ($CONF_{mean}(D, A)$). As each policy is different in its own respect, it is assumed that the fuzzy logic rules for each privacy policy will be different, thereby granting the system flexibility in determining the rules for the respective policies.

2.2. Fuzzy model overview

The decision-making model that was chosen is based on the principles of fuzzy logic i.e. decisions cannot entirely be Boolean in nature. The model assumes that each co-owner of the shared data item has varying levels of confidence (or trust) on the different accessors. The decision being made will be based on the content sensitivity of the data item and the confidence that the co-owners have on the different accessors.

In general, a fuzzy logic decision-based system follows a broad procedure which includes *fuzzification, inference* and defuzzification. *Fuzzification* is the process where crisp values are taken as input to obtain membership degree values. *Inference* involves determining a predetermined fuzzy decision by aggregating the fuzzy inputs obtained from *fuzzification* to obtain the overall membership degree. *Defuzzification* is the process where the overall membership degree of the fuzzy decision is mapped to a crisp value. The general fuzzification model can be observed in Figure 1. For the purpose of inference and defuzzification, the model adopts the Mamdani-style inference. Based on the crisp value obtained after the defuzzification process, the model will determine if the accessor is permitted to access or perform an action on a shared data item.

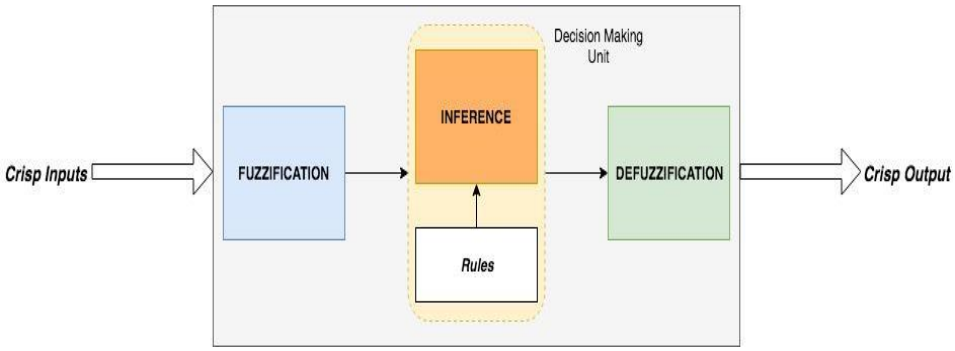

Figure 1. General fuzzification model

2.2.1. Membership functions and fuzzification

For the process of fuzzification, the linguistic variable inputs need to be identified first. In the proposed model, these variables are the mean content sensitivity level of the shared data item and mean confidence level attributed to the accessor by the co-owners. Figures 2 and 3 represent the membership functions of the linguistic variables of mean content sensitivity level and mean confidence level respectively which are attributed by the co-owners of the shared data item. Figure 4 shows the output membership functions of the 'Comment Policy'.

For mean content sensitivity level, the model has assumed the membership functions to be 'Very Low', 'Low', 'Medium', 'High' and 'Very High'. Similarly, for mean confidence level, the model assumes the membership functions to be 'Very Low', 'Low', 'Medium', 'High' and 'Very High'. The output membership functions are 'Deny', 'Maybe' and 'Permit' which will determine the respective privacy policy for a particular accessor.

