IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CYBER-PHYSICAL-SOCIAL COMPUTING AND NETWORKING

Received December 31, 2017, accepted January 22, 2018, date of publication February 22, 2018, date of current version March 13, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2807783

Reliable Decision Making of Accepting Friend Request on Online Social Networks

MD. ARAFATUR RAHMAN[1,2], (Member, IEEE), VITALIY MEZHUYEV[1], (Member, IEEE), MD ZAKIRUL ALAM BHUIYAN[3], (Senior Member, IEEE), S. M. NAZMUS SADAT[1], SITI AISHAH BINTI ZAKARIA[1], AND NADIA REFAT[4]

[1]Faculty of Computer Systems and Software Engineering, Universiti Malaysia PAHANG, Kuantan 26300, Malaysia
[2]IBM Center of Excellence, Universiti Malaysia PAHANG, Kuantan 26300, Malaysia
[3]Department of Computer and Information Sciences, Fordham University, Bronx, NY 10458, USA
[4]Center for Modern Language and Human Science, Universiti Malaysia PAHANG, Kuantan 26300, Malaysia

Corresponding author: Md. Zakirul Alam Bhuiyan (mbhuiyan3@fordham.edu)

This work was supported in part by RDU, funded by University Malaysia Pahang, Malaysia, under Grant RDU170304, and in part by the Fordham University Faculty Research Startup Grant.

ABSTRACT Online social network (OSN) is a platform, where users are able to share information among them easily and instantly. The sensitive information of an user can be misused by his/her friends or friends of friends due to the lack of reliable friend request acceptance (FRA), which is one of the key issues in OSNs. The existing FRA techniques are functioning based on either *blind* (i.e., without knowing information of a user, who sends the friend request to become a new friend, referred to as *friend-to-be*) or *manual search* method. Although, in the second method, the OSN user accepts a new friend based on his/her profile, however, it is not guaranteed that the profile is not fake. A approach is to bring down the misused information by filtering FRA using a reliable method to find out more information about the *friend-to-be*. This paper has proposed such a method for reliable decision making (RDM) of accepting friend request on OSNs in order to identify the attributes of a *friend-to-be*. RDM is a function with several parameters, such as security, flexibility, effectiveness, and satisfaction. To prove the reliability of the proposed method, an extensive quantitative study was carried out, which results indicated user's preferences for proposed method compared with the existing FRA methods.

INDEX TERMS Friend request acceptance, online social networks (OSNs), reliable decision making.

I. INTRODUCTION

Online Social Networks (OSN) is a medium where people are allowed to share personal backgrounds, interests, activities, and connections with OSNs users [1]. The evolution of Internet technologies led to significant growth of the OSNs, e.g., Facebook, Twitter, LinkedIn, Google+ and so on. Among them Facebook is the largest online social network in the world which has over 1.86 billion active users. OSN allows registered users to create profiles, send messages, update status, upload photos and videos to connect with family members, friends and business associates. In a process of making a friend, OSNs users give an access to their personal information to other people, from old friends to strangers. The sociable and communal atmosphere of OSNs is very striking to users and it makes easy for the users to unveil information about themselves and their contacts with other users [2]. Moreover, it is dangerous to share sensitive information in online [3]–[5], e.g., time-related information [6], personal characteristics and activities, and user's habits. Such sensitive information is targeted by attackers [6], [7] who are involved in malpractice for unwanted purposes such as robbery, kidnapping, stalking, etc. For instance, in March 2013, a teenage girl was murdered while stay at home alone in Tulsa, USA [8]. A few hours before of her death, she tweeted, "*Have the house to myself everybody gone*" [8]. Therefore, the posted information in online may cause the user in danger [9]–[11].

As a consequence, the sensitive information of an user can be misused by his/her friends or friends of friends due to the lack of reliable Friend Request Acceptance (FRA), which is one of the key issues in OSNs. The existing FRA techniques are functioning based on either *blind* or *manual search* method. In the former one, a user allows FRA without knowing information of a user who sends the friend request to become a new friend, referred to *friend-to-be*. Although in the second method, the OSN user accepts the new friend based on the user's profile, however, it is not guaranteed that the profile is not fake. One of the approaches is to bring down the misused information by filtering FRA using a

reliable method to find out more information of the *friend-to-be*. We can clarify this issue with an example depicted in Fig. 1, where a user denoted as U has a set of attributes, $\{a_1, a_1, ..a_n\}$, and a *friend-to-be* denoted as $F^{1,1}$ has also a set of attributes $\{a_1^{1,1}, a_1^{1,1}, ..a_n^{1,1}\}$. If a user takes a decision for accepting *friend-to-be* based on the matching factor, it would be considered as Reliable Decision Making (RDM). Moreover, the reliability will be more if the method analyzes all the friends' attributes of *friend-to-be* (e.g., it has l levels and each level has m users, as shown in Fig. 1). This is reasonable as a person's behaviour, attitude and attributes are directly influenced by his/her friends.

