A Fuzzy Modeling Approach for Group Decision Making in Social Networks *

Gulsum Akkuzu[1], Benjamin Aziz[2], and Mo Adda[3]

University of Portsmouth, School of Computing, United Kingdom
gulsum.akkuzu@port.ac.uk
benjamin.aziz@port.ac.uk
mo.adda@port.ac.uk

Abstract. Social networks have been commonly used, people use social networks with various purposes, such as, enjoying time, making business, and contacting their friends. All these activities are mainly based on sharing data. In social networks, making decision on data sharing process has become one of the main challenge because it involves people who have different opinions on the same problem. Diversified opinions cause uncertainties in decision making process. Fuzzy logic is used to overcome uncertainties' situations. In this work, we provide a fuzzy logic based decision making framework for SNs. The proposed fuzzy logic based framework uses data sensitivity value and trust value (confidence value) to make the group decision. Users express their opinions on data security features to obtain aggregated decision. Facebook data sharing process is chosen as a case study.

Keywords: aggregated group decision making · social network · fuzzy systems.

1 Introduction

Social networks (SNs) enable users to communicate with each other via data sharing[1]. The common issue for SNs is to make decision on data which is related to more than one user [2–4], the reason is to reach aggregated decision on the data sharing process.

To obtain aggregated decision, group decision making (GDM) is proposed. GDM is a process that involves a group of people who state their opinions on different options in order to chose the best option [5–7]. In the traditional group decision making, decisions are made by administrators or experts even if the case related to different people. This case is still seen in many organisations where important decisions are made by restricted board of people. Urena et al. [9] compares the traditional group decision making ,in which the experts have just right to express their opinions on alternative situations, with social network. Based on their comparison, SNs bring the global group decision making which

* Supported by organization x.

means all people can give their opinions on a case which is related to them. Even though group decision making is possible in SNs, it is still a problem in many SNs especially in online social network (OSN) while data is shared. People either use the traditional decision making process even if the data is owned by different users. These confusions are because of the data is owned more than one user (data is called co-owned data), and having different decision criteria to share the data in OSNs. They also cause vagueness on decision making process. To overcome uncertainty situations fuzzy logic was introduced by Zadeh [8], the fuzzy logic resolves the uncertainties particularly in decision making process.

We introduce an aggregated group decision making system for SNs data sharing process, and introduce a fuzzy logic approach to deal with uncertainty situations while the decision is made. Two factors are important when the sharing decision is made on data. The first factor is the data sensitivity value and second one is the trust in the group of people who will have access the shared data. The proposed system provides alternatives to co-owners on the data security features which have effects on the data sensitivity value. Based on co-owners' choices the proposed fuzzy logic based system makes the final decision.

The rest of the paper is organised as follows. Section 2 gives similar research papers. Section 3 presents the proposed work's framework and its mathematical expressions. We introduce our fuzzy system in Section 4 with the experimental results. We finalise the work in Section 5.

2 Related Work

Group decision making is an important and challenging process, because it includes decision makers' doubts, problems, and uncertainties [10]. Therefore, finding appropriate ways to help decision makers is one of the key and critical point. The consensus-reaching process, which is an approach to get aggregated decision on final decision in group decision making problems, has been provided by researcher to help decision makers in social networks [5, 11, 12]. Wu and Chiclana [11] propose a trust based consensus approach to tackle group decision making problem. In work [12] consistency is used as an approach to control consensus-reaching process. Liang et al. [10] introduces an approach in which social connections of decision makers effect to get final aggregated decision in social networks. This work supports Liang et al. [10] on the point that shows users' relations have effects to make decision in SNs. Beside the users' relations, we also introduce the data sensitivity value has effect on decision making in SNs.