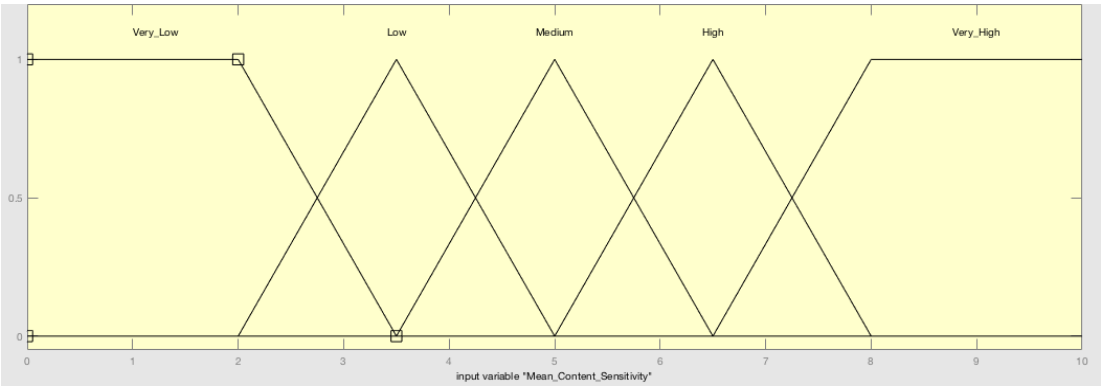

Figure 2. Membership functions of mean content sensitivity level

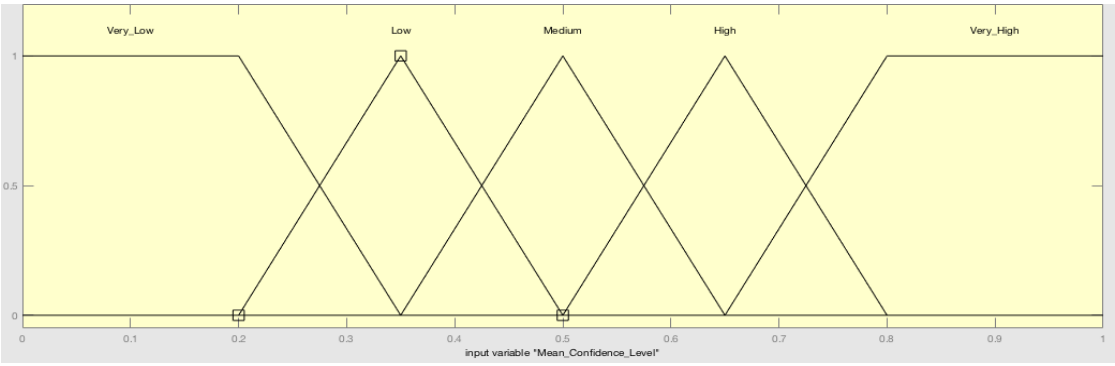

Figure 3. Membership functions of mean confidence level

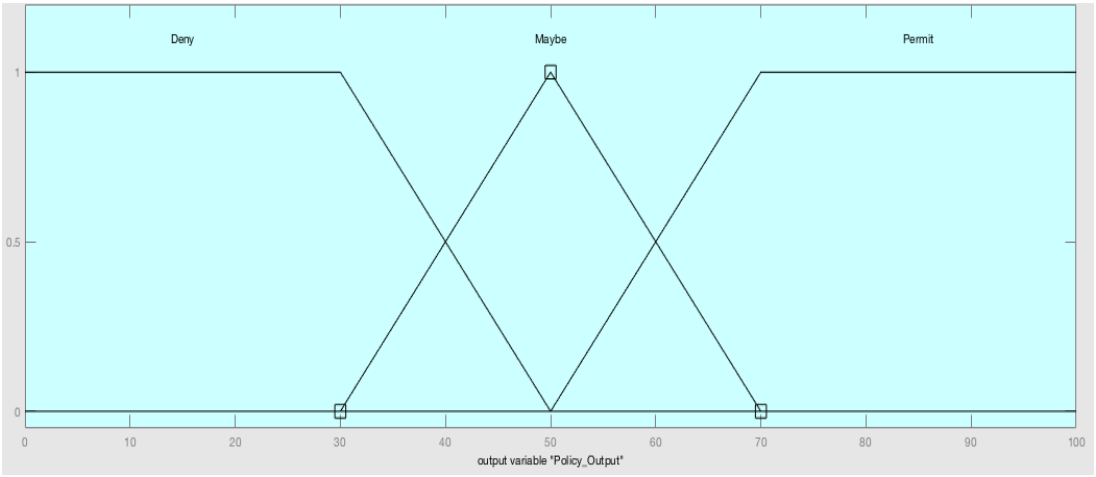

Figure 4. Output membership functions of the comment policy

2.2.2. Fuzzy rules and inference [23, 24]

Based on the fuzzy rules, a fuzzy inference viz. an output that is not entirely Boolean is obtained. Fuzzy logic rules are defined in the following format:

IF *x* is *A* AND *y* is *B* THEN *z* is *C*

where x, y and z are linguistic variables; A, B and C are fuzzy sets belonging to their respective fuzzy inputs X, Y and Z. These rules are made in order to infer the fuzzy outputs.

The model assumes that for each privacy policies, different sets of rules need to be applied. Table 1 shows a set of rules which have been defined for the 'Comment Policy' and Table 2 summarizes the contents of Table 1 in the form of fuzzy matrix. Additional sets of rules can be made similarly for the 'View Policy', 'React Policy' and 'Share Policy'.

Table 1. Definition of fuzzy logic rules for the comment policy

S.N.	Antecedent (IF)	Consequent (THEN)
1.	IF $CSL_{nean}(D)$ is 'Very Low' and $CONF_{mean}(D,A)$ is 'Very Low'	THEN $PP_{comment}(D,A)$ is 'Maybe'
2.	IF $CSL_{nean}(D)$ is 'Very Low' and $CONF_{mean}(D,A)$ is 'Low'	THEN $PP_{comment}(D,A)$ is 'Permit'
3.	IF $CSL_{nean}(D)$ is 'Very Low' and $CONF_{mean}(D,A)$ is 'Medium'	THEN $PP_{comment}(D,A)$ is 'Permit'
4.	IF $CSL_{nean}(D)$ is 'Very Low' and $CONF_{mean}(D,A)$ is 'High'	THEN $PP_{comment}(D,A)$ is 'Permit'
5.	IF $CSL_{nean}(D)$ is 'Very Low' and $CONF_{mean}(D,A)$ is 'Very High'	THEN $PP_{comment}(D,A)$ is 'Permit'
6.	IF $CSL_{nean}(D)$ is 'Low' and $CONF_{mean}(D,A)$ is 'Very Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
7.	IF $CSL_{nean}(D)$ is 'Low' and $CONF_{mean}(D,A)$ is 'Low'	THEN $PP_{comment}(D,A)$ is 'Maybe'
8.	IF $CSL_{nean}(D)$ is 'Low' and $CONF_{mean}(D,A)$ is 'Medium'	THEN $PP_{comment}(D,A)$ is 'Permit'
9.	IF $CSL_{nean}(D)$ is 'Low' and $CONF_{mean}(D,A)$ is 'High'	THEN $PP_{comment}(D,A)$ is 'Permit'
10.	IF $CSL_{nean}(D)$ is 'Low' and $CONF_{mean}(D,A)$ is 'Very High'	THEN $PP_{comment}(D,A)$ is 'Permit'
11.	IF $CSL_{nean}(D)$ is 'Medium' and $CONF_{mean}(D,A)$ is 'Very Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
12.	IF $CSL_{nean}(D)$ is 'Medium' and $CONF_{mean}(D,A)$ is 'Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
13.	IF $CSL_{nean}(D)$ is 'Medium' and $CONF_{mean}(D,A)$ is 'Medium'	THEN $PP_{comment}(D,A)$ is 'Maybe'
14.	IF $CSL_{nean}(D)$ is 'Medium' and $CONF_{mean}(D,A)$ is 'High'	THEN $PP_{comment}(D,A)$ is 'Permit'
15.	IF $CSL_{nean}(D)$ is 'Medium' and $CONF_{mean}(D,A)$ is 'Very High'	THEN $PP_{comment}(D,A)$ is 'Permit'
16.	IF $CSL_{nean}(D)$ is 'High' and $CONF_{mean}(D,A)$ is 'Very Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
17.	IF $CSL_{nean}(D)$ is 'High' and $CONF_{mean}(D,A)$ is 'Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
18.	IF $CSL_{nean}(D)$ is 'High' and $CONF_{mean}(D,A)$ is 'Medium'	THEN $PP_{comment}(D,A)$ is 'Deny'
19.	IF $CSL_{nean}(D)$ is 'High' and $CONF_{mean}(D,A)$ is 'High'	THEN $PP_{comment}(D,A)$ is 'Maybe'
20.	IF $CSL_{nean}(D)$ is 'High' and $CONF_{mean}(D,A)$ is 'Very High'	THEN $PP_{comment}(D,A)$ is 'Permit'
21.	IF $CSL_{nean}(D)$ is 'Very High' and $CONF_{mean}(D,A)$ is 'Very Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
22.	IF $CSL_{nean}(D)$ is 'Very High' and $CONF_{mean}(D,A)$ is 'Low'	THEN $PP_{comment}(D,A)$ is 'Deny'
23.	IF $CSL_{nean}(D)$ is 'Very High' and $CONF_{mean}(D,A)$ is 'Medium'	THEN $PP_{comment}(D,A)$ is 'Deny'
24.	IF $CSL_{nean}(D)$ is 'Very High' and $CONF_{mean}(D,A)$ is 'High'	THEN $PP_{comment}(D,A)$ is 'Deny'
25.	IF $CSL_{nean}(D)$ is 'Very High' and $CONF_{mean}(D,A)$ is 'Very High'	THEN $PP_{comment}(D,A)$ is 'Maybe'