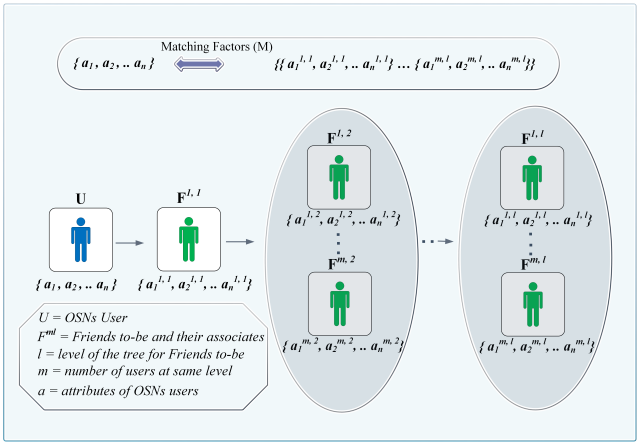

FIGURE 1. Overview of RDM for accepting friend request on OSNs.

To this aim, this paper designed a reliable method for decision making of accepting friend request on online social networks through an automated filtering approach. More in details, we design an algorithm for estimating matching factor based on the attributes of *friend-to-be* and his/her friends. Subsequently, we define the RDM as a function (R_l) with several parameters such as security, flexibility, effectiveness and satisfaction, as shown in Eq. 1. Finally, in order to prove the reliability of the proposed FRA method, this study has followed a survey as a quantitative approach and the findings reflect that the users prefer to use the proposed method compared to the existing FRA methods.

$$R_l = f(S_c, F_l, E_f, S_t) \tag{1}$$

where, S_c, F_l, E_f and S_t are denoted as security, flexibility, effectiveness and satisfaction, respectively.

The paper is organized as follows: Section II introduces the related works. Section III describes the features of friend requests, along with the existing methods of friend request acceptance. The proposed reliable method is presented in Section IV. The research method is described in Section V, while the research findings is analyzed in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORKS

There are several works have been done on OSNs with different aspects such as security, trust, discovering friendship and conserving privacy. In security point of views, there are works [12]–[16] that consider adversaries' attack on OSNs users' identities, attributes, as well as their social relationships. Adversaries can belong to existing social relationship or be strangers/fraudulent users [17]. Fong *et al.* [18] proposed an access model that formalized and generalized the privacy preservation mechanism for Facebook. Carminati et al. proposed an access control mechanism for the information sharing in web-based social networks in [19]. The major difference between the proposed method and [18] is that they used the decentralized architecture for the access control, which may invite potential security breaks (e.g., forming an identity, attributes, and trust information). In particular, [20] can provide automatic access policy generation for users' profile information. Mislove *et al.* [21] discussed the possible inference on user profile based on existing relationships, which could be a powerful attack on identifying real identities applying user attributes.

Sherchan *et al.* [22] summarized the trust management in social networks into three aspects, such as trust information collection, trust evaluation, and trust dissemination. They also discussed the propagative property of the trust, which can be used to create trust chains. Guo *et al.* [23] characterized existing social relationship of OSNs user as 1-hop trust relationship and further established a multi-hop trust chain during the recommendation process. In addition, from the same source, the authors are along the line of discussing the context-specific or context-aware trust between OSNs users, so that they can control it for establishing multi-hop trust chain for users with specific attributes. The proposed architecture also highlights trust management in different types of professional social networks.

In terms of making friendships, Daly and Haahr [24] discussed the establishment of friendship chains using social attributes. Similarly, Chen and Fong [25] used trust factor in collaborative filtering (CF) algorithm to recommend OSNs users on Facebook, where they analyzed the similarity based on users' interests and attributes. One of their following work [26] had the same idea, but tried to use data mining approach to gather users' information to input for the recommendation. However, the above works fail to consider users' privacy concerns on both identity and their social attributes.

Li *et al.* [27] proposed a privacy-preserving personal profile matching schemes for mobile social networks, by using polynomial secret sharing. Dong *et al.* [28] designed a secure friend discovery scheme based on verifiable secure dot product protocol by using homomorphic encryption. Due to their distributed approaches, both of the above schemes lack the ability to prevent active attacks when users change their attributes to satisfy the query requirements. Their previous papers [29]–[37] also discuss the private matching schemes in e-Health/m-Health systems and others' issues.

Most of the aforesaid procedures are not completely fulfilled the user safety as well as other compliance during the acceptance of friend request or making associates with others. Unlike the aforementioned works, this paper proposed to

design a reliable decision making of accepting friend request on online social networks through an automated filtering approach, which will reduce the misuse of the sensitive information of the OSN users.

III. FRIEND REQUEST FEATURES & EXISTING FRA METHODS ON OSN

The following sub-sections describe the features of friend request on OSNs and the existing OSNs FRA methods, which need to be discussed for designing a new reliable FRA Method.

A. FEATURES

There are several features are available in OSNs, which are explained below:

1) FRIEND REQUEST SETTING

A user can adjust his/her preference for accepting friend by exploiting Friend Request Setting (FRS). FRS offers two types of feature such as ''Everyone'' and ''Friends of Friend''. The former one indicates that every user on a particular OSN platform can become a user's friend. On the contrary, the later one indicates that only the friends of a user's friends can become his/her friend. It limits friend requests to the users who are not interested to make random friends. It also can assist a user to keep information private and secure compared to the former one.

2) FIND FRIEND

A user can be connected with his/her old/new friends utilizing this feature. It can help to generate a list of people and their profiles according to the user's provided information such as name, hometown, college or university, e-mail etc. The user can also use this list if he/she can't remember someone's name. By this feature, a user has the higher possibility to search accurately, as the people rarely have same attributes in their personal details [38].