Fuzzy logic is an approach to tackle within ability of binary logic which is underlying on modern computer. Fuzzy logic is used to describe fuzziness, therefore, it can easily be applied to decision making. Fuzzy logic approach has been commonly used to tackle decision making problems with different alternatives in different areas such as education [13], health [14], Internet of Things [15], social networks [5, 9, 16, 17]. Due to fuzzy logic the effectiveness in decision making, it has also been applied to solve group decision making issues. Thirumalai and Senthilkumar [18] propose a fuzzy model to resolve the group decision making

problems in business area, the proposed approach uses membership and non-membership attributes to make the group decision. Similarly, Kahraman et al. [19] used the fuzzy logic to overcome group decision problems in facility location selection. This paper uses the fuzzy logic approach to remove uncertainties in group decision making process for SNs.

3 Background

This section introduces the models and the framework of this work.

3.1 CIAPP Security Model

To ensure the protection of data security; Confidentiality, Integrity, and Availability (CIA) model was developed, which is the model to guide policies to ensure the information security [20]. In CIA model, confidentiality is a boundary to limit access to information, integrity is a guarantee of limited access to the information, and availability is assured that the information is only accessed by authorised people [20, 21]. The information security is also needed in SNs in order to protect users' sensitive data [22]. The data sensitivity is a measurement that is calculated with the number of authorised people, however, Akkuzu et al. proposed a model in which Privacy and Possession features are added to extend CIA model [23]. The proposed model is CIAPP model in which Privacy and Possession are added to CIA model. Hence Privacy and Possession features are used to control information and network security. In SNs, users are asked directly to set the data sensitivity value [24] to define the level of data privacy. However, users may not be enough knowledgeable to set the data sensitivity value. It might be easier to ask their choices on the data security features, with their choices on the data security features the data sensitivity value can be calculated. To do so, we provide a model the CIAPP data security features are used to calculate the data sensitivity value. Table 1 indicates the related features to data sensitivity in OSNs. Table 1's features are deduced from [21], the information security subjects are divided into five circles based on the goals and disciplines. Deduced five features are combined to measure the data sensitivity in OSNs.

Table 1. Related Information Security Features to SNs

Subject of Protection	Discipline
Confidentiality,Integrity,Availability,Privacy	Information
Possession	Information and Network

3.2 Framework

Figure 1 introduces simply the structure of the framework for group decision. First, the data is uploaded by owner (the person who starts sharing process),

he decides the targeted group for the data, and lastly the owner notifies the co-owners to get their opinions on the data sharing process. Then, the process which is given in Figure 1 starts, co-owners are notified with the data and the targeted group which the data will be available for them. Once co-owners know which data is intended to be shared with whom, they select individually data security features (CIAPP) [21] that are seen as a threat for their privacy if the data is shared.

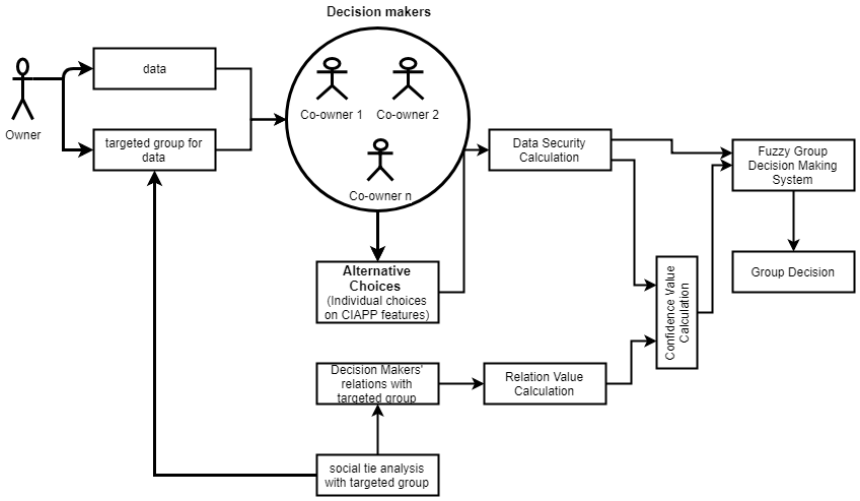

Fig. 1. The framework for group decision making with fuzzy system

3.3 Collective Measures for Decision Making

Collective measures are the models that are the main requirements for making decision, this is because they are used input values for fuzzy system.