Table 2. Fuzzy matrix

Parameters		$CSL_{nean}(D)$				
		Very Low	Low	Medium	High	Very High
$CONF_{mean}(D, A)$	Very Low	Maybe	Deny	Deny	Deny	Deny
	Low	Permit	Maybe	Deny	Deny	Deny
	Medium	Permit	Permit	Maybe	Deny	Deny
	High	Permit	Permit	Permit	Maybe	Deny
	Very High	Permit	Permit	Permit	Permit	Maybe

2.2.3. Defuzzification

This object of the defuzzification process is to obtain a crisp output value based on the rule inference obtained in the inference process. Using the crisp value, an algorithm can be formulated in order to make the final decision to determine a privacy policy for a data item to be accessed by an accessor. There are many ways to perform defuzzification. The fuzzy model designed will obtain the crisp value by following the centroid technique. This is achieved by:

- Computing the centroid of the output membership functions.
- Limiting the height of each membership function by obtaining the degree of membership of the respective outputs and computing the resulting area.
- Computing the weighted average of the centroids using the computed areas.

3. RESEARCH METHOD

The following algorithm 1 gives an overview of the steps which will be followed by the model to determine the resolution of the privacy policies of the co-owners of the given shared data item. The process first begins when the co-owners of the shared data item D determines its content sensitivity from a range of 0 to 10, 0 denoting extremely low content sensitivity and 10 denoting extremely high content sensitivity. After setting the content sensitivity of D, co-owners will proceed to determine the confidence level of an accessor based on the type of relationship between the accessor and the respective co-owner; for example, 'friends', 'friends of friends', 'family', 'close friends', etc. The values of the confidence level will range between 0% and 100%; 0% denoting no confidence and 100% denoting full confidence. The co-owners will assign each group of accessors a value which denotes how much he or she considers a particular group of accessors trustworthy to access or perform actions on D. The algorithm will thus calculate the mean content sensitivity and mean confidence level which will be used as crisp inputs to the fuzzy model. On the basis of the crisp inputs, pre-defined rules and the relevant membership functions, the fuzzy model will make an inference. If the inference is 'DENY' or 'PERMIT', access to the respective privacy policy will denied or permitted respectively. However, if the inference is 'MAYBE', the model will proceed to apply defuzzification and find a crisp output. If the crisp output is less than the mean centroid value of 'MAYBE' and 'PERMIT' output membership functions, then the final decision for the respective privacy policy will be 'DENY', or else the final decision will be 'PERMIT'. Figure 5 shows a 3-dimensional plot of the fuzzy model proposed.