3) FRIEND REQUEST

If person X wants to become a friend with another person Y, X has to send a request exploiting this feature. After receiving the request, Y can accept the friend request by analysing Y's profile that basically includes profile picture, name, and mutual friends and so on. Y can reject the X if he/she is not interested. Y can investigate more information of X by connecting through X's time-line.

4) PEOPLE YOU MAY KNOW

This feature suggests a list of few friends that might be known based on mutual friends of user's friend. Their features are consisted of profile picture, name, and mutual friends of friends you may know. The user can add or remove a friend from the provided list as well. It is also called as a friend recommendation system.

B. METHODS

There are two methods in OSNs, which have been identified in order to accept the friend requests such as: (1) blind acceptance [39]; and (2) manually search information. Indirectly, we can make an assumption of the criteria of a person based on the methods of friend requests acceptance [40].

1) BLINDLY ACCEPTANCE

It is a method where user used to accept friend requests without considering any information about friend-to-be. By employing blindly acceptance method, the user may get at least one attribute of friend-to-be (i.e., name) or maximum three attributes of friend-to-be (i.e., profile picture; name; and a mutual friend). Generally, two attributes are being displayed on friend requests which are profile picture and name of a friend-to-be. This method is easy and quick to be done. Here, the user only needs to place the confirmation after receiving the friend request. However, it is extremely unsafe to make friend with strangers without knowing their credentials. [39], [41].

2) MANUALLY SEARCH INFORMATION

Manually search information is another method of accepting friend request of the two, where the OSNs user used to accept friend requests by complying identical attributes with friend-to-be. Furthermore, the information is acquired by confirming the timeline of friend-to-be. In some cases the acquisition of information can be restricted if the friend-to-be set their profile is being private. And so, this method is beyond in complex and time consuming for fulfilling the information. For example, if any well-known person is a user of a particular OSNs, and he can get enormous friend requests in a day, then it could be quite distressing for his/her to apply manually search information in order to comply friend-to-be one by one. So, this method is not appropriate to apply in daily life.

IV. PROPOSED RELIABLE FRA ON OSN

As mentioned earlier, sharing information online is disclosed OSNs users to a danger especially if strangers are in their friend list. This is because, the attackers are able to analyze and extract personal characteristics and activities and misuse that information for illegal purposes. In this paper, we proposed a reliable decision making for FRA in OSNs that counteract aforesaid issues. The method and algorithms for evaluation of the correspondence of user and friend-to-be profiles (''prospect to become a friend'') are in the following:

A. INPUT

1) Profile of a user and profiles of his/her friends.
2) Profile of a friend-to-be and profiles of his/her friends.

B. OUTPUT

Value [0;1] of user' and friend-to-be' profiles matching, referred to as Matching Factor (M) (''prospect to become a friend'').

TABLE 1. Sample of algorithms application for the evaluation of prospect to become a friend.

Types of attributes (Facebook Interest Categories)	Attributes of a user A_u	Attributes of a friend-to-be A_f (n=1)	Attributes of a friend a friend-to-be (n=2)	Attributes of a friend of a friend of a friend-to-be (n=3)	Attributes of a friend of a friend of a friend of a friend-to-be (n=4)
Weight	1	1	1/2	1/4	1/8
Sports	{Race, Chess}	{Race, Chess}	{Chess, Cycling}	{Football, Race}	{Chess, Swimming}
Music	{Pop,Rock}	{Pop,Rock}	{Jazz,Blues}	{Pop,Country}	{Opera, Classic}
Common attributes, $A_u f$	{ Race, Chess, Pop, Rock }		$Chess_{1/2}, Race_{1/4}, Pop_{1/4}, Chess_{1/8}$ Weight of common attributes $W^{ufs} = \Sigma_{n=2}^{\lvert A_{ufs}\rvert} W_n^{ufs} = 1/2 + 1/4 + 1/4 + 1/8 = 1.125$ Maximum possible weight of attributes of friends of a friend-to-be $W^{fs} = \Sigma_{n=2}^{\lvert A_{fs}\rvert} W_n^{fs} = 4 * 1/2 + 4 * 1/4 + 4 * 1/8 = 3.5$		
Prospect to become a friend	$M_1 = \frac{2\lvert\{Ra,Ch,Po,Ro\}\rvert}{\lvert\{Ra,Ch,Po,Ro\}\rvert+\lvert\{Ra,Ch,Po,Ro\}\rvert} = \frac{2*4}{4+4} = 1(100\%)$ where, $Ra = Race, Ch = Chess$ $Po = Pop, Ro = Rock$		$M_2 = \frac{W^{ufs}}{W_{fs}} = \frac{1.125}{3.5} \approx 0.32(32\%)$		

C. MATHEMATICAL MODEL

Input information is a graph, which vertices are users' profiles and edges are friends' relationships. In this graph, two *labelled rooted trees* are allocated.

T_u is a rooted tree of friend relationships of a user. The root of the tree T_u is a vertex V_u user profile. T_f is a rooted tree of friend relationships of a *friend-to-be*. The root of the tree T_f is a vertex V_f *friend-to-be* profile.

D. BASED ON THE DEPTH OF THE SEARCH ALGORITHM, THERE ARE THREE POSSIBLE APPROACHES

1) First (simplified) algorithm takes into account only attributes of user' and *friend-to-be'* profiles (vertexes V_u and V_f).
2) Second (expanded) algorithm takes into account attributes of user' profile, profile of a *friend-to-be* and profiles of friends of a friend-to-be (vertex V_u and tree T_f).
3) Third (full) algorithm takes into account attributes of vertexes of the trees T_u and T_f.