$$S_d = \frac{\sum_{i=1}^{m}(P_i * (w_i))}{f} \tag{1}$$

S_d represents the data sensitivity, it ranges between [0,1]. The numerator gives the summation of the data Confidentiality, Integrity,Availability, Privacy, and Possession (CIAPP) [21] probabilities, in which P_i indicates the probability of CIAPP concerns that is chosen by co-owners and w_i is the weight of the properties. The denominator f indicates the total number of the features. Model 1 clearly indicates that the more worried users on the data sharing the higher sensitivity value. Also, more worrying data security features cause the higher data sensitivity value.

We model confidence value with the owner trust relation in the targeted group, co-owner trust relation in the targeted group, and the sensitivity value. We first show the calculation of trust relation;

$$R_o : f(r_{o1}, r_{o2}, ..., r_{osi}) = \frac{\sum_{j=1}^{s_i}(r_{oj})}{s_i} \tag{2}$$

R_o represents the owner's trust in each member of the targeted group and s_i represents the size of the targeted group. $f(r_{o1}, r_{o2}, r_{o3}, ..., r_{osi})$ represents the relation value between the data owner and each member in the targeted group.

$$R_{ci} : f(r_{c1}, r_{c2}, ..., r_{csi}) = \frac{\sum_{j=1}^{s_i}(r_{cj})}{s_i} \tag{3}$$

R_{ci} represents the co-owner's trust in each member of targeted group and s_i represents the size of the targeted group. From equation 2 and 3, we finalise the trust relation with the following formula;

$$R = \prod_{l=1}^{c} R_{li} * \prod_{k=1}^{c} R_{ki} \tag{4}$$

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 R_{ci}. R_{oi}, R_{ci} and R range $\in [0, 1]$.

With the equation 1,2 and 3 we can now calculate the Confidence value ($C_f \in [0, 1]$) in targeted group as follows;

$$C_f = 1 - S_d * (1 - R) \tag{5}$$

3.4 Proposed System's Social Network Analysis for GDM

A social network is a platform in which users communicate with each other via data. It is represented with a graph *G(V,E)*, with nodes V representing users V=$V_1, V_2, ..., V_n$ and E=$E_1, E_2, ..., E_n$ are edges indicating the relations between users [25]. Social networks are classified into two classes, namely directed social network and undirected social network [26]. While the direction of edges is important in directed social network, the edges do not have direction in undirected network. This work includes an undirected social network dataset. We use the Stanford University Facebook large network dataset [27], which has 4039 nodes, 88234 undirected edges, and average clustering coefficient 0.6. The representation of dataset's nodes and edges is shown in Figure 2.

In the dataset, nodes represent the users and edges represent the relation between nodes. Let us assume that User 0 wants to share the data ($data_{id} = d_1$) with his friends (346 people, in this case the network depth is 1), the data is related to User 1 and User 2. User 0 notifies the User 1 and User 2 by giving them the *data id* and the *targeted group*.

User 1 and User 2 now need to choose which data security features are worrying them if the d_1 is shared with User 0' friends. Their choices are used to get

