Dynamic Weight on Static Trust for Trustworthy Social Media Networks

Mohammad Khaliqur Rahman
Dept. of Information and Communication Technology
Bangladesh University of Professionals
Dhaka, Bangladesh
mkrahman.dhk@gmail.com

Muhammad Abdullah Adnan
Dept. of Computer Science and Engineering
Bangladesh University of Engineering and Technology
Dhaka, Bangladesh
adnan@cse.buet.ac.bd

***Abstract*—Something in our mind does not always reflect with our fingers on keyboard and mouse, but we respect our blood which might be the way out of the wariness in usage of social media networks today. Social media networks are already the largest network among the population across our globe and for sure, it will not stop expanding its territory. Security vulnerabilities on the other side have been mounting in parallel. A comprehensive effort to change ourselves along with reversing the process or architecture of social media network sites might be the solution of this serious but unavoidable problem. We can create a trusted social media network model that will ensure trust level of a user to connect with other users. Users can trust each other based on the trust level. A lot of research has been done on trust model for social media networks and till now none is established effectively as most of them fail to capture user's trustworthiness with full proof. In order to signpost user's trustworthiness, we model trust with two components: i) Static Trust and ii) Dynamic Weight on Trust. Static Trust is captured by anti-anonymity process based on genealogical tree which will not be changed frequently. And Dynamic Weight on Trust is an algorithmic process to determine score based on predefined scoring scale that is applied on user's genealogical tree and community members. Evaluation of the above model on selected user group is quite positive in taking decision for users when (i) connecting with new friends (ii) self-representing in trustworthy manner. Our proposed trust model fully eliminates anonymity in social media networks which will be a trusted zone for users.**

Keywords—social networks; trust model; genealogical tree; social trust.

INTRODUCTION

The age of human civilization is more than 5500 years in geographical space [1] and currently leading to post-modern civilization specifically Age of Big Data [2]. Cyberspace is a product of this era [3]. In contrast the age of social media networks is less than 20 years [4] in cyberspace which consist of virtual society without social guardians. Although our maturity in cyberspace is less than one human generation [5], the growth of social media networks is unpredictably high [7]. Due to this large number of population in borderless environment, nowadays social media networks are being treated as social, national or even world threat considering the fact that economies, businesses, terrorisms and crimes are using it as the world's fastest and largest information passing and storage. Moreover, many studies are found [31] [32] describing the dark sides of social media and its destructive as well as influential power. Social thinkers and experts are trying to motivate people to use social media like STOP-THINK-CONNECT to protect individuals from the harmful effect of social media networks. Most of the organizations are making new strategies to secure their businesses from this clutch. Countries are taking steps like banning some social media entirely, limiting access for certain period, or educating people to get only the positive parts of social media networks.

Since 2004, social media network sites are using web 2.0 that enabled users to publish their generated content for establishing virtual community with their own view and thoughts [7]. Consequently millions of people are daily uploading their messages, pictures, videos and creating their own pages where others put likes, follow their favorites, post their comments or views. If we think this is the first generation user of social media networks then what will happen with second, third, fourth and so on generations? Due to young age of social media networks, it has not risen yet, but when it will pass the first generation; obviously people will be eager to trace their ancestor's likes, messages, comments, videos and finally lifestyles. Current social media networks focused on friends, fans, followers and professional connections but lack in focusing on family relationship or family tree though only Facebook has option for adding family relatives to some extent. In addition, existing social media network sites are maintaining weak ties [8] that lead anonymity of people; which is the key of several cybercrimes and trustless CyberSociety [9]. Problem of anonymity will be minimized and future needs of people will be implemented by our novel trust model that is Dynamic Weight on Static Trust in short DWSTrust model. In this model, we realize two aspects of human trust: static and dynamic. Static trust indicates the trustworthiness of a user which is determined by predefined set of rules on family tree member(s) such as his parents and own generation. We put dynamic weight on this static trust based on algorithmic solution on member's family tree and community in social media networks using a set of numeric values for each member in accordance with the generation. Our developed web application implementing our trust model is evaluated on selected user groups. Results show more than 85% people feel more confident and safe when connecting with new friends, 80% think our model eliminates anonymity in social-network and 86% people think our system help them in decision making.

The remaining part of this paper is organized as follows. Section 2 covers literature review of various trust models for social media networks. Section 3 presents the current anonymity process and family tree existence in social media network sites. In Section 4, we propose our novel trust model. To validate our model, we built an application software implementing our trust model and evaluated based on user feedback which is described in section 5. Benefits and limitations of this model are discussed in Section 6. Finally we conclude our paper in Section 7 with future plan.

RELATED WORKS

This section analyzes most current and wide spread works related to trust model of social media networks. There are two types of trust models considering reputation systems i) direct (peer to peer feedback) and ii) indirect (based on inference) [10]. Both of them are feedback-oriented. Direct trust is calculated by aggregating and averaging quantitative feedbacks from one user to another. Many researchers developed algorithms to calculate score considering time span like - reputation will be blurred over the time [11]. On the other hand OnlyLast [12] reputation system stands on the latest reputation - it does not consider anything other than the last reputation. In contrast, we are using totally different type of data for direct trust which is genealogical tree.

