Hybrid Multi-faceted Computational Trust Model for Online Social Network (OSN)

Manmeet Mahinderjit Singh
School of Computer Sciences
University Sains Malaysia
Glugor, Penang

Teo Yi Chin
School of Computer Sciences
University Sains Malaysia
Glugor, Penang

***Abstract*—Online Social Network (OSN) is an online social platform that enables people to exchange information, get in touch with family members or friends, and also helps as a marketing tool. However, OSN suffers from various security and privacy issues. Trust, fundamentally, is made up of security with hard trust (cryptographic mechanism) and soft trust (recommender system); user's trustworthiness for this platform has decrement signed. In this paper, the authors leverage the multi-faceted model trust concept from user-centric and personalized trust model and present weightage and ranking for its important features by employing statistical means. Next, the multi-faceted model trust is combined with an existing Action-based model and Context recommender. The contributions of this research are an enhanced trust algorithm and an enhanced context-based, recommender-based trust, which has been tested based on user-acceptance. Overall, the result demonstrates OSN as fairly better by employing a multi-faceted model which embeds both actions incomparable to recommender type.**

Keywords*—*Multi-facet Trust; Recommender Trust Model; Action Trust; Online Social Network; Security

I. INTRODUCTION

In recent years, online social networks (OSNs) have attracted millions of users worldwide and become part of their daily life. Websites such like LinkdedIn, Twitter, Google+ and Facebook which have been built on social networks are among popular OSNs with millions of users visiting them daily. The purpose of an OSN is, among others, for exchanging personal information, opinion, photographs, building friendships across borders, and as a tool for business advancement and marketing Nevertheless, OSN sites have flaws related to privacy and security leading to untrustworthiness in this technology [1, 12, 23, 24]. There are unprotected user profiles in OSNs which contain