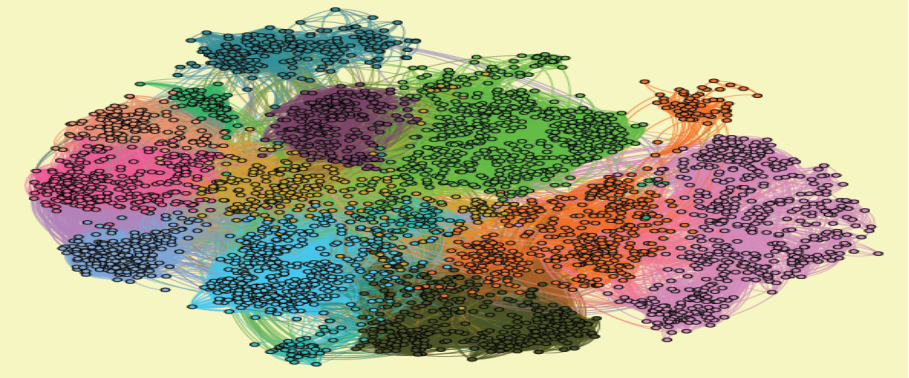

Fig. 2. The SNAP Facebook dataset network representation

the data sensitivity value (see Equation 1) which is one of the input variable for our fuzzy system to make group decision. Table 2 represents users' choices on CIAPP features of d_1.

Table 2. User 1 and User 2 Relation Values

User id	Confidentiality	Integrity	Availability	Privacy	Possession
User1	✓	X	X	X	✓
User2	✓	✓	✓	✓	✓

With CIAPP security features selections (the weights of features are set 1) on Table 2 and Equation 1, the d_1's sensitivity value becomes $0,7$.

The relation values calculation is computed with 3. Table 3 indicates the relation values for each user.

Table 3. User's choices on CIAPP features for d_1

User id	Relation value with targeted group
User1	0,04
User2	0,02

S_i is 347 since User 0 has 347 friends , therefore, the targeted group size is equal to the number of User 0's friends. User 1 has connection with 16 people from User 0' friends. Similarly, User 2 has connections with 9 people from User 0' friend group. Table 4 represents the numbers of known people for each user. The dataset's (Facebook dataset) relations between nodes and targeted group representations are given in Figures 3, 4 and 5.

Table 4. User's choices on CIAPP features for d_1

User id U_i	The number of known people by U_i
User0	346
User1	16
User2	9

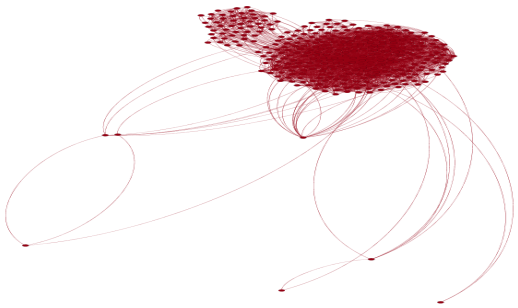

Fig. 3. User 0's relations: Targeted group for data

Fig. 4. Exist relations User1's in targeted group

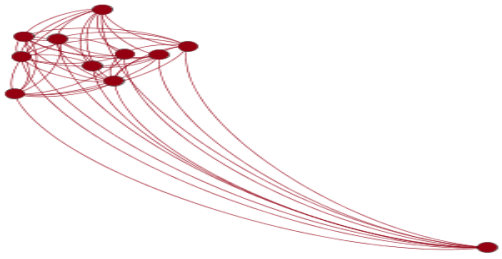

Fig. 5. Exist relations User2's in targeted group

User 0's relation with the targeted group is equal to 1. We now can use Equation 4 to find the relation value that is used to find out the confidence value (Equation 5). The relation value becomes $R = 1 * 0,06 = 0,06$. The last calculation is confidence value, which is the second input variable for our fuzzy system. It is computed with the data sensitivity value and the relation value (see Equation 5). This confidence value is calculated as $Cf = 1 - S_d(1 - R) = 0,65$. The input values for the fuzzy system to make decision are $0,7$ and $0,65$. The decision out of these two input values are given in Section 4.1 (see Figure 7).