Indirect reputation system works on inferences based on various data processing algorithms such as deep learning [23], TISoN [13], TidalTrust [14], RN-Trust [15], SWTrust [16] algorithms that work on social/trusted graph where nodes are users, edges are relationships, edges labels are trust levels. Signed edge initiated by Guha et al. [17] to consider not only trust but also distrust which means positive and negative edges. After that several researchers worked on improving edge sign prediction in different ways. Keungegis et al. [18] analyzed multiple levels such as (i) global level: signed clustering coefficient and relative signed clustering coefficient, (ii) node level: negative ranking and popularity measure, (iii) link level: spectral similarity measure. They concluded with the phrase “the enemy of my enemy is my friend.” Link label prediction problem arose by P. Agrawal et al. [19] and proposed MF-LiSP (Matrix Factorization for Link Sign Prediction) where they used 1 for positive links and 0 for negative links in their theorem. Leskovec et al. [20] worked on links in a social network to define its sign, depending on whether it expresses a positive or negative attitude from the generator of the link to the recipient, which refers to trust among both of them implementing socio-psychological theories of balance and status. S.H. Yang et al. [22] worked on the same principle. A. Papaoikonomou [23] also worked on the same principle to define level of trust between couple of users according to their ratings on set of items. Their focus was to complete the full graph using partially labeled signed social graph. Unlike indirect trust algorithms, we are using signed value for friends score based on Trusted or Non Trusted state.

There are many other researchers who worked on modeling the trust to quantify it as a score to safe potential victim based on past activity by predicting future. ReGret [24] reputation system considered individual, social and ontological dimensions to minimize false, biased, incomplete and correlated evidence problem during reputation calculation. PeerTrust [25] measured trust of peers based on the feedback evaluation considering five different factors. FcTrust [26] worked on dishonest feedback and collusion problem of any feedback based reputation system. SecuredTrust considered load balance to ensure service quality during processing enormous data [10]. Jai Ganesh et al. [27] built Facebook reputation system focusing non-transactional peer to peer reputation in the area where friends and family networks are stronger than that from exchanging goods and services. This system has 10 attributes to rate and calculate the weighted average of ratings provided by all peers to represent the reputation or trust score. Sybil attack is one of the most general problems that still exist in this system where identity of user is a key factor for the problem.

Recent survey [28] said that trust communities or trust zone will play a vital role to safeguard the privacy concerns and balance the open nature of social media networks. They defined the trust communities that create an environment where members do not need to worry about privacy and can share their feelings, views and experiences freely and frankly. Since quantification of trust is getting more complicated, another most recent survey [29] insisted on investigating it from multifaceted networks consisting of four distinct layers of communication protocols, information exchange, social interactions, and cognitive motivations. Moreover, to make decision, different application domains need different aspects of trust such as emotional, logical and relational trust. Our research, inspired by those survey reports, focuses on real world social-trust to be implemented on online social media networks.

ANONIMITY IN SOCIAL MEDIA

A. *Current Anonymity and Anti-Anonymity Process*

In current popular Social Network Sites (SNSs), e.g. Facebook, Twitter, LinkedIn, MySpace, Hi5, accounts can easily be created with anonymity by using anonymous email addresses. Most of the popular email services require phone numbers where they send verification CODE or voice contact. User is asked to enter that code to activate the corresponding email account. Mobile number or phone number is trusted as those are registered according to a country’s government policy. But there are many email services that do not follow the verification process. There are very few email services that made phone number as mandatory as shown in TABLE I. A large number of free and public email service providers are not enforcing this *anti-anonymity* process. As a result anonymity still exists at large. Moreover, corporate emails or domain based email addresses can be anonymous.

TABLE I. EMAIL SERVICES LIST

Email Services	Phone Number Required	Comments
Yandex.com	No	
Mail.com	No	
GMX.com	No	
Outlook.com	Not Mandatory	Need phone number or alternate email address
Inbox.com	Unknown	Temporarily stopped to create new registration due to up-gradation
Tutanota.com	No	
Gmail.com	Yes	
Yahoo.com	Yes	
AIM.com	Yes	

B. *Family tree and anonymity*

Many researches show that healthy family relationships decrease human mentality for violence, even in the online social networking platform. This implies that presence of family members will make a person more inclined to safe and peaceful sharing, surfing, posting any video or connect with others. In current social and economic context, many families are trying hard to make strong and healthy bonding among family members. It is true that many of them are not able to balance with time and effort in both family and work. Family tree in social media networks can create opportunity to group all family members in virtual platform called "cyberFamily". Family interaction in SNSs can open a new window to maintain good relationship in a stronger and consistent way between all family members.

Except Facebook there is no option for family tree buildup in popular SNSs. It denotes that Facebook thought about this requirement but is not focusing on it too much. As of now Facebook has option for adding family members which is shown as a list in personal profile. There is no tree view or generation view for family tree. In addition, a family tree can contain anonymous users. In some SNSs with anonymity process, if someone can manage an anonymous email address then it is possible to create an account, sign-in with, and eventually it is possible to find a place in the SNSs anonymously.

Proposed Trust Model

Social Media is the top most channels for communication among people across the globe. Anonymity and virtual connectivity with each other create insecure cyberspace which leads people to uneven social behavior and commit cybercrime or instigate worldwide crime. Governments from most of the countries are concerned to protect people from the wicked domain of this modern innovation. Though, life without social media is considered to be impossible nowadays. So, secure interaction in social media is a crying need for the people around the world.

Genealogical or Family Tree is the main component to build our trust model. There exist many sites to manage family tree. But those are not popular as social network sites. On the other hand many popular social network sites are not focused in putting family tree. Although the notion of family tree is missing in these sites, often family members coexist in the same network as a friend or follower or fan. Hence we can easily build a family tree even if it does not exist in the architecture of the SNSs. Using the family tree, we propose our novel approach for securing social media by calculating trust. To realize trust quantitatively, we compute two quantities for trust baseline: A. Trust Value, B. Trust Score. Trust Value captures the static component of human trust while Trust Score changes dynamically with human connection in SNSs. Both of those trust indicators are based on Generation Circle illustrated in *Fig. 1.*

A. Generation Circle

We introduced a novel concept of "*Generation Circle*" this is the basis of our dynamic weight and static trust calculation. Trust scaling is made by this circle. Inner side of the circle represents ancestors and outer side for future generations.