This paper elaborates on first and second approach.

E. PROPERTIES OF THE TREES T_u AND T_f

- To each vertex of T_u and T_f a unique label $\overline{1, N}$ is assigned. 1 is the label of the root. N is a constant, defining the depth of the search.
- Vertices of T_u and T_f contain set of attributes of a user and a *friend-to-be.*
- Directions of edges of T_u and T_f go away from the root(out-tree).
- Edges of T_u and T_f are friends' relationships of a user and of a *friend-to-be* correspondingly.

Assumption: T_u and T_f have not cycles, so any two vertices can be connected by a unique simple path.

F. FIRST ALGORITHM

1. From user' profile (vertex V_u), detect his/her types of interests (correspondingly to Facebook Interest Categories, i.e. Sport, Music, Movies etc.).
2. Declare two supersets of attributes A_u and A_f, which elements are sets of values of interests of a user and of a *friend-to-be* correspondingly.
   $A_u = \{Sp_u, Mu_u, Mo_u \dots\}$
   $A_f = \{Sp_f, Mu_f, Mo_f \dots\}$
   $where, Sp = Sports, Mu = Music, Mo = Movie$
   e.g.
   $Sp_u = \{Fo, Sw\}$,
   $Sp_f = \{Fo, Aw\}$;
   $Mu_u = \{Po, Ro\}$,
   $Mu_f = \{Po, Co\}$. $where, Fo = Football, Sw = Swimming, Aw = Arm - wrestling$
   $where, Po = Pop, Ro = Rock, Co = Country$
3. Define the set of common attributes $A_u f$ as an intersection of A_u and A_f $Au_f = A_u \cap A_f$
   e.g. A_u = { Fo, Sw, Po, Ro } A_f = { Fo, Aw, Po, Co } $A_u f = A_u \cap A_f = \{Fo, Po\}$
4. Define value of user' and friend-to-be' profiles matching as ratio

$$M_1 = \frac{2|A_{uf}|}{|A_u| + |A_f|} \tag{2}$$

Remark 1: Multiplier 2 in the numerator is added with the purpose of normalization of value of M_1 (to compensate summation of attributes in denominator). For example,

$$M_1 = \frac{2|\{Fo, Po\}|}{|\{Fo, Sw, Po, Ro\}| + |\{Fo, Aw, Po, Co\}|} = \frac{2 * 2}{4 + 4} = \frac{1}{2}$$

In given sample, M_1 is a value (0.5) of common interests of a user and a friend-to-be; so the method gives 50% prospect to become a friend.

Fig. 2 shows function $M_1(|A_{uf}|)$, which is linearly growing with linearly increasing amount of common interests ($|A_u| = |A_f| = 10$).

Advantages: Simplicity of implementation of the algorithm and its computational effectiveness.

Disadvantages: Unreliable results in case of possible dummy friend-to-be account (or when it specially adjusted to friend account). To overcome it, second algorithm takes into accounts profiles of friends of a friend-to-be up to some depth N.

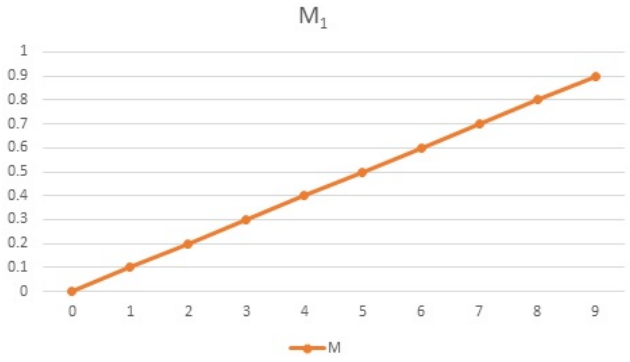

FIGURE 2. Dependency of prospect to become a friend from number of common interests.

G. SECOND ALGORITHM

1) Define set of waited attributes A_u of a user. Assign value 1 to weight of every attribute of the set A_u.
2) Define set of common attributes $A_f s$ of friends of a friend-to-be.
(a) Set value N of the depth of the tree T_f traversal.
(b) Starting from the root V_f traverse T_f up to the depth N and form the common set of weighted attributes $A_f s$ of friends of a *friend-to-be*.
Weight W of an attribute of a vertex n set back proportional to 2 to the power of n.

$$W_n = 2/2^n \tag{3}$$

where $n = \overline{1, N}$
Formula (3) allows us to express decreasing with the level of friendship weight of attributes. Attributes of the root node V_f (friend-to-be' profile, n = 1) have weight 1; weights of the attributes of friends of a friend-to-be (n = 2) are 1/2; weights of attributes of friends of friends of a friend-to-be (n = 3) are 1/4 etc.
For example, all friends of a *friend-to-be* have an attribute "Ro" in Music interests. Weight of this attribute for a friend-to-be is $W_1^{Ro} = 1$; weight of this attribute for a friend of a friend-to-be is $W_2^{Ro} = 1/2$; weight of this attribute for a friend of a friend of a friend-to-be is $W_3^A = 1/4$ etc.
Considering depth of search $N = 4$, total weight of the Rock attribute is

$$W^{Rock} = \Sigma_{n=1}^{4} W_n = 1 + 1/2 + 1/4 + 1/8 = 1.875$$

Remark 2: Practically, it is enough to take into account only attributes up to the level 5, which values will be taken into account with weight $1/16 = 0.0625$.
3) Define set of common attributes $A_u f$ as intersection of A_u and $A_f s$

