International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206491

User Opinion based Trust Value Prediction for Online Social Network

Abinaya R
Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

Article Info
Volume 6, Issue 4
Page Number : 491-500
Publication Issue :
July-August-2020

Article History
Accepted : 15 Aug 2020
Published : 22 Aug 2020

ABSTRACT

Online social networking has caused profound changes in the way people communicate and interact. Preserving information privacy is indispensable in such social applications as the shared information would be sensitive. The issue becomes more challenging because of participation of multiple parties on the same shared data. Here propose an efficient trust collection based data sharing technique to allow or disallow the shared resources considering the authorization requirements of all the multiple parties. A logical representation of the proposed data sharing technique is prepared to analyze the privacy of data before sharing to public users. A user in this system is associated with a few trusted users that were selected from the user's friends. When the user wants to share information to the account, the service provider sends information to the user's trustees. The user must obtain at least k (i.e., recovery threshold) threshold values from the trustees before being directed to public share. Considering that a user continually posts data items in an OSN, here model the threshold selecting problem as a sequential decision-making problem. More specifically, we formulate the problem as a multi-armed bandit problem and apply the upper confidence bound (UCB) policy to solve the problem. This shows that dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold.

Keywords : Online Social Network, Group Sharing, Trust Value Estimation, Upper Confidence Bound Algorithm, Privacy Preserving.

I. INTRODUCTION

Social networking websites are varied and that they comprise a range of new information and conversation gear such as availability on laptop computers and smart phones, mobile gadgets inclusive of tablet computers and smartphones, virtual image/video/sharing and "web logging" diary entries on line. Online community services are consideration a social network provider, even though in a broader sense, social community carrier commonly method an character-targeted carrier whereas online community services are institution-focused. Social networking sites allow users to communicate ideas, photos and videos, posts, and tell others approximately on-line or actual international activities and events with humans of their community. While in-character social networking, which includes amazing in a village marketplace to speak about events has existed for the reason that

earliest trends of cities, the Web enables people to connect to others who live in exclusive places, starting from across a town to internationally. Depending at the social media platform, contributors may be capable of contact some other member. In other instances, members can contact all people they have a connection to, and ultimately each person that contact has a connection to, and so on. LinkedIn, a profession social networking provider, typically requires that a member in my opinion realize another member in real lifestyles earlier than they touch them on-line. Some services require individuals to have a pre-existing connection to touch other participants.

Social Engineering

There are different aspects of social engineering scamming techniques which trick users into entering sensitive information. This section describes a few of the well-known techniques.

- **Phishing attacks** are when emails, on the spot messages or other messages claiming to be from a depended on source ask for information. For instance, an email may additionally seem like from a financial institution and will direct a consumer to enter a password at a fake login page, or tell a person to call a smartphone quantity or risk having their account closed. Some Internet browsers, such as recent variations of Mozilla Firefox and Internet Explorer, have taken steps to help pick out fake web sites.
- **Spear phishing** is a sort of phishing attack that looks to be from a colleague, employer or friend and consists of a link or something to download. (This is frequently the result of account hijacking.) These links or downloads may be malicious, which includes viruses or fake websites that solicit non-public information.
- **Misleading solicitations** A social network would possibly use social engineering to make humans sense obligated to enroll in. This regularly takes place when one individual joins and (frequently inadvertently) affords the social community with get admission to his or her touch list. The social network then sends out emails to all of his or her contacts, frequently implying they're from the man or woman who joined. For instance, it's been said that Tagged.Com solicits contacts of customers with emails claiming the recipient has been "tagged." These emails state: "Is <user name> your pal? Please respond or <user name> might imagine you stated no :(" or "<user name> sent you photos on Tagged." The recipient can also consider that is a private invitation from the user and sense obligated to sign up for the network, giving out his or her statistics and possibly perpetuating the solicitations.
- **Hijacked accounts.** A legitimate account may be taken over by an identification thief or malware for the reason of fraud such as posting spam, sending out malware, stealing the non-public information of contacts or even soliciting contacts to ship cash. One traditional situation is when a hijacked account sends out messages mentioning that the account proprietor is distant places and in desperate straits. Contacts are urged to right now cord cash. A user may not realize his or her account has been hijacked for pretty some time. An assault may also be in the shape of a chat communication.

Large-scale networks:

Large-scale community is a term that synonymous with "macro-stage" as used, mainly, in social and behavioral sciences, in economics. Originally, the term become used significantly within the sciences (see massive-scale network mapping).