Generation circle will be built gradually and as much as possible. People will be able to create profile for their kids as well, so that no one will be out of the circle in social media. Parents will be able to ensure their kids safety as they can see the trust value and score of their kids. Adults will be ensured that they are in safe place and connecting with trusted people. This model will capture users' family tree for thousand years, even when the user is not present in the world but the future generations will know about their root. This model will make our social media more reliable and acceptable for thousand years as this contains the generation in long run. Anyone can start creating their generation circle anytime and continue updating it generation by generation. People under this umbrella will do less likely harmful things as their blood relatives and family members are present in the scene, so that anonymity and uneven social behavior will be reduced.

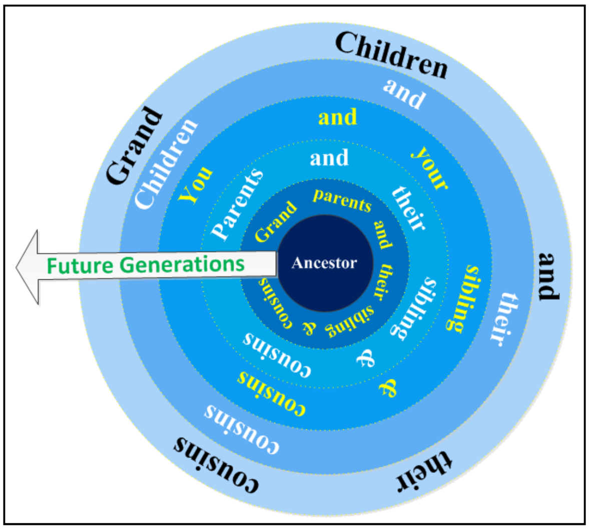

Grand Children and their cousins
Children and their cousins
You and your sibling & cousins
Parents and their sibling & cousins
Grand parents and their sibling & cousins
Ancestor
Future Generations

Fig. 1. Generation Circle

B. Trust Value (Static Trust)

Elimination of anonymity is the motivation to define *Trust Value*. Genealogical tree is the evidence of human root. So, this is the right choice for *Trust Value* assessment. We are assessing *Trust Value* based on following logics:

1) Trusted (Fully): At least parents (single or two) and five blood relatives accepted the request by creating family tree.

2) Partially Trusted: At least parents (single or two) and three blood relatives accepted the request by creating family tree or user was trusted but score is under minimum range to become Trusted which is (2+5=7) TABLE III.

3) Non-Trusted: Not yet achieved above two conditions.

Maintaining three states of *Trust Value* is the best way to guide users before connect with anyone online. Direct indicator is very useful for users in making quick decision. In our applied logics; parents must be entered, single parent is acceptable but both are expected in order to become *Trusted* or *Partially Trusted*. Step by step a user will be *Trusted* from *Non-Trusted* state by exposing their family tree and *request-response* process TABLE II. Trusted zone or communities will be built in SNSs which is currently missing by name/indicator. We named this trust (*Trust Value)* as *Static Trust*, since it is never changed once anyone become *Trusted* unless the user removes someone from the family tree and does not meet *Trust Value* logics.

C. Request-Response to build Static Trust (Trust Value)

Static Trust is determined based on a person's Request-Response process. Implication of this process is to remove anonymity in SNSs. Since, responders accept the blood relation exists with the requester.

Our proposed trust model works on this request-response mechanism, explained in TABLE II. In this table Sally invited three blood relatives to confirm her trust level, as she is a new user with *Non-Trusted* state and did not has any invitation. Sally added her parents and then invited three blood relatives. Invitation notification can be sent by email or SMS or any other convenient way. Whenever the invited user signed-up using the invitation code then the requester user will be stepped up toward *Trusted*. In this way if a person got 3 blood relatives with her parent(s) in the *Generation Circle* then she will be *Partially Trusted*. Consequently when she got 5 blood relatives to accept her invitation then the requester user is *Trusted*.

D. Trust Score (Dynamic Weight on Trust)

This is the second part of our trust model which will play vital role in measuring the weight on trust (WOT). *Trust Score* is a quantitative measurement to determine WOT dynamically. This score is calculated using two components such as i) *Generation Circle Fig 1,* ii) Friends community. We start from user's own generation that has the value 0 and called *Generation Number* represented by *g* is one *Generation Circle* and this value increases or decreases based on |g|+1 toward descendent (future generations) or ancestor shown in TABLE III. Next, each member of friend's community can be *Trusted* or *Non-Trusted* based on our *Static Trust (Trust Value)*. Each *Trusted* friend will add 1 (positive value); on the other hand each *Non-Trusted* friend will reduce 1 (negative value) to the users score shown in TABLE III. Generations have shown in TABLE III, is not limited to and it will be expended in both directions (Ancestor and Descendent). Here we used own generation as 0 and then descendants increased by 1 and ancestors are decreased by 1 for each generation. The justification of this value is real world matter. For instance, in our *Generation Circle* each generation must grow one by one. It is not possible to grow generations by skipping any generation. In real world complex scenario it is possible to find that mother or father can be married with one step upper/lower generation relative. Multi-marriage factor can make some complexity but in our system it is handled by the theory: *always take the greatest value of multi-generation impact*.