$$Au_{fs} = A_u \cap A_{fs}$$

4) Compute sum of weights of common attributes, from 1 till $|A_u fs|$

$$W^{ufs} = \Sigma_{n=1}^{|A_{ufs}|} W_n^{ufs} \tag{4}$$

5) Compute sum of weights of all attributes of friends of a friend-to-be, from 1 till $|A_f s|$

$$W^{fs} = \Sigma_{n=1}^{|A_{fs}|} W_n^{fs} \tag{5}$$

6) Compute M_2 as normalized value of weights of common attributes

$$M_2 = \frac{W^{ufs}}{W^{fs}} \tag{6}$$

Remark 3: Formulas (4) and (5) start computation from friend-to-be' vertex (n = 1) and so take into account friend-to-be' attributes, which already have been done by first algorithm - formula (2). For decision making it is reasonable to exclude from (4) and (5) a friend-to-be' vertex, i.e. start algorithm from a friend of a friend-to-be (n = 2).

This will allow users to compare independent results of two formulas (2) and (6) and also check dummy (or specially created) friend-to-be profiles. Table 1 illustrates this idea.

Following first algorithm and formula (2) a user and a friend-to-be have 100% matching interests and so highest (100%) prospect to become a friend. However, analyses of profiles of a user and friends of a friend-to-be, made by formula (6) starting from n = 2 shows 32% prospect to become a friend, which can say about incomplete compliance.

This why in OSNs interface, it is reasonable to shows two values: Correspondence of profile of a user and a friend to be, calculated by formula (2). Correspondence of profile of a user and friends of a friend-to-be, calculated by formula (6) starting from n = 2.

Further elaboration

- ◇ Check for dummy friend-to-be profile (Give a warning if a friend-to-be does not have sufficient amount of friend relationships).
- ◇ Setting of importance (ranking) of attributes for friends search.
- ◇ Highlighting potentially dangerous values of interests (violence, terrorism, suicide etc.)

V. RESEARCH METHOD

A quantitative research has been conducted to know participant's responses on accepting friend request in Online Social Networks (OSNs). The participants of this study are the UMP students who have Facebook accounts, as Facebook is the most prominent OSN. The survey consists of 12 items, which utilize the Likert-type scale of 4 scale starting from 1 = strongly disagree to 4 = strongly agree, measuring the acceptance or opinion of different friend request systems. The 12 items are based on the four criteria (3 for security, 3 items for flexibility, 3 for effectiveness and 3 for satisfaction).

VI. RESEARCH FINDINGS

This section describes the outcome of the survey in terms of reliability that focuses on the user perceptions and consideration on security, flexibility, effectiveness, and satisfaction level approaches of accepting a friend request on OSNs. The hypothesis of this study is: the proposed method will be a reliable decision making for FRA on OSNs if and only

if it outperforms the existing methods in terms of security, flexibility, effectiveness, and satisfaction.

A. USER PERCEPTIONS TOWARDS SECURITY

This section illustrates the user or participants attitudes towards three different approaches of friend request acceptance.

It is observed through the above Figure 3, participants mostly give their consent on the proposed method which is mean (m) = 3.62 while in blind and manual method received respectively m = 1.60 and m = 2.58. The users are showing positive attitude towards the proposed method on security aspect since it takes less time to make friend with secured manner. Moreover, it gives the profile of a friend to be with maintaining the similar characteristics and it is completely absent in other approaches i.e., blind or manual method. In blind approach, users are less concerned about security while in the manual method the users prefer more time but security is needed. In the proposed method, it is observed that it takes less time and secure way to make friends in OSNs. Thus, participants liked this approach more than the other two approaches.

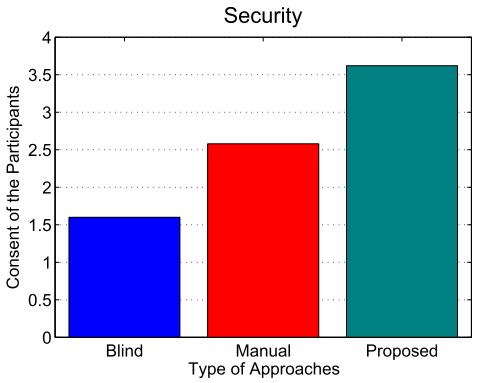

FIGURE 3. Users evaluation of security of different FRA approaches on OSNs.

B. USER PERCEPTIONS TOWARDS FLEXIBILITY

This Figure 4 represents the user flexibility on OSNs that focuses the user friendliness and time consuming issues.

It is noticed that the majority users agreed that the proposed method is much better i.e., m = 2.98 in terms of flexibility with the other approaches i.e. blind method m = 1.48 and manual method m = 2.14. The reasons behind this result is that the major portion (i.e., m = 2.98) believes to make friend with only the person who has the same type of features because it is secured and comfortable to be a friend with them.

C. USER PERCEPTIONS TOWARDS EFFECTIVENESS

This section illustrates the user perception of the effectiveness of the different approaches.