The term social media is commonly used to describe social networking sites inclusive of:

1. Facebook – a web social networking site that lets in customers to create their non-public profiles, proportion photos and videos, and communicate with different customers
2. Twitter – a web service that lets in users to submit "tweets" for their followers to look updates in actual-time
3. LinkedIn – a networking website for the enterprise network that allows users to create professional profiles, submit resumes, and communicate with different experts and job-seekers.
4. Pinterest – a web network that lets in users to show images of items discovered on the net by using "pinning" them and sharing thoughts with others.
5. Snapchat – an app on mobile devices that allows users to send and share photos of themselves doing their daily activities.

Social media technologies has many different types of forms such as blogs, photo sharing, products/services review, business networks, forums, micro-blogs, social bookmarking, social gaming, social networks, video sharing, and virtual worlds. The development of social media is started on with simple platforms consisting of sixdegrees.Com. Unlike instant messaging customers such as ICQ and AOL's AIM, or chat clients like IRC, iChat or Chat Television, sixdegrees.Com was the first on line business that turned into created for real people, the use of their actual names.

II. RELATED WORK

Nemi Chandra Rathore, et al., [1] proposes an OSN represents its registered users with a set of dynamic web pages that mimic users real social network. These pages contain her/his profile and other resources likewall posts, photos, videos and so on. During interaction, OSN users post number of messages, photos, videos, etc., into their own or others user spaces. Such resources are known as multi-party resources. Each multi-party resource is associated with multiple number of users called stakeholders that may have their own privacy preferences. These preferences may lead to policy conflicts that make the access control a challenging task. To address the multi-party access control issues, present OSNs provide a preliminary level of protection mechanism. For instance, Facebook allows a tagged user in a group photo to report/remove the tag, if she/he does not want to share that with others. However, that photo still remains visible to others. Further, if a stakeholder wants to fully remove the photo, she/he has to request the user who has uploaded it. Here propose a simple and flexible access control model where stakeholders collaboratively specify access policies equipped with simple conflict resolution technique. The scheme uses trust among stakeholders (of the resource) and requester to take access decision.

Stephan Hammer, et al., [2] proposed a smart energy system which is able to guide users in saving energy with the help of controlling devices, which includes lighting or displays, depending on context facts, including the brightness in a room or the presence of customers. However, proactive decisions should also match the customers' preferences to hold users' agree with inside the device. Wrong decisions may want to negatively have an impact on users' attractiveness of a system and at worst could cause them to abandon the device. In this work, a model created based on trust, known as User Trust Model (UTM), for automatic decision-making is proposed, which is based on Bayesian Networks. The UTM's creation, the initialization with empirical records accumulated in an online survey, and its integration in a workplace setting are described. Furthermore, the

outcomes of a consumer examine investigating users' experience and acceptance is provided.

Lei Xu, et al., [3] the proposed trust-based privacy management mechanism, introduce a threshold based on which the user makes the final decision on data posting. Simply speaking, a high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users opinion that provide highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving. Considering that a user continually posts data items in an OSN, we model the threshold selecting problem as a sequential decision-making problem. More specifically, we formulate the problem as a multi-armed bandit problem and apply the upper confidence bound (UCB) policy to solve the problem. Simulation results show that dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold. A trust-based approach was proposed for collaborative privacy management in Social Network. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more considerate of other users' privacy.

Hu and Hongxin, et al., [4] proposes a multiparty access control scheme in OSN. Users in OSN can post statuses and notes and uploads images and video on their own spaces, tag others to their content, and share the content with their friends. Users can also post information in their friends' spaces. The shared content may be viewed by multiple users. In order to enable a collaborative management of data sharing in OSNs, the multiparty access control (MPAC) model was recently proposed. When two users disagree on whom the shared data item should be exposed to, it causes a privacy conflict. To address such an difficulty, a MultiParty Access Control (MPAC) version became recently proposed, consisting of a systematic technique to become aware of and resolve privateness conflicts for collaborative records sharing in OSNs. In this process take some other step to look at the problem of studying the strategic behavior of rational controllers in multiparty access control, wherein every controller aims to maximize her/his very own benefit by means of adjusting her/his privateness putting in collaborative data sharing in OSNs. Here first formulate this trouble as a multiparty control process and display the unique Nash Equilibrium (NE) that's crucial because at an NE, no controller has any incentive to trade her/his privacy placing. Then present algorithms to compute the NE and show that the gadget can converge to the NE in just a few iterations. A numerical analysis is also provided for various scenarios that demonstrate the interplay of controllers in the multiparty control game.