4 Our Fuzzy-Based Group Decision Making Model

We start with defining the key components for determining the data sensitivity value and the trust (we use confidence in this paper) in targeted group. For our problem, there are five data security features that have effects to calculate the data sensitivity value. We use five data security features from Cherdanseva et al.' s work [21], these are namely, confidentiality,integrity, availability, privacy, and possession (CIAPP) (see Equation 1). For example, a user can be worried about his data's confidentiality if the data is viewed by people who may cause a threat for him. The second key component is confidence value in targeted group, we calculate the confidence value by using relations between user and targeted group (see Equation 5).

As we mentioned earlier, our fuzzy system has two inputs and one output, data sensitivity and confidence in targeted group are inputs and decision is output variables. In the fuzzy set, there is no predefined boundary between objects, therefore, each element of the set is associated with a value which indicates to what degree the element is a member of the set. Fuzzy decision is based on the fuzzy logic in which the decision values range [0,1] rather than binary values (0 or 1). Table 5 lists the input and output variables and their ranges.

Table 5. Membership Database

Linguistic Variables	Type	Membership Functions (Linguistic)	Membership Values (Python Values)
Sensitivity Value & Confidence Value	Inputs	Low	Range [0,.2,.3,.4]
Sensitivity Value & Confidence Value	Inputs	Medium	Range [.4,.5,.6,.7]
Sensitivity Value & Confidence Value	Inputs	High	Range [.6,.8,.9,1]
Decision	Output	No	Ranges[0, 0, .2,.4]
Decision	Output	Maybe	Ranges[.2,.4,.5,.7]
Decision	Output	Yes	Ranges[.6,.8,1,1]

The next step is to define the fuzzy sets and their membership function values, the membership function returns the degree of membership for a given value

within a fuzzy set. Fuzzy sets can have different shapes such as trapezoidal, triangular, gaussian, and rectangle. We choose the trapezoidal, we use the clustering method to define the membership functions' ranges (Fuzzy c-means clustering technique is used). Figure 6 represents the input and output variables' membership function values.

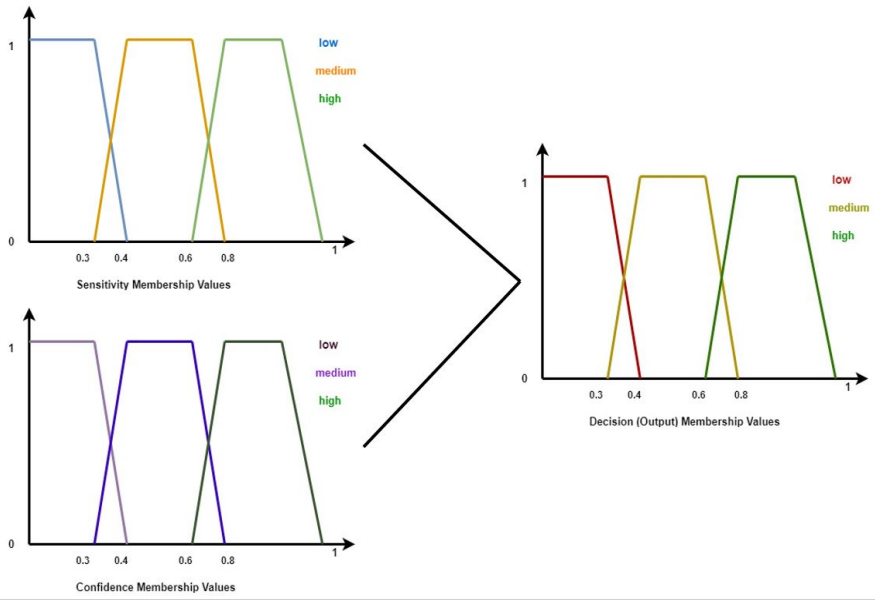

Fig. 6. Fuzzy Input-Output Membership Functions

We can now the define the our system's fuzzy rules, we use the expert knowledge to define the fuzzy rules. In our system, there are two input variables and each input variable have three different membership value, therefore we have maximum nine rules (3*3). Table 6 indicates the rules.