It is demonstrated in the Figure 5 that users found the proposed method of accepting friend request is more effective than the other two approaches. Thus, they consented more on this approach (m = 3.56) while in the blind (m = 2.16) and manual approach (m = 2.76) appeared to them less effective

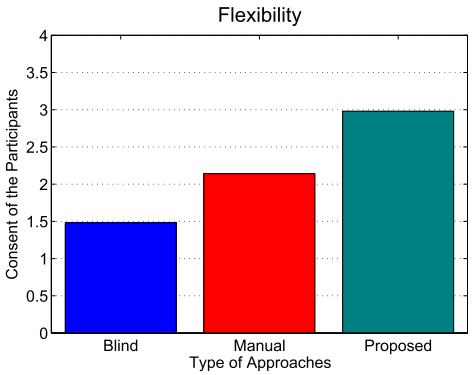

FIGURE 4. Users evaluation of fallibility of different FRA approaches on OSNs.

for OSNs. The outcome of this result suggests that users are more concerned about security and time consumption.

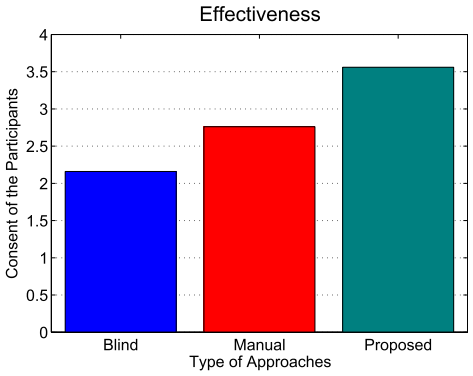

FIGURE 5. Users evaluation of effectiveness of different FRA approaches on OSNs.

D. USER PERCEPTIONS TOWARDS SATISFACTION

In this study, it is aimed to analyze the user opinion on satisfaction on different method of OSNs.

The Figure 6, represents the opinion of users satisfaction that gives the highest level i.e., m = 3.46 on proposed method i.e. which is unlike the other approach i.e., blind method m = 1.66 and manual method m = 2.62. Satisfaction on OSNs is related with the concern of the users on consumption to fix their connections. Therefore, the proposed method relies on utmost user satisfaction by conveying security, flexibility, less time-consuming facilities.

E. T-TEST RESULT

This T-test result is aimed to show whether there are any significant differences among the three approaches. In this T-Test as shown in Table 2, it is noticed that each criterion (i.e., security, flexibility, effectiveness, and satisfaction) has a significant outcome and they vary with each other. Thus, in all criteria the p value is $p > 0.05$, that validates the hypothesis of the work.

VII. CONCLUSION

Sharing information with unknown OSN user is a risk which leads being a target by the attackers. In order to address this

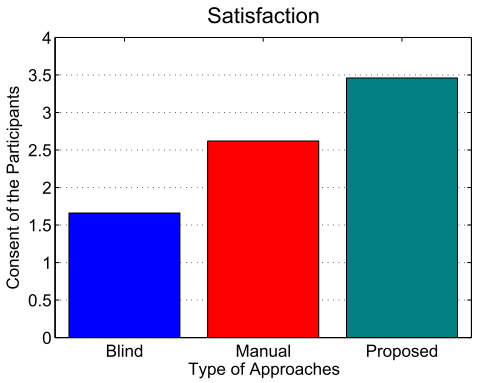

FIGURE 6. Users evaluation of satisfaction of different FRA approaches on OSNs.

TABLE 2. T-test analysis.

Method	Mean	SD	df	t	p	Features
Blind &	1.60	0.72	49	-14.28	0.00*	Security
Proposed	3.62	0.63				
Manual &	2.58	0.64	49	-08.14	0.00*	
Proposed	3.62	0.63				
Blind &	1.48	0.57	49	-10.05	0.00*	Flexibility
Proposed	2.98	0.76				
Manual &	2.14	0.72	49	-00.61	0.00*	
Proposed	2.98	0.76				
Blind &	2.16	0.76	49	-09.61	0.00*	Effectiveness
Proposed	3.56	0.64				
Manual &	2.76	0.62	49	-06.79	0.00*	
Proposed	3.56	0.64				
Blind &	1.66	0.51	49	-18.99	0.00*	Satisfaction
Proposed	3.46	0.50				
Manual &	2.62	0.75	49	-06.51	0.00*	
Proposed	3.46	0.50				

issue, we studied the existing FRA methods and identified their limitations. Based on those, we proposed a reliable method for decision making of accepting friend request on OSNs. More in detail, we designed an automated filtering algorithm that estimated a matching factor, which utilized for making reliable decision on accepting a friend request. It is evident from the findings that the proposed method is more reliable compared to the existing FRA methods, which validated the hypothesis of this study.

REFERENCES

[1] H. M. Abdullah and A. M. Zeki, "Frontend and backend Web technologies in social networking sites: Facebook as an example," in *Proc. 3rd Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Amman, Jordan, 2014, pp. 85–89.

[2] B. Liu, Z. Xiao, T. Zhang, and J. Cao, "Analysis on the security mechanisms of user data protection in Facebook," in *Proc. 7th Int. Conf. Comput. Converg. Technol. (ICCCT)*, Seoul, South Korea, 2012, pp. 532–536.

[3] D. Gunatilaka, "A survey of privacy and security issues in social networks," in *Proc. 27th IEEE Int. Conf. Comput. Commun. (ICCC)*, Washington, DC, USA, 2011, pp. 1–12.

[4] C. Vorakulpipat, A. Marks, Y. Rezgui, and S. Siwamogsatham, "Security and privacy issues in Social Networking sites from user's viewpoint," in *Proc. Technol. Manage. Energy Smart World (PICMET)*, Portland, OR, USA, 2011, pp. 1–4.