TABLE II. REQUEST AND RESPONSE PROCESS

Name	Trust Value	Name	Trust Value	Relation	Invited By
Sally	Non-Trusted	Sohana	Non-Trusted	Sister	Sally
Sally	Non-Trusted	John	Non-Trusted	Brother	Sally
Sally	Non-Trusted	Robin	Non-Trusted	Brother	Sally
Sohana, John and Robin accepted the request sent by Sally. Sally has added her parents already in her family tree and she became partially trusted.					
Sally	Partially Trusted	Bob	Non-Trusted	Son	Sally
Sally	Partially Trusted	Jolly	Non-Trusted	Daughter	Sally
Whenever Bob and Kim accept the request, Sally will be fully trusted.					

TABLE III. TRUST SCORE

Relation	Generation	
	Number (*g*)	Score (|*g*|+1)×*v* (G)
Siblings and cousins	0	1
Children and their cousins	1	2
Grand Children and their cousins	2	3
Great Grand Children and their cousins	3	4
Great Great Grand Children and their siblings	4	5
Parents	-1	2
Grand Parents and their siblings	-2	3
Great Grand Parents and their siblings	-3	4
Great Great Grand Parents and their siblings	-4	5
Friends Community		
Trusted Friend	N/A	1
Non-Trusted Friend	N/A	-1

For example, if a user is trustworthy but WOT is less than the expected or negative then it will reflect vulnerability of users' activities. *Trusted* user will be able to communicate with other user easily. *Non-Trusted* user will also be able to communicate with other user with *Non-Trusted* notification. *Trusted* or *Non-Trusted* people can have *Trusted* friends or *Non-Trusted* friends and this will reflect in their Dynamic WOT.

We added the sensitivity parameter *v* (TABLE III) to make variance of *Trust Score* on horizontal (same generation) and vertical (different generation) growth of family tree. To establish significant difference on *Trust Score* in horizontal and vertical growth, value of the parameter needs to be increased. By default we used *v*=1. In sensitivity analysis part we explained in detail of its impact.

In our model, user can put privilege on their family tree to protect data privacy. Family tree can be secured by making it private or viewable for specific user or public. Trust level will be created based on response and acceptance of a user's invitation to his relatives. This model also ensures loose-coupling among users in a trusted environment. Once someone is *Trusted*, people will feel free and secure to communicate with the user.

Direct reflection of dynamic social bonding with other people is the key of calculating *Trust Score* which stands for the dynamic weight on *Static Trust*. From TABLE III, we can calculate Dynamic WOT according to the following equation:

$$TS = \sum_{g=NG}^{AG} X_g \times (|g|+1) \times v + X_{tf} \times T + X_{nf} \times N \qquad (1)$$

where,

TS	=	Trust Score / Dynamic WOT
X_g	=	Number of family members added in the particular generation circle
v	=	Sensitivity parameter for vertical vs horizontal growth of family tree
AG	=	Number of ancestor generations
NG	=	Number of next (descendent) generations
g	=	Generation Number
X_{tf}	=	Number of Trusted Friends
T	=	Trusted Friends value is always 1
X_{nf}	=	Number of Non-Trusted Friends
N	=	Non-trusted friends value is always -1

To implement our novel trust model we defined following algorithms and procedures to retrieve users' generation (Algorithm 1), that uses couple of procedures named getParent() and getChildren() to identify parents and children. SET of parents and children are merged to create single SET of all family members of the user along with *Generation Score G* according to TABLE III.

Algorithm 1: getGenerationTree

```
Input:   User $a$ to find his ancestors and descendent
Output:  set of all members $M$ in the Family Tree with generation score $G$
if $a$ != 0 then
    $M := (a,G)$
    $M := M$ U getParent($a$,-$G$) U getChildren($a$,$G$)
end if
return $M$
```

Recursive procedure getParent (Procedure 1) and getChildren (Procedure 2) are to traverse root parents and all children of the family tree. Both works from same point that is user *a* then getParent() go upward and getChildren() go downward.

Procedure 1: getParent()

```
Input:   Member a to find his ancestors, score G of member a
Output:  set of all parent members P in Family Tree with generation level
if a = 0 then
    return Null
else
    for each Parent x of a
        P := P U (x,G-1) U getParent(x,G-1)
    end for
    return P
end if
```

Procedure 2: getChildren()

```
Input:   Member a to find his descendent, score G of member a
Output:  set of all children members C in Family Tree with generation
         level
if a = 0 then
    return Null
else
    for each Children x of a
        C := C U (x,G-1) U getChildren(x,G-1)
    end for
    return C
end if
```

Output of Algorithm 1 is set of all members *M* that is the input to getTrust (Algorithm 2). This algorithm is pretty simple to determine the users' *Static Trust* (*Trust Value*) in three numeric state, where 0=*Non-Trusted*, 1=*Partially Trusted*, 2=*Trusted* basis on *Trust Value* logics. Here Minimum Trust Score (MINTS) to become *Trusted* is 7. Because in our logic to become *Trusted* user must have parents (at least single) which will give 2 points then at least five blood relatives will be participated that will give another at least 5 points. So, MINTS goes to (2+5) = 7 to be *Trusted*. This MINTS used in getTrust (Algorithm 2).

Algorithm 2: getTrust

```
Input:    User a, members (blood relatives) of his/her family tree those
          are responded against request M
Output:   Trust value t which will be 0=Non-Trusted, 1=Partially-
          Trusted, 2=Trusted
constant MINTS:=7
if checkParents(a) = true then
    if count(M)>=5 then
        t := 2
    else if count(M)>=3 then
        t := 1
    else
        t := 0
    end if
else
    t := 0
end if
if t = 2 and getTrustScore(a) < MINTS then
    t := 1
end if
return t
```

Dynamic WOT (*Trust Score*) calculated by getTrustScore (Algorithm 3) that is to generate second component of our trust model. In this algorithm we implement (1) to aggregate number of member and multiplication with generation score *G*. Furthermore, signed value of friends (*Trusted* =1 and *Non-Trusted* = -1) summarized to get final *Trust Score*.