4.1 Using the Proposed Fuzzy System to Make Group Decision

The fuzzy system, which is represented in Section 4, has fuzzification, rule evaluation, aggregation of the rules, output, and defuzzification steps.

- Fuzzification:Obtains membership values from crisp values.
- Rule evaluation: Obtains the consequence of each rule, then combines output of each rule into a single fuzzy set with fuzzy aggregation operator.
- Aggregation: is the process to unify the outputs of all rules.
- Defuzzification: Converts fuzzy quantities into crisp numbers as the output.

Table 6. Fuzzy System Decision Making Rules

Rule number	Rules
1	If x_1 is low AND x_2 is low then decision=maybe
2	If x_1 is low AND x_2 is medium then decision=maybe
3	If x_1 is low AND x_2 is full then decision=yes
4	If x_1 is medium AND x_2 is low then decision=maybe
5	If x_1 is medium AND x_2 is medium then decision=maybe
6	If x_1 is medium AND x_2 is full then decision=yes
7	If x_1 is high AND x_2 is low then decision=no
8	If x_1 is high AND x_2 is medium then decision=maybe
9	If x_1 is high AND x_2 is full then decision=yes

We give a sample output of our fuzzy system in Figure 7. Given decision output value is obtained with the *sensitivity variable value =0.7 and the confidence variable value=0.65*. The output value is *Maybe with its degree= 0.45*.

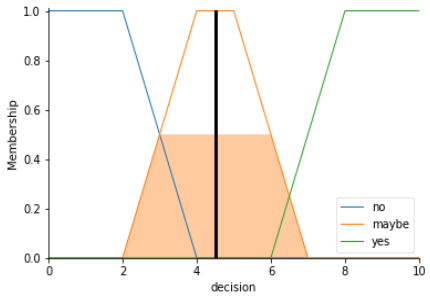

Fig. 7. Decision Value

5 Conclusion

Making decision on a co-owned data in SNs has been a problem, SNs' users (data owners) either ignore other users' (co-owners, also known decision makers) opinions on co-owned data or have difficulties to decide which co-owners' decisions are more important than others. Therefore, it is necessary to develop a system which can give co-owners' aggregated opinions on co-owned data to help data owners to make decision. To do so, in this contribution we develop a framework in which co-owners' express their opinions on co-owned data security features, co-owners' relations with the targeted group are calculated. We represent the aggregation of the co-owners' choices on CIAPP features. With co-owners' choices and their relation values, the developed fuzzy system gives the final decision.

In the future work, we aim to extend the work with adding the trust values between users to show whose decision is more important than the others on

decision making process. Then, see the effects of trust values on final group decision. And, also use the consensus reaching techniques to extend the work.

6 Acknowledgements

The authors would like to acknowledge the anonymous reviewers for providing their precious comments and suggestions. Also acknowledge is given to Turkish Education Embassy for their financial supports.