Algorithm 1. Model workflow

```
Let
D : Shared Data Item
A : Accessor of Shared Data Item D
CSLi(D) : Content Sensitivity Level set by the ith Co-owner of D
CONFi(D) : Confidence Level set by the ith Co-owner of D
PP(D,A) : Privacy Policies on D for a given Accessor A
        = [view_policy(D,A), react_policy(D,A), comment_policy(D,A), share_policy(D,A)]
n : Number of Co-owners
CSLmean(D) : Mean Content Sensitivity Level for D
        = ΣCSLi(D) / n
CONFmean(D, A) : Mean Confidence Level on Accessor A for D
        = ΣCONFi(D, A) / n

FOREACH(PP(D,A) as p)
        fuzzyOutputs[] = applyFuzzyRules(p, CSLmean(D), CONFmean(D, A));
        fuzzyInference = aggregrateOutputs(fuzzyOutputs);
        IF(fuzzyInference == 'DENY') THEN
                p = 'DENY';
```

```
        ELSE IF (fuzzyInference == 'MAYBE')
                crispResult == applyDefuzzification(p, fuzzyOutputs);
                meanCentroidValue = getMeanCentroidValue('MAYBE', 'PERMIT');
                IF(crispResult < meanCentroidValue)
                        p = 'DENY';
                ELSE
                        p = 'PERMIT';
                ENDIF
        ELSE
                p = 'PERMIT';
        ENDIF
ENDFOREACH
```

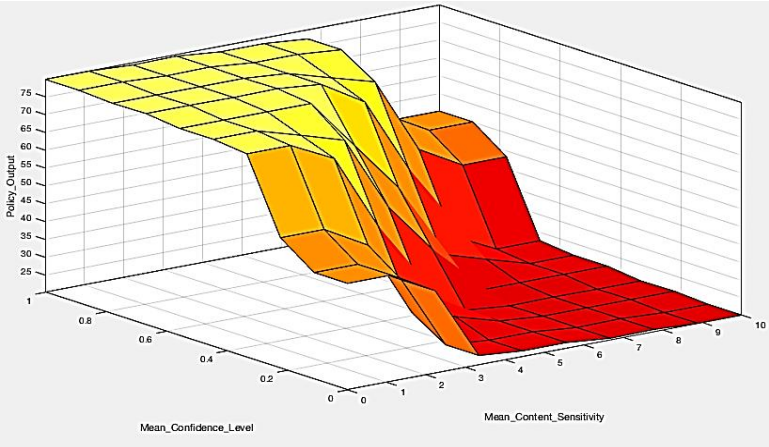

Figure 5. 3 Dimensional plot of the fuzzy model proposed

4. RESULT AND DISCUSSIONS

This section will explain the usability and evaluation of the model with a case scenario which is followed by the analysis of the model and related discussions.

4.1. Model evaluation

In this scenario, Bob, Mary, Alice and John are four friends. Bob shares a picture of all of them hanging out on his profile and tags them. All four of them are co-owners of the picture shared by Bob. Even though Bob has no concerns of making the picture public, Alice, Mary and John have their own set of privacy preferences and want to limit the visibility of the picture. Each of them assigns a content sensitivity level to the picture (from 0 to 10) and depending on the type of relationships they have with different users or accessors, they set their confidence level accordingly for different groups of accessors. Table 3 shows a sample set of possible inputs from Bob, Mary, Alice and John and the mean output. Table 4 shows a sample set of confidence level inputs by the four co-owners for different groups of accessors. During the retrieval of shared data content in an accessors' feed, the model will evaluate the privacy policies of the shared picture and accordingly determine the appropriate access. Table 5 shows the mean confidence level for a user named Jack who is an accessor.