Algorithm 3: getTrustScore

```
Input:    User a, members with generation score G of his/her family
          tree M, friends F with trust value, sensitivity parameter v
Output:   Trust Score TS of the member a
TS := 0
for each x element of M do
    TS := TS + absolute(M(x)*G)
end for
for each x element of F do
    if F(x).trustvalue =2 then
        TS = TS + 1
    else
        TS = TS - 1
    end if
end for
return TS
```

E. Data Flow

Data flow illustrates the *request-response* process demonstrated in the TABLE II. In addition it shows both *Trusted* and *Non-Trusted* friends connected with the user along with added parents and blood relatives. According to the data flows of diagram *Fig. 2,* user *Sally* has been done activities described in TABLE II. At the beginning, her *Trust Value* was *Non-Trusted* and *Trust Score* was equal 0. Afterward, two parents (DataFlow-1) added and she got |g|+1* 2=2*2=4 as score, *Trust Value* was unchanged. She sent request to three blood relatives (DataFlow-2). After acceptance of her requests (DataFlow-3), *Sally* got 1 point for sister, 1 point for each brother, so total score was 4+1+1+1=7 as a result she became *Partially Trusted*. She sent request (DataFlow-4) to her son and daughter, consequently they accepted her requests (DataFlow-5) then *Sally* got another 4 points and total points grown up to 11 and *Trust Value* changed to *Trusted* state. Next, she started to add her friends. First she added one *Non-Trusted* friend (DataFlow-6), as a result she lost 1 point from her total points. Afterward she added another *Trusted* friend and got 1 point. There is no limit or threshold on *Trust Score* for both positive and negative points. Finally, her trust indicator has shown *Trusted* with *Trust Score* 11.

EVALUATION OF THE MODEL

A. Comparison with different systems

Most of the e-commerce sites use reputation system to show level of trust of seller or buyer, that implements peer to peer feedback or inference based signposting mechanism and often use STAR (☆) or numeric values for signaling. Moreover, reputation system is not viable in social media sites, because of asymmetric process, where one post, viewed by many people and it is not expected that all the viewers will provide feedback. In contrary social media network sites do not have any transactional interactions between a person's post and other persons' views.

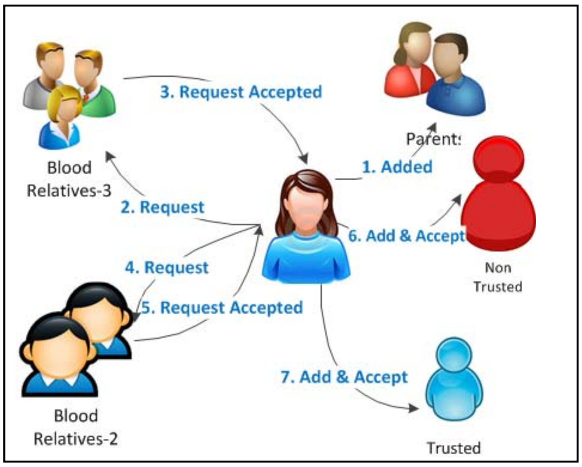


Fig. 2. Data flow of the model

On the other hand social media network sites have severe problems with anonymity. In this paper we eliminate the anonymity problem of the social media networks using genealogical tree.

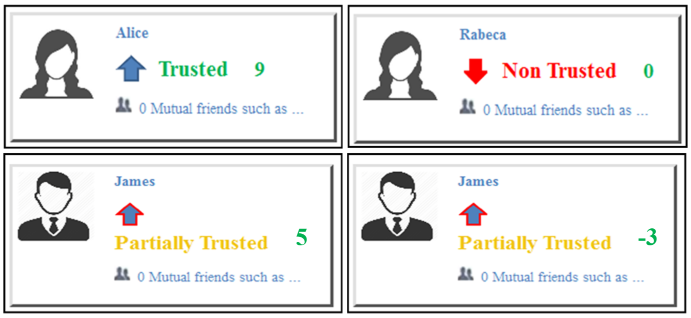
Genealogical sites are getting popular in current world to find identity using blood relations that inherently eliminate anonymity. TABLE IV, shows the number of transactions or users exist in various reputation system, social media sites and genealogical sites. This infers that genealogical records are increasing and people are motivated to build their family tree. In this discussion we emphasize that next generation social network sites would be genealogy based social media network, where people will never be anonymous rather they will be present with their ancestors and all family tree members.

TABLE IV. TRUST IN VARIOUS SYSTEMS

Various Systems	Trust	Sites	# of Users (millions) [6]
Reputation System	Trust built by feedback mechanism.	eBay	162 (1st quarter 2016)
		Amazon	304 (end of 2015)
		Alibaba	423 (2016)
Genealogical Sites	Trust created on family tree and relatives.	Ancestry	Paid user: 2 Family tree: 70 Historical records:16000
		MyHeritage	Family tree: 80
Social Network Sites (March 2016)	Trust on friendship, common interest, liking or followers etc.	Facebook	Registered user: 2000+ Active user: 1650
		Twitter	Registered user: 1000+ Active user: 310
		LinkedIn	Registered user: 433 Active user: 106
Our Proposed Model-DWSTrust	Trust built on family tree and friends.	WeInTrust	Evaluated by more than 100 registered users and 56 users participated in survey.