References

1. Scott, J. (1991). Social network analysis: A handbook. 1991. LonZ don: Sage Publications. p210.
2. Liu, Y., Fan, Z. P., and Zhang, X. (2016). A method for large group decision-making based on evaluation information provided by participators from multiple groups. Information Fusion, 29, 132-141.
3. Herrera-Viedma, E., Cabrerizo, F. J., Chiclana, F., Wu, J., Cobo, M. J., and Konstantin, S. (2017). Consensus in group decision making and social networks.
4. Akkuzu, G., Aziz, B., and Adda, M. (2019, January). Fuzzy logic decision based collaborative privacy management framework for online social networks. In 3rd International Workshop on FORmal methods for Security Engineering: ForSE 2019. SciTePress.
5. Dong, Y., Zha, Q., Zhang, H., Kou, G., Fujita, H., Chiclana, F., and Herrera-Viedma, E. (2018). Consensus reaching in social network group decision making: Research paradigms and challenges. Knowledge-Based Systems, 162, 3-13.
6. Cook, W. D., and Kress, M. (1985). Ordinal ranking with intensity of preference. Management science, 31(1), 26-32.
7. Hochbaum, D. S., and Levin, A. (2006). Methodologies and algorithms for group-rankings decision. Management Science, 52(9), 1394-1408.
8. Zadeh, L. A. (2008). Is there a need for fuzzy logic?. Information sciences, 178(13), 2751-2779.
9. Urena, R., Chiclana, F., Melancon, G., and Herrera-Viedma, E. (2019). A social network based approach for consensus achievement in multiperson decision making. Information Fusion, 47, 72-87.
10. Liang, Q., Liao, X., and Liu, J. (2017). A social ties-based approach for group decision-making problems with incomplete additive preference relations. Knowledge-Based Systems, 119, 68-86.
11. Wu, J., and Chiclana, F. (2014). A social network analysis trustconsensus based approach to group decision-making problems with interval-valued fuzzy reciprocal preference relations. Knowledge-Based Systems, 59, 97-107.
12. Herrera-Viedma, E., Alonso, S., Chiclana, F., and Herrera, F. (2007). A consensus model for group decision making with incomplete fuzzy preference relations. IEEE Transactions on fuzzy Systems, 15(5), 863-877.
13. Al-Samarraie, H., Teng, B. K., Alzahrani, A. I., and Alalwan, N. (2018). E-learning continuance satisfaction in higher education: a unified perspective from instructors and students. Studies in Higher Education, 43(11), 2003-2019.
14. Ekin, T., Kocadagli, O., Bastian, N. D., Fulton, L. V., and Griffin, P. M. (2016). Fuzzy decision making in health systems: a resource allocation model. EURO Journal on Decision Processes, 4(3-4), 245-267.

15. Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., and Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. In Exploring the convergence of big data and the internet of things (pp. 141-154). IGI Global.
16. Capuano, N., Chiclana, F., Fujita, H., Herrera-Viedma, E., and Loia, V. (2018). Fuzzy group decision making with incomplete information guided by social influence. IEEE Transactions on Fuzzy Systems, 26(3), 1704-1718.
17. Martinez-Cruz, C., Porcel, C., Bernab-Moreno, J., and Herrera-Viedma, E. (2015). A model to represent users trust in recommender systems using ontologies and fuzzy linguistic modeling. Information Sciences, 311, 102-118.
18. Thirumalai, C., and Senthilkumar, M. (2017, February). An Assessment Framework of Intuitionistic Fuzzy Network for C2B Decision Making. In Electronics and Communication Systems (ICECS), 2017 4th International Conference on (pp. 164-167). IEEE.
19. Kahraman, C., Ruan, D., and Doan, I. (2003). Fuzzy group decision-making for facility location selection. Information Sciences, 157, 135-153.
20. Samonas, S., and Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. Journal of Information System Security, 10(3).
21. Cherdantseva, Y., and Hilton, J. (2012). The Evolution of Information Security Goals from the 1960s to today. Unpublished. February.
22. Hu, H., Ahn, G. J., and Jorgensen, J. (2011, December). Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In Proceedings of the 27th Annual Computer Security Applications Conference (pp. 103-112). ACM.
23. Akkuzu, G., Aziz, B., and Adda, M. (2019, January). Fuzzy logic decision based collaborative privacy management framework for online social networks. In 3rd International Workshop on FORmal methods for Security Engineering: ForSE 2019. SciTePress.
24. Petkos, G., Papadopoulos, S., and Kompatsiaris, Y. (2015, August). PScore: a framework for enhancing privacy awareness in online social networks. In 2015 10th International Conference on Availability, Reliability and Security (pp. 592-600). IEEE.
25. Boyd, D. M., and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of computermediated Communication, 13(1), 210-230.
26. Scott, J. (2017). Social network analysis. Sage. Pages (12-25).
27. J. McAuley and J. Leskovec. Learning to Discover Social Circles in Ego Networks. NIPS, 2012.