Table 6 summarizes the different outputs obtained after the rule evaluation process (refer to the rules for the 'Comment Policy' in Table 1). Based on the outputs obtained, the model will aggregate them to make an inference. Aggregation can be achieved in different ways, but the most common method is to choose the fuzzy set which has the highest confidence value. In this scenario, the model makes an inference of 'DENY' as it has the highest confidence value from the other output membership functions. For comparison purposes, the crisp output obtained after performing defuzzification of the inference using the weighted centroid technique was computed as 41.4 based on the crisp inputs. However, the inference was 'DENY', the algorithm would have determined that the 'Comment Policy' for the accessor named Jack for the shared data item D co-owned by Bob, Mary, John and Alice is 'DENY'. As a result, Jack would be unable to comment on the shared data item D. Similarly, different rules can be applied for the 'View Policy',

'React Policy', 'Share Policy' or other relevant policies and an inference can be made to resolve the respective privacy policy for a shared data item for any accessor requesting access.

Table 3. Sample inputs

S.N.	Name of Co-owner	Sensitivity level (0 - 10)	Mean content sensitivity of shared data item D
1.	Bob	3.0	6.0
2.	Mary	7.0	
3.	John	6.0	
4.	Alice	8.0	

Table 4. Sample confidence level inputs

S.N.	Name of Co-owner	Relationship with accessor	Confidence / trust level (0 - 100%)
1.	Bob	No relation (public)	40%
2.		Friends of friends	65%
3.		Friends	90%
4.		Close friends	100%
5.	Mary	No relation (public)	20%
6.		Friends of friends	40%
7.		Friends	50%
8.		Close friends	70%
9.	Jhon	No relation (public)	30%
10.		Friends of friends	55%
11.		Friends	60%
12.		Close friends	70%
13.	Alice	No relation (public)	10%
14.		Friends of friends	20%
15.		Friends	45%
16.		Close friends	55%

Table 5. Mean confidence level calculation for accessor jack

S.N.	Name of Co-owner	Relationship with Jack	Confidence / trust level	Mean confidence level
1.	Bob	Close friends	100%	55%
2.	Mary	Friend of friend	40%	
3.	John	Friends	60%	
4.	Alice	Friend of friend	20%	

Table 6. Rule evaluation output for comment policy

S.N.	Input 1 (mean content sensitivity)	Input 2 (mean confidence level)	Output (comment policy)
1.	$Medium_{0.33}$	$Medium_{0.66}$	$Maybe_{0.33}$
2.	$Medium_{0.33}$	$High_{0.33}$	$Permit_{0.33}$
3.	$High_{0.66}$	$Medium_{0.66}$	$Deny_{0.66}$
4.	$High_{0.66}$	$High_{0.33}$	$Maybe_{0.33}$

4.2. Analysis and discussions

Given the amount of variance in users' opinions with regards to determining the sensitivity of the content and the trustworthiness of the accessors, the implementation of the model offers several advantages. The model firstly, takes into consideration every user or stakeholder who is concerned with the shared data and not just that of the owner. This solves the current problem in OSNs where the owner of the data can share content to a wide audience with limited restrictions. Another notable difference in this model from other implementations is that instead of evaluating the trustworthiness of the data owner (e.g. in [18]), it determines the trustworthiness of the users who are trying to access the shared data item. As a result of this, co-owners of the shared data are provided a safeguard to limit the visibility of the shared content from the unintended audience in case they find it sensitive in nature. In terms of usability, the implementation of this model eliminates the review of the data owner's privacy settings every time he or she disseminates a shared data item. By attributing the confidence level to the accessor instead of the data owner, it is easier for the users to set up default privacy configurations for every accessor based on their relationship with the respective user. The model can further be enhanced by enforcing fine-grained controls [25] to improve the performance. The model could also potentially be integrated with advanced facial recognition algorithms [26, 27] wherein the results of the model could determine whether tags should be generated automatically or not for the respective user based on his or her privacy policy preferences.