B. Development of the Application

We have developed the system using PHP 5.6.*, apache 2.4.*, MySql5.5.22 database in Linux platform and hosted on www.weintrust.com. The web application calculates *Static Trust* and Dynamic WOT based on *Trust Value* logics and *Trust Score* by Equation (1). Both are implemented using Algorithms 1, 2 and 3. This approach can be integrated with any social network sites. The home page of the application shows three parts (a) own information with own trust indicator, (b) generation information with number of trusted/ non-trusted ancestors/descendants, (c) friends information with their trust value and score *Fig. 3.* A user can see his/her friend list with *Trust Value (Static Trust)* and *Trust Score (Dynamic WOT)* from the application individually. Due to page limitation we omit the details of our GUI design for the web application.



Alice
Trusted 9
0 Mutual friends such as ...

Rabeca
Non Trusted 0
0 Mutual friends such as ...

James
Partially Trusted 5
0 Mutual friends such as ...

James
Partially Trusted -3
0 Mutual friends such as ...

Fig. 3. Friends Information

We evaluated our system in two dimensions: (i) User Experience, (ii) Performance of the system with users.

C. User Experience

People get interested to use our system for new experience and thought, direct trust indicator and dynamic weight on trust. Staying with ancestors and descendants encourage them to use our application. On the other hand they were concerned about their data privacy which was mitigated using privilege based data access control. By default only family members are able to see their tree and communicate with other members directly. In our survey we selected user group (56) according to three basic categories based on usage of social networks such as Regular , Occasional and Do not use SNSs. We judged user experience on our model in 6 categories: 1) Effectiveness 2) Decision Making 3) User Friendly 4) Behavioral Change 5) Anonymity 6) Safety. We asked multiple questions in each category to get their feedback regarding our novel trust model as well as its social benefit. Aggregated values of each group of questions are presented in *Fig. 4*.

D. Performance Evaluation

Since, *Trust Value* is static, in considering performance issues we designed our system in such a way that *Trust Value* will be preserved at user level and it is easy to retrieve without hampering performance. Once a user achieves the *Trusted* state, generally this data will not be updated, except for couple of cases mentioned earlier. This static nature of *Trust Value* gives the opportunity to store *Trust Value* for each user. Hence we do not need to compute *Trust Value* every time to get *Trust Score*. This approach improved the performance of computing both trust value and score for each friend. *Trust Score* is calculated dynamically whenever the *Trust Value* of any friend is updated. We measured performance in two ways: (a) Adding more members into the family tree distributed in different generations, (b) Adding large number of *Trusted*, *Partially Trusted* and *Non-Trusted* friends.

i) Growth of Family Members

In *Fig. 5,* we put two types of data for each of the two columns. Here dashed series stands for a users' family tree with 100, 200, 300, 400 and 500 members in one generation. And dotted series for same number of family members distributed in 4 generation circles such that each ¼ of members are spread out equally across own, parents, grandparents and children's generations. Y axis represents the time in millisecond and X axis shows members. Average time difference between each 100 members' increments for single generation is 37.5 millisecond and for multi generations are also 37.5 millisecond. This concludes that various generations do not have any impact on performance.

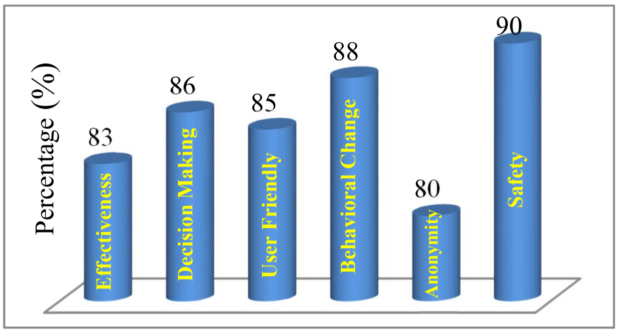


Fig. 4. User Feedback

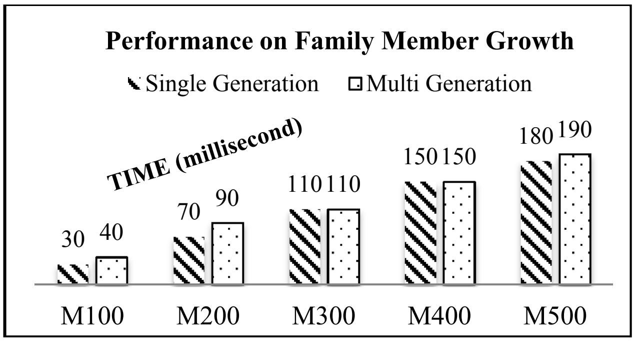


Fig. 5. Growth of Family Members

ii) Friends' Growth over Family Member

Using growth of friends with equally distributed state such as *Non-Trusted*, *Partially Trusted* and *Trusted*, over the growth of family members distributed in four different generations, evaluated in *Fig. 6.* Here X axis shows friends' growth and five different color stands for number of family members along with time in millisecond put Y axis. Average difference between 100 family members with different number of friends such as (100, 200, 300, 400 and 500) is 100 millisecond. Consequently, for 200 members with same series of friends average process time is 110, for 300 members is 110, for 400 members is 100.75, for 500 members is 110.75. We can summarize that growth of friends over members are almost consistent even the process is taking time to gather generation information.

The above performance testing is done on local server (dual core 3.10 GHz, 8GB RAM) with other server applications running. So it took little bit long time to perform the testing process. Performance will be increased by putting all those things in cloud based implementation using BigData platform. And also there are scopes to tune performance on processing family tree data for such implementation.