Mehregan, et al., [5] the policy negotiation framework to be presented is designed to allow co-owners to collaboratively arrive at an access control policy while balancing two considerations. 1. Privacy preferences: The co-owners want to make sure that only certain users may access the co-owned objects. The participatory nature of the negotiation process allows the co-owners to reflect their subjective privacy preferences in the final access control policy. 2. Sharing needs: An object is created to make it available to other users due to the co-owners desire. The negotiation process allows each co-owner to state a desirable level of availability for the co-owned object. This specified level of availability will be used as an objective measure of policy quality. The need for human consent in organizational settings, the proposed implementation explores interactive coverage negotiation, an approach complementary to that of earlier work. Specifically, here propose an extension of Relationship-Based Access Control (ReBAC) to support multiple ownerships. In which a policy negotiation protocol is in place for co-owner

to come up with and give consent to an access control policy in a structured manner. Here devised two algorithms for verifying policy satisfy ability, both employing a modern SAT solver for solving sub problems.

III. Existing Methodologies

The In OSN trust plays a quite important role in network-based applications, such as peer-to-peer (P2P) systems, opportunistic mobile networks and online social networks. In existing OSNs, the trust relationship between users has been explored to protect sensitive data of users, or to verify the user's identity. They categorized studies on social trust based on three criteria, namely trust information collection, trust evaluation, and trust dissemination. The mechanism proposed in this paper involves evaluating the trust values between two users based on their interactions. Though current OSNs do not yet impose restrictions on the sharing of co-owned data, the problem of collective privacy management has been investigated this problem by using game theory. To aggregate different individuals' privacy policies, they proposed a Clark-Tax mechanism which can encourage individuals to report their true preferences on privacy policies. Here proposed a space segmentation approach to detect the conflicts among individual privacy policies. And they proposed a conflict resolution mechanism that considers both the privacy risk and the data sharing loss. The existing work, formulated the multiparty access control problem as a game played by multiple users. And an iterative update algorithm was proposed to compute the equilibrium of the game. Based on the multiparty access control model, proposed model can facilitate collaborative control of the personally identifiable information in a data item.

To describe the trust degree greater correctly, this process divides nodes into 4 classes, which are service nodes, feedback/remarks nodes, and recommendation nodes and controlled nodes. In social networks, trust represents the level of confidence approximately the reliability and correctness of user's behaviors. Service reliability indicates the trustworthiness of carrier that provider nodes provide; feedback/remarks effectiveness represents the trustworthiness of comments that comments nodes go back; recommendation credibility expresses the trustworthiness of recommendation that recommendation nodes provide. In this work, the world wide trust of the node i, denoted as Ti, the chance of i being accurate. The service reliability is denoted as STi; the feedback effectiveness is denoted as FTi; and the recommendation credibility is denoted as CTi.

In this work, let i be a service node, j be a feedback node and k be a recommendation node; and M_i, M_j, M_k are the managed nodes of i, j, k, respectively.

Trust Measurement Process

In this model, the specific feedback value $f_{vj,i}$, given by the feedback node j, is known by the system. Therefore, here implement the calculation method of service reliability based on the user feedback value $f_{vj,i}$, which is shown by Eq. (1).

$$ST_i = \frac{\sum_{j \in set\,(i)} f_{v_{j,i}} \cdot \lambda(j,i)}{\sum_{j \in set\,(i)} \lambda(j,i)},\ FT_j \geq \theta \qquad \rightarrow \text{Eq. (1)}$$

In Eq. (1), set(i) is the set of feedback nodes that communicated with service node i, and θ is the threshold of feedback effectiveness. $\lambda(j, i)$ presents the influence effect of node j on node i. In addition, FT_j represents the feedback effectiveness of node j.

In social networks, feedback nodes may calculate some trust nodes maliciously and praise some distrustful nodes. Therefore, here also calculate the trust degree of $f_{vj,i}$. In this work, calculate the effectiveness of feedback based on similarity of specific feedback values. The effectiveness of

feedback of node *j* can be calculated through a formula as shown by Eq. (2).

$$FT_j = \frac{\sum_{i \in set(j,r)} f_{v_{j,i}} . f_{v_{r,i}}}{\sqrt{\sum_{i \in set(j,r)} f^2_{v_{j,i}}} . \sqrt{\sum_{i \in set(j,r)} f^2_{v_{r,i}}}} \quad \rightarrow \text{Eq. (2)}$$

In Eq. (2), set (*j*, *r*) represents the node-pair set both nodes are communicated with node *i*. The calculation method of feedback service reliability, the recommendation credibility of node *k* is computed by Eq. (3).

$$CT_k = \frac{\sum_{i \in Rset(k)} ST_i . \lambda(k, i)}{\sum_{i \in Rset(k)} \lambda(k, i)} \quad \rightarrow \text{Eq. (3)}$$

$\lambda(k, i)$ presents the influence effect of node *k* on node *i*. There are two factors affecting the value of $\lambda(k, i)$. One is the time interval $T = t_n - t_p$, t_n presents the current time, and t_p presents the time that node *k* recommends node *i*. Then the connection degree $\omega_{k,i}$ of the relationship between node *i* and node *k*. Thus, $\lambda(k, i)$ is shown as Eq. (4).

$$\lambda(k, i) = \frac{1}{t_n - t_p} . \omega_{k.i} \quad \rightarrow \text{Eq. (4)}$$

In this paper, how to determine the connection degree $\omega_{k,i}$ is considered. Regarding to the successful transaction defined as Tr_{suc} and the number of total transactions defined as $|Tr|$ between node *k* and node *i*, we determine the connection degree $\omega_{k,i}$, which is shown as Eq. (5).

$$\omega_{k,i} = \frac{\sum_{m=1}^{|Tr|} Tr_{suc}}{|Tr|} \quad \rightarrow \text{Eq. (5)}$$

In Eq. (5), successful transaction denoted as Tr_{suc} is called indicative function, if CT > Threshold, $Tr_{suc} = 1$, otherwise, $Tr_{suc} = 0$.

Depending on the above analysis, the global trust degree is represented in Eq. (6). In Eq. (6), α, β and γ are weights for service reliability, feedback effectiveness and recommendation credibility, and $\alpha + \beta + \gamma = 1$.

$$T_i = \alpha \cdot ST_i + \beta \cdot FT_i + \gamma \cdot CT_i$$

If a service node provides distrust service, i.e. the feedback service reliability is lower than the service threshold ρ. In the service punishment cycle, a node should not offer any service to user. If a trust node provides distrust remarks, i.e. the feedback effectiveness is less than the threshold θ, the node will enter the feedback punishment cycle. A node should not request any service in the feedback punishment cycle. If a recommendation node presents mistrust recommendation, i.e. the advice credibility is less than the advice threshold δ, the node will input the recommendation punishment cycle. In the recommendation punishment cycle, a node should not offer any recommendation.

Secure photo sharing using trust based collaborative approach

The proposed trust-based privacy management mechanism, introduce a threshold based on which the user makes the final decision on data posting. Simply speaking, a high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users opinion that are provides highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving. Considering that a user continually posts data items in an OSN, here model the threshold selecting problem as a sequential decision-making problem. More specifically, we formulate the problem as a multi-armed bandit problem and apply the upper confidence bound (UCB) policy to solve the problem. This shows that dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold. A trust-based information sharing approach is proposed for collaborative privacy management in OSNs. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more

considerate of other users' privacy. The trusted parameters are adjusted with the help of bandit approach. By applying the UCB policy, the user can make a rational trade-off between data sharing and privacy preserving.

IV. METHODOLOGY

Introduction for UCB Algorithm

The algorithms we have presented so far have one systematic weakness: they don't keep track of how much they know about any of the arms available to them. They pay attention only to how much reward they have gotten from the arms.

This approach that they'll under-discover alternatives whose initial experiences had been now not profitable, even though they don't have enough records to be confident approximately the arms. Using the usage of an algorithm that can pay attention to not handiest what it knows, but additionally how it knows. The algorithm, UCB that well found in this chapter does exactly this. Before describe how the UCB algorithm continues track of the how much it knows, back on the epsilon-Greedy and Softmax algorithms and take a extra abstract perspective on them. Both the epsilon-Greedy algorithm and the Softmax set of rules share the following large homes:

- The algorithm default preference is to select the arm that presently has the maximum expected value.
- The algorithm sometimes makes a decision to explore and chooses an alternative that is not the one that currently seems best.
- The epsilon-Greedy algorithm explores with the aid of deciding on from all the fingers completely at random.

The Softmax algorithm explores by randomly choosing from all the arms with probabilities which might be more-or-less proportional to the envisioned price of every of the arms. If the other arms are particularly worse than the first-class arm, they are chosen with very low opportunity. If the arms all have similar values, they are each chosen nearly equally often. In order to achieve better performance by making an effort to have these two algorithms explore less over time, both algorithms can be set up to modify their basic parameters dynamically over time. We called this modification annealing.

As we did with the epsilon-Greedy and Softmax algorithms, well start off by implementing a class to store all of the information that our algorithm needs to keep track of:

```
Class UCB1():
def__init_(self, counts, values):
self counts = counts.
Self values = values.
return
def-initialize (self, n_arms):
self.counts = [0 for col in range (n_arms)]
self.values = [0.0 for col in range (n_arms)]
return
```

Upper Confidence Bound Algorithm

Upper Confidence Bound (UCB) is the widely used solution method for problems multi-armed bandit. This algorithm is based on the principle of optimism in the face of uncertainty.

In other words, the more uncertain we are about an arm, the more important it becomes to explore that arm.

- Distribution of action-fee features for 3 different arms a1, a2 and a3 after several trials. This distribution shows that the action value for a1

has the highest variance and for this reasons most uncertainty.

- UCB says that we should choose the arm a_1 and receive a reward making us less uncertain about its action-value. For the next trial/timestep, if we still are very uncertain about a_1, we will choose it again until the uncertainty is reduced below a threshold.

The intuitive reason this works is that when acting optimistically in this way, one of two things happen:

- Optimism is justified and we get a high-quality reward that is the objective in the long run.
- The optimism changed into not justified. In this situation, play an arm that believed would possibly supply a large reward while in truth it does no longer. If this happens sufficiently often, and then we will learn what the true payoff of this action is and not choose it in the future.

Steps in UCB Algorithm

- Play every of the K actions as soon as, giving initial values for suggest rewards similar to every action at
- For each round t = K:
- Let Nt(a) constitute the range of instances action a became performed so far
- Play the motion at maximizing the following expression:

$$Q(a) + \sqrt{\frac{2 \log t}{N_t(a)}}$$

- Observe the praise and replace the imply reward or predicted payoff for the chosen motion

Remember, inside the random exploration we just had Q(a) to maximize, whilst right here we have two terms. First is the action value function, whilst the second one is the self assurance time period.

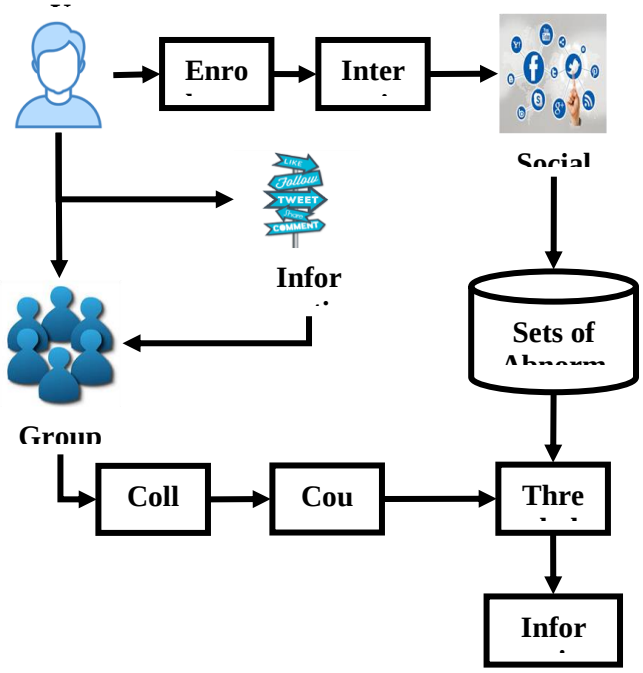
- Each time a is selected, the uncertainty is reduced: $N_t(a)$ increments, and, as it appears in the denominator, the uncertainty term decreases.

$$N_t(a) = \sqrt{\frac{2 \log t}{N_t(a)}}$$

- On the another side, an action other than *a* is selected at each time, value of t increases, but $N_t(a)$ remains constant; because t appears in the numerator, the uncertainty estimate increases.

$$t = \sqrt{\frac{2 \log t}{N_t(a)}}$$

- Because of the use of the natural logarithm the value increases get smaller over time; all actions will eventually be selected, but actions with lower value estimates.
- This will points to the optimal action being selected repeatedly in the end.



The proposed work is illustrated in fig 4.

Here shows the process of trust value estimation on shared data on OSN framework. User can create a group and share data on OSN. Shared data shown to the users within the same group. Given the data item

that a user wants to post and the privacy policy specified by the user, every involved user makes a "vote" to state whether he/she approves of the privacy policy. The importance of the vote depends on the trust value between the two users. Only when the aggregation of the votes satisfies a certain condition, the data can be posted. Moreover, the trust values between users are not fixed. A user will lose the trust of others if he/she posts a data item that incurs privacy loss of others. Also, a user can gain more trust from others if he/she adopts others' opinions. The interaction between the trust value and the privacy loss implies that if the user wants to reduce his/her privacy loss, then when posting a co-owned data item, the user should always consider others' privacy requirements rather than taking a unilateral decision. Here also implement comment blocking system to avoid unnecessary comments on shred information. Keyword matching will find the negative set comment and block the negative comments automatically.

V. CONCLUSION

A trust-based mechanism for collaborative privacy management was proposed. Here proposed a bandit approach to help the user make a tradeoff between data sharing and privacy preserving. The UCB policy was proposed for the stochastic multi armed bandit problem. As mentioned before, the performance of the learning policy is measured by regret. It has been shown that the UCB policy can achieve a logarithmic regret uniformly over the number of trials. When a user is about to post a data item, the user first solicits the stakeholders' opinions on data sharing, and then makes the final decision by comparing the aggregated opinion with a pre-specified threshold. The more the user trusts a stakeholder, the more the user values the stakeholder's opinion. If data sharing of one user suffers a privacy loss of another user, then the user's trust in another user decreases. The trust based mechanism can help reduce the average privacy loss.

VI. REFERENCES

[1]. Rathore, Nemi Chandra, and Somanath Tripathy. "A trust-based collaborative access control model with policy aggregation for online social networks." Social Network Analysis and Mining 7, no. 1 (2017): 7.

[2]. Rathore, Nemi Chandra, and Somanath Tripathy. "Collaborative access control model for online social networks." In 2016 IEEE 6th International Conference on Advanced Computing (IACC), pp. 19-24. IEEE, 2016.

[3]. Hammer, Stephan, Michael Wißner, and Elisabeth André. "Trust-based decision-making for energy-aware device management." In International Conference on User Modeling, Adaptation, and Personalization, pp. 326-337. Springer, Cham, 2014.

[4]. Sridharan M, Siva Ragavan S, Ranjith Kumar R, Arvind K A, Praveen Kumar S. "Trust-based collaborative privacy management in online social networks." International Journal of Advanced Research in Computer and Communication Engineering Vol. 8, Issue 3, March 2019.

[5]. Xu, Lei, Chunxiao Jiang, Nengqiang He, Zhu Han, and Abderrahim Benslimane. "Trust-based collaborative privacy management in online social networks." IEEE Transactions on Information Forensics and Security 14, no. 1 (2018): 48-60.

[6]. Hu, Hongxin, Gail-Joon Ahn, Ziming Zhao, and Dejun Yang. "Game theoretic analysis of multiparty access control in online social networks." In Proceedings of the 19th ACM symposium on Access control models and technologies, pp. 93-102. ACM, 2014.

[7]. Xu, Lei, Chunxiao Jiang, Jian Wang, Jian Yuan, and Yong Ren. "Information security in big data: privacy and data mining." Ieee Access 2 (2014): 1149-1176.

[8]. Mehregan, Pooya, and Philip WL Fong. "Policy negotiation for co-owned resources in relationship-based access control." In Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies, pp. 125-136. ACM, 2016.

[9]. Bubeck, Sébastien, and Nicolo Cesa-Bianchi. "Regret analysis of stochastic and nonstochastic multi-armed bandit problems." Foundations and Trends® in Machine Learning 5, no. 1 (2012): 1-122.

[10]. Gong, Neil Zhenqiang, and Di Wang. "On the security of trustee-based social authentications." IEEE transactions on information forensics and security 9, no. 8 (2014): 1251-1263.

Cite this article as :

Abinaya R, "User Opinion based Trust Value Prediction for Online Social Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 491-500, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206491
Journal URL : http://ijsrcseit.com/CSEIT206491