5. CONCLUSION AND FUTURE SCOPE

Social media, if used unwisely or in a carefree manner, can inadvertently lead to the dissemination of critical information. This paper proposes a multi-party access mechanism for shared data belonging to multiple concerned users, so that its access by malevolent users can be avoided or minimized to a great extent. The proposed method aims to resolve the conflicts which occur when the owner and other stakeholders have different views on the access rights of the shared data. The aim of this work is to automate the resolution process to ensure the impartial settlement of such conflicts. Future works involve introducing fine-grained negotiation between the various stakeholders to improve the efficiency of the resolution. Facial recognition algorithms are generating tags nowadays automatically, so new approaches must be put forth to provide added security in such cases.

REFERENCES

[1] K. Liang, J. K. Liu, R. Lu and D. S. Wong, "Privacy Concerns for Photo Sharing in Online Social Networks," *in IEEE Internet Computing*, vol. 19, no. 2, pp. 58-63, 2015. DOI: 10.1109/MIC.2014.107

[2] M. Smith, C. Szongott, B. Henne and G. von Voigt, "Big data privacy issues in public social media," *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Campione d'Italia,* pp. 1-6, 2012. DOI: 10.1109/DEST.2012.6227909.

[3] Y. Liu and N. Li, "Retrieving Hidden Friends: A Collusion Privacy Attack against Online Friend Search Engine," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 833-847, Apr. 2019. DOI: 10.1109/TIFS.2018.2866309.

[4] H. Gao, J. Hu, T. Huang, J. Wang and Y. Chen, "Security Issues in Online Social Networks," in *IEEE Internet Computing*, vol. 15, no. 4, pp. 56-63, Jul-Aug. 2011. DOI: 10.1109/MIC.2011.50.

[5] Sindhu S., and Bhuvaneswari A., "A Survey on Multi-Party Privacy Conflicts in Online Social Networks," *International Journal of Advanced Engineering and Global Technology*, vol. 04, no. 04, pp. 2073-2079, 2016.

[6] Rathore, Nemi and Somanath, Tripathy, "Collaborative access control model for OSN," *6th IEEE International Conference on Advanced Computing, At Bhimavaram Andra Pradesh India,* 2016.

[7] Hu Hongxin, Ahn, Gail-Joon and Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms. Knowledge and Data Engineering," *IEEE Transactions on Knowledge and Data Engineering,* vol. 25, no. 7, pp. 1614-1627, 2013.

[8] Such Jose and Criado Natalia, "Multiparty Privacy in Social Media," *Communications of the ACM,* vol. 61, no. 8, pp. 74-81, 2018.

[9] Such Jose and Criado Natalia, "Resolving Multi-Party Privacy Conflicts in Social Media," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 7, pp. 1-15, 2016.

[10] Ali Shaukat, Rauf Azhar, Islam Naveed and Farman Haleem, "A framework for secure and privacy protected collaborative contents sharing using public OSN," *Cluster Computing,* vol. 22, pp. 7275-7286, 2019.

[11] Cheng Yuan, Park Jaehong, Sandhu Ravi, "Attribute-Aware Relationship-Based Access Control for Online Social Networks," *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 292-306, 2014.

[12] Shan Fangfang, Li Hui, Li Fenghua, Guo Yunchuan, Niu Ben, "HAC: Hybrid Access Control for Online Social Networks," *Security and Communication Networks,* vol. 2018, pp. 1-11, 2018.

[13] Carminati Barbara, Ferrari Elena, Perego Andrea, "Rule-Based Access Control for Social Networks," *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops: OTM Confederated International Workshops and Posters, AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET, OnToContent, ORM, PerSys, OTM Academy Doctoral Consortium, RDDS, SWWS, and SeBGIS 2006,* Montpellier, France, October 29 - November 3, 2006. Proceedings, Part II, 2006.