E. Sensitivity Analysis:

Generally users will be intended to increase *Trust Score* to become trustworthy. Our focus is to encourage users to increase vertical growth of family rather horizontal growth. So, large value of the parameter *v* will increase *Trust Score* once a user adds more generations rather than increase members in own generation or trusted friends. In the sensitivity analysis illustrated in *Fig. 7*, we consider 30 family members in own generation (represented by BLUE), equal distribution of members in two generations (represented by RED) and equal distribution of members in three generations (represented by GREEN). We use three different values for the sensitivity parameter (*v*=1, 2 or 3) in (1) and show that Trust Score increases more for vertical growth. Although the growth of score across generations increase, the percentage of score uplift remain same.

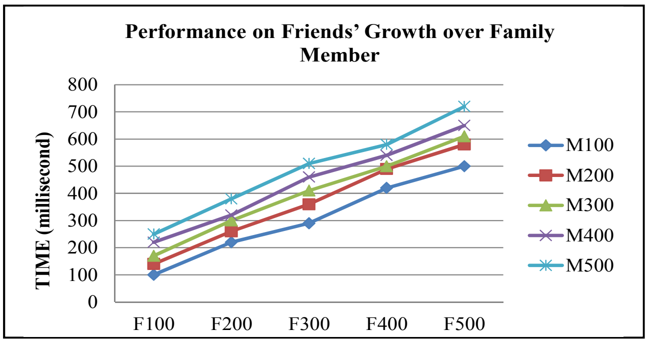


Fig. 6. Friends' Growth over Family Member

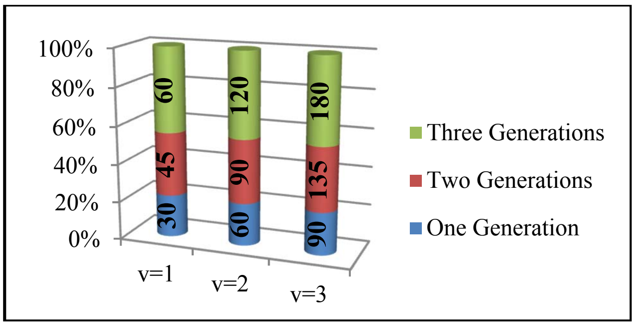


Fig. 7. Sensitivity Analysis

DISCUSSIONS

A. Benefits:

Our trust model addresses two distinct trust components of social trust. One is trust indicator and another is trust weightage. Our novel concept enables a user to take concrete decision on "whom to trust". While interacting with a new person on social media networks, a user will be able to judge instantly. Even after connecting, a user will be able to continuously monitor all of his/her friends' WOT. Correlating the trust value and score, a user will be very safe from unexpected online social interaction. This is the prime advantage of our model.

This model can also reduce uneven social behavior of people who maintain one face online and another in real world. In general anonymity aggravates this behavioral change. Since our system protects anonymity or pseudo-anonymity by staying with family concept, human attitudes remain consistent in both cyber and real world.

On the aspect of social people online, it is expected to improve their behavior and make interested to contribute in the real world society, because offline society exists in online community. According to survey [28], high fame of social media networks and their open nature exacerbate the worries to users regarding various cybercrimes. In order to draw a line between openness and defend from malicious users, it is vital to build trust communities. According to this notion our novel trust model is able to build a trusted community to ensure reduced cybercrimes. No system or model can guarantee complete trustworthiness, but our model is able to make a cyber-environment trustworthy similar to real world.

Considering future generation needs our model is the best suited, because it aims to contain direct link between ancestors, current and future generations via social media networks. When one generation will pass away social media users will feel for their ancestors achievements. Putting this real world future requirement in mind, we embedded genealogical tree to measure trust.

Beside the trust and archive of ancestor historical data, our model will resolve some core current issues of social media networks. One of them is death declaration. Even this feature exists with some social media networks, still it has no answer for "who will declare the death." Family members are exists in our model; they may be allowed to make the declaration.

Recent news shows that Facebook will be the largest graveyard [30].The same issue will arise for all social media networks as well, because those will be in trouble with data fed by death people. No one will be able to claim or pay for the archived data of death people in current model of social media. This problem can be resolved by implementing our novel model, hence, family members are directly coexist.

B. Limitations:

There is no full-proof system or model. Our model also has some limitations. Fake CyberFamily entry could be a big problem which is common for all public online registration system. To achieve falsified *Trust Value* and high *Trust Score*, fake *Generation Circle* would be created. *Non-Trusted* people can create *Non-Trusted* zone that could lead grouping of anonymous users in the same place. In contrast, detection of a single malicious identity will provide the opportunity to detect malicious community as a whole. So, this is a good sign to protect users from harmful community or user. Finally anonymity can also be eliminated scientifically from our model using DNA test that is provided by current genealogical site vendors. That is the real removal of anonymity.

Sybil attacks are also one of the most common problems for any social media networks. This will be reduced due to chain of identity, request and response required in our model to build *Static Trust*. An attacker needs to spend long time in our social media networks trust model to arrange such an attack that requires a lot of *Trusted* friends to boost WOT.

Future Plan and Conclusion

This trust model can be used to generate primary *Trust Value* with *Score* and on top of this we can implement any reputation system based on past activity to predict future action. There are some other parameters which can be used to calculate weight on trust such as how long users are in the social network that refers to time span of a particular users' existence in SNSs. Non existing relationship in real world can exist in virtual world; this is the key vulnerability in the point of trust. Our model achieves *Trust Value* generated from existing relationships in real world and then indicates reliability in virtual world. Besides *Static Trust*, *Dynamic WOT* reflects the aggregation of positive score for *Trusted* friends and negative score for *Non-Trusted* friends. To the best of our knowledge, this is a novel approach for realization of the two inherent characteristics (static and dynamic) of human trust in the Trust Model for SNSs. We try to keep our trust model simple and easy to visualize such that this model can be implemented in any of the existing SNS or Genealogy based sites. Finally our trust model enables signal on trust that will minimize fraudulent activities, anonymity or pseudo-anonymity which effectively creates an environment with positive behavior and overall safe zone for total online user base. In future we will work to improve our model by incorporating other parameters and also work on death model of social media users based on our proposed trust model.