[5] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, Jul./Aug. 2011.

[6] H. Q. Nguyen-Son, M. T. Tran, H. Yoshiura, S. Noboru, and I. Echizen, "A system for anonymizing temporal phrases of message posted in online social networks and for detecting disclosure," in *Proc. 9th Int. Conf. Availability, Rel. Secur. (ICARS)*, Fribourg, Switzerland, 2014, pp. 455–460.

[7] F. Hattingh, A. Buitendag, and W. Thompson, "User willingness to accept friend requests on SNS: A Facebook experiment," in *Proc. IST-Africa Conf.*, Le Meridien Ile Maurice, Mauritius, 2014, pp. 1–8.

[8] T. Maune, Newson6. (2013). *Family of North Tulsa Teenage Girl Devastated by Her Stabbing Death*. Accessed: May 31, 2017. [Online]. Available: http://www.newson6.com/story/21445401/family-of-north-tulsa-teenage-girl

[9] J. Caramujo and A. M. R. da Silva, "Analyzing privacy policies based on a privacy-aware profile: The Facebook and LinkedIn case studies," in *Proc. IEEE 17th Conf. Bus. Informat. (CBI)*, Lisbon, Portugal, 2015, pp. 77–84.

[10] J. P. Mangalindan, Mashable. (2015). *Facebook Likes Don't Go as Far as They Used to in News Feed Update*. Accessed: May 31, 2017. [Online]. Available: https://mashable.com/2015/04/21/news-feed-facebook-likes/#Ju0I7WzcLuqP

[11] J. Constine. TechCrunch. AOL. (2016). *How Facebook News Feed Works*. Accessed: May 31, 2017. [Online]. Available: https://techcrunch.com/2016/09/06/ultimate-guide-to-the-news-feed/

[12] C. Sibona and S. Walczak, "Unfriending on Facebook: Friend request and online/offline behavior analysis," in *Proc. 44th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Kauai, HI, USA, 2011, pp. 1–10.

[13] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," in *Proc. IEEE 24th Int. Conf. Data Eng. (ICDE)*, Cancún, Mexico, Apr. 2008, pp. 506–515.

[14] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Proc. 13th Amer. Conf. Inf. Syst. (AMCIS)*, Keystone, CO, USA, 2007, pp. 339–350.

[15] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," *IEEE Netw.*, vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010.

[16] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2019–2036, 4th Quart., 2014.

[17] V. Sharma, I. You, and R. Kumar, "ISMA: Intelligent sensing model for anomalies detection in cross platform OSNs with a case study on IoT," *IEEE Access*, vol. 5, pp. 3284–3301, 2017.

[18] P. W. L. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2009, pp. 303–320.

[19] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in Web-based social networks," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, pp. 1–38, 2009.

[20] A. C. Squicciarini, F. Paci, and S. Sundareswaran, "PriMa: A comprehensive approach to privacy protection in social network sites," *Ann. Telecommun.-Ann. Telecommun.*, vol. 69, pp. 21–36, Feb. 2014.

[21] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in *Proc. 3rd ACM Int. Conf. Web Search Data Mining*, 2010, pp. 251–260.

[22] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 1–33, 2013.

[23] L. Guo, C. Zhang, and Y. Fang, "A trust-based privacy-preserving friend recommendation scheme for online social networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 4, pp. 413–427, Jul. 2015.

[24] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *IEEE Trans. Mobile Comput.*, vol. 8, no. 5, pp. 606–621, May 2009.

[25] W. Chen and S. Fong, "Social network collaborative filtering framework and online trust factors: A case study on Facebook," in *Proc. 5th Int. Conf. Digit. Inf. Manage. (ICDIM)*, Thunder Bay, ON, USA, 2010, pp. 266–273.

[26] C. Wei, R. Khoury, and S. Fong, "Web 2.0 recommendation service by multi-collaborative filtering trust network algorithm," *Inf. Syst. Frontiers*, vol. 15, no. 4, pp. 533–551, 2013.

[27] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 2435–2443.

[28] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1647–1655.

[29] L. Guo, X. Liu, Y. Fang, and X. Li, "User-centric private matching for eHealth networks—A social perspective," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, Dec. 2012, pp. 732–737.

[30] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: A privacy-preserving attribute-based authentication system for eHealth networks," in *Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Macau, China, 2012, pp. 224–233.