[14] Carminati Barbara, Ferrari Elena, "Privacy-Aware Collaborative Access Control in Web-Based Social Networks," *IFIP Annual Conference on Data and Applications Security and Privacy,* pp. 81-96, 2008.

[15] Sara Joseph Nithya, "Collaborative data sharing in online social network resolving privacy risk and sharing loss," *IOSR Journal of Computer Engineering*, vol. 16, no. 5, pp. 55-61, 2014.

[16] Rathore N.C. and Tripathy S., "A trust-based collaborative access control model with policy aggregation for online social networks," *Social Network Analysis and Mining,* vol. 7, pp. 1-13, 2017.

[17] Wishart Ryan, Corapi Domenico, Marinovic Srdjan, Sloman Morris, "Collaborative Privacy Policy Authoring in a Social Networking Context," *Proceedings-2010 IEEE International Symposium on Policies for Distributed Systems and Networks*, pp. 1–8, 2010.

[18] Xu Lei, Jiang Chunxiao, He Nengqiang, Han Zhu and Benslimane Abderrahim, "Trust-Based Collaborative Privacy Management in Online Social Networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48-60, 2018.

[19] Akkuzu Gulsum, Aziz Benjamin and Adda Mo, "Fuzzy Logic Decision Based Collaborative Privacy Management Framework for Online Social Networks," *ICISSP 2019*, Prague - Czech Republic, 2019.

[20] Zheng B., *et al.*, "Scalable and Privacy-Preserving Data Sharing Based on Blockchain," *J. Comput. Sci. Technol.*, vol. 33, pp. 557–567, 2018.

[21] J. Sun, X. Zhu and Y. Fang, "A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation," *2010 Proceedings IEEE INFOCOM, San Diego, CA*, pp. 1-9, 2010.

[22] L. Xu, T. Bao, L. Zhu and Y. Zhang, "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," in *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 591-602, Mar. 2019.

[23] S. Begicheva, "Fuzzy Model for Evaluating the Quality of Medical Care," *2019 IEEE 21st Conference on Business Informatics (CBI)*, Moscow, Russia, pp. 5-8, 2019.
[24] J. Cózar, A. Fernández, F. Herrera and J. A. Gámez, "A Metahierarchical Rule Decision System to Design Robust Fuzzy Classifiers Based on Data Complexity," in *IEEE Transactions on Fuzzy Systems*, vol. 27, no. 4, pp. 701-715, Apr. 2019.
[25] Jianqiang Li, *et al*., "Enforcing Differential Privacy for Shared Collaborative Filtering," in *IEEE Access*, vol. 5, pp. 35-49, 2017.
[26] P. Jonathon Phillips, *et al.*, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," *Proceedings of the National Academy of Sciences*, 2018.
[27] H. Wang, J. Hu and W. Deng, "Face Feature Extraction: A Complete Review," in *IEEE Access*, vol. 6, pp. 6001-6039, 2018.

BIOGRAPHIES OF AUTHORS

Nisha P. Shetty has published in the areas network security and machine learning. Currently she is working in the area of social network security. She serves as Assistant Professor in in the Dept. of Information & Communication Technology, Manipal Institute of Technology, Manipal. She has completed her Bachelors and Masters in Computer Science and Engineering from Visvesvaraya Technological University, Karnataka, India. She is now pursuing her PhD. at Manipal Institute of Technology, MAHE, Manipal.

Dr. Balachandra's research area includes Network Security, Algorithms, and Operating systems. He has more than 30 publications in national and international conferences/journals. Currently he is working as the Professor and Head in the Dept. of Information & Communication Technology, Manipal Institute of Technology, Manipal. He has 25 years of teaching experience in various Institutes.

Saleh Mowla completed his B.Tech in Information and Communication Technology from Manipal Institute of Technology, Manipal, India. He has co-authored publications in the fields of Data Mining as well as Data Security in the healthcare sector. His primary research areas of interests are Data Mining, Cloud Computing, Databases and Software Engineering.