References

[1] A. Takács-Sánta, "The Major Transitions in the History of Human Transformation of the Biosphere," Human Ecology Review, Vol. 11, No. 1, 2004.

[2] http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact in-the-world.html?pagewanted=all&_r=1

[3] L. Hui-Lin et al., "A Comparative study of protocol analysis for Spatiality of a Text-based Cyberspace," 20th eCAADe Con. Poland, '02.

[4] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication 13 page 210–230, 2008.

[5] Charlesworth, B., "Evolution in Age-structured Populations," University of Cambridge Press., 1980, pp. 28–30.

[6] https://en.wikipedia.org/wiki/ , http://www.statista.com/statistics/

[7] A. M. Kaplan *, Michael Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," Business Horizons Volume 53, Issue 1, Jan–Feb 2010, Pages 59–68

[8] C. Haythornthwaite, "Strong, Weak, and Latent Ties and the Impact of New Media," 34th Hawaii Intl. Conf. of System Sciences, Jan 2001.

[9] C. Richards, "Computer Mediated Communication And The Connection Between Virtual Utopias And Actual Realities," Cultural Attitudes Towards Communication and Technology, 173-184, 1998.

[10] A. Das and M. M. Islam on "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," IEEE trans. on depend. and secure comp., vol. 9, no. 2, 2012.

[11] A. Das, M. M. Islam and G. Sorwar on "Dynamic Trust Model for Reliable Transactions in Multi-agent Systems," in Proc. of ICACT, pp. 1101 – 1106, Feb 2011.

[12] C. Dellarocas on "Efficiency and robustness of binary feedback: Mechanisms in trading environments with moral hazard." MIT Center for eBusiness Working Paper #170, 2003.

[13] S. Hamdi, A. Bouzeghoub et al., "Trust Inference computation for online Social Networks," 12th IEEE Intl. Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[14] J. A. Golbeck. "Computing and applying trust in web-based social networks," PhD thesis, College Park, MD, USA, 2005. AAI3178583.

[15] M. Taherian, M. Amini, and R. Jalili,"Trust inference in web-based social networks using resistive networks," 3rd ICIW, p 233–238, 2008.

[16] W. Jiang and G. Wang.,"Swtrust: Generating trusted graph for trust evaluation in online social networks," 10th IEEE Intl. Conference on Trust, Security and Privacy in Computing and Communications TrustCom, pages 320–327, 2011.

[17] R. Guha, R. Kumar, P. Raghavan and A. Tomkins,"Propagation of trust and distrust," in Proceedings of the 13th intl. conference on WWW, New York, NY, USA, 2004.

[18] J. Kunegis, A. Lommatzsch and C. Bauckhage, "The slashdot zoo: mining a social network with negative edges," in Proceedings of the 18th intl. conference on WWW, New York, NY, USA, 2009.

[19] P. Agrawal, V. K. Garg and R. Narayanam, "Link Label Prediction in Signed Social Networks," in Proc. of the 23rd IJCAI, Beijing, China, '13.

[20] J. Leskovec, D. Huttenlocher and J. Kleinberg, "Predicting positive and negative links in online social networks," in Proceedings of WWW '10, New York, NY, USA, 2010.

[21] S.-H. Yang, A. J. Smola, B. Long, H. Zha and Y. Chang, "Friend or Frenemy?: Predicting Signed Ties in Social Networks," in Proceedings of the SIGIR '12, New York, NY, USA, 2012.

[22] S.-H. Yang, A. J. Smola, B. Long, H. Zha and Y. Chang, "Friend or Frenemy?: Predicting Signed Ties in Social Networks," in Proceedings of SIGIR '12, New York, NY, USA, 2012.

[23] A. Papaoikonomou, M. Kardara, T. Varvarigou, "Trust Inference in Online Social Networks," in Proc. of ASONAM, August, 2015.

[24] J. Sabater and C. Sierra, "Social Regret, A Reputation Model Based on Social Relations," ACM SIGecom Exchanges - Chains of Commitment, vol. 3, pp. 44-56, Dec. 2001.

[25] L. Xiong and L. Li, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.

[26] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," Proc. IEEE Ninth Int'l Conf. Young Computer Scientists (ICYCS '08), pp. 1963-1968, 2008.

[27] Jai Ganesh and Puneet Sethi, "Reputation and Trust in Social Networks: Empirical results from a Facebook Reputation system" Nineteenth Americas Conference on Information Systems, August 15-17, 2013.

[28] Sherchan, W., Nepal, S., and Paris, C. "A Survey of trust in social networks." ACM Comput. Surv. 45, 4, Article 47 (August 2013).

[29] Jin-Hee Cho, Kevin Chan, and Sibel Adalı, "A survey on trust modeling," ACM Comput. Surv. 48, 2, Article 28 (October 2015), 40 pages. DOI: http://dx.doi.org/10.1145/2815595

[30] http://www.dailymail.co.uk/news/article-3479288/Facebook-world-s-biggest-virtual-graveyard-profiles-dead-people-living-users-end-century-say-experts.htm

[31] A. Banerjee et al., "Security Threats of Social Networking Sites: An Analytical Approach," Intl. Journal of ERMCA, ISSN: 2319-7471, Vol. 3 Issue 12, Dec.-2014, pp: (1-4)

[32] M. Chewae et al., "How Much Privacy We Still Have on Social Network?", International Journal of Scientific and Research Publications, Volume 5, Issue 1, Jan'15 Edition, ISSN 2250-315