[31] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 9, pp. 1927–1941, Sep. 2014.
[32] C. Vorakulpipat, A. Marks, Y. Rezgui, and S. Siwamogsatham, "Security and privacy issues in sites from user's viewpoint," in *Proc. Technol. Manage. Energy Smart World (PICMET)*, Portland, OR, USA, 2011, pp. 1–4.
[33] M. Z. A. Bhuiyan, G. Wang, J. Wu, J. Cao, X. Liu, and T. Wang, "Dependable structural health monitoring using wireless sensor networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 4, pp. 363–376, Jul./Aug. 2017.
[34] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generat. Comput. Syst.* vol. 74, pp. 76–85, Sep. 2017.
[35] J. Li *et al.*, "Secure distributed deduplication systems with improved reliability," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3569–3579, Dec. 2015.
[36] S. Peng, G. Wang, and D. Xie, "Social influence analysis in social networking big data: Opportunities and challenges," *IEEE Netw.*, vol. 31, no. 1, pp. 11–17, Jan./Feb. 2017.
[37] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.* vol. 72, pp. 1–12, Jan. 2018.
[38] M. Fire, D. Kagan, A. Elyashar, and Y. Elovici, "Friend or foe? Fake profile identification in online social networks," *Social Netw. Anal. Mining*, vol. 4, no. 1, p. 194, 2014.
[39] I. Gulenko, "Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness," *Inf. Manage. Comput. Secur.*, vol. 21, no. 2, pp. 91–101, 2013.
[40] R. Chakraborty, C. Vishik, and H. R. Rao, "Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing," *Decision Support Syst.*, vol. 55, no. 4, pp. 948–956, 2013.
[41] R. Dey, Y. Ding, and K. W. Ross, "Profiling high-school students with Facebook: How online privacy laws can actually increase minors' risk," in *Proc. Conf. Internet Meas. Conf.*, 2013, pp. 405–416.

MD. ARAFATUR RAHMAN (M'14) received the Ph.D. degree in electronic and telecommunications engineering from the University of Naples Federico II, Naples, Italy, in 2013. He was a Post-Doctoral Research Fellow with the University of Naples Federico II in 2014 and a Visiting Researcher with the Sapienza University of Rome in 2016. He is currently a Senior Lecturer (equivalent to an Assistant Professor) with the Faculty of Computer Systems and Software Engineering, University Malaysia PAHANG. He has developed excellent track record of academic leadership as well as management and execution of international ICT projects that are supported by agencies in the Italy, EU, and Malaysia. He has co-authored of over 60 prestigious IEEE and Elsevier journal and conference publications. His research interests include Internet-of-Things, wireless communication networks, cognitive radio network, and vehicular communication. He is a fellow of the IBM Center of Excellence, Malaysia. He has received number of prestigious international research awards, notably the Best Paper Award at ICNS'15, Italy. He received the Best Masters Student Award, ITEX'17 Awards in International Exhibitions, Malaysia, and iENA'17, Germany. He has served as the publicity chair, session chair, programme committee and member of technical programme committee in numerous leading conferences worldwide.

VITALIY MEZHUYEV (M'14) received the B.S. and M.S. degrees in physics and informatics from Berdyansk State Pedagogical University (BSPU), Ukraine, in 1997, the Ph.D. degree in physics instruction from Kiev National Pedagogical University in 2002, and the Sc.D. degree in information technologies from Odessa National Polytechnic University, Ukraine, in 2012. From 2004 to 2014, he was the Head of the Department of Informatics and Software Engineering, BSPU. He is currently a Professor with the Faculty of Computer Systems and Software Engineering, University Malaysia PAHANG, and the Head of the Software Engineering Research Group. During his career, he participated in the multiple international scientific and industrial projects, devoted to formal modeling, design, and development of advanced software systems as a network-centric real-time operating system; IDEs for the automation of development of parallel real-time applications; tools for specification, verification, and validation of software products; visual environment for metamaterials modeling and others. His current research interests include formal methods, metamodeling, safety modeling and verification of hybrid software systems, and the design of cyber-physical systems.

MD ZAKIRUL ALAM BHUIYAN (M'09–SM'17) was an Assistant Professor with the Temple University. He is currently an Assistant Professor with the Department of Computer and Information Sciences, Fordham University, Bronx, NY, USA. His research interests include dependable cyber physical systems, WSN applications, big data, cloud computing, and cyber security. He has over 100 publications that have appeared in the prestigious journals/conferences in the domain, including the IEEE TII, IEEE TC, IEEE TPDS, IEEE TDSC, ACM CS, ACM TOSN, ACM TAAS, IEEE SECON, IEEE/IFIP DSN, IEEE SRDS, IEEE DCOSS, IEEE MASS, and IEEE DASC. He is a member of the ACM. He has received the IEEE TCSC Award for Excellence in Scalable Computing for Early Career Researchers (2016–2017), the IEEE Outstanding Leadership Award (2016) and Service Award (2017), the Young Scientist Funding Award, China, the Provincial Best Ph.D. Thesis Award, and the Best Paper Awards (IEEE MASS 2016 and IEEE ISPA 2013). He has served as the general chair, program chair, workshop chair, publicity chair, TPC member, and a reviewer of various international journals/conferences. He is currently the General Chair for IEEE DASC 2018, Greece, and DependSys 2018, China, and the Program Chair for IEEE I-SPAN 2018, China, and IEEE SmartWorld 2018, China, and a TPC Member of IEEE INFOCOM 2018, USA. He has also served as an Associate/Lead Guest Editor for key journals, including the IEEE TRANSACTIONS ON BIG DATA, the *ACM Transaction on Cyber-Physical Systems*, *Information Sciences*, the IEEE INTERNET OF THINGS JOURNAL, and FGCS.

S. M. NAZMUS SADAT is currently pursuing the Ph.D. degree with the Faculty of Computer Systems and Software Engineering, University Malaysia PAHANG. His main areas of research interest are social networking.

SITI AISHAH BINTI ZAKARIA is currently pursuing the master's degree with the Faculty of Computer Systems and Software Engineering, University Malaysia PAHANG. Her main areas of research interest are social networking.

NADIA REFAT is currently pursuing the Ph.D. degree with the Center for Modern Language and Human Sciences, University Malaysia PAHANG. Her main areas of research interests are technology-based learning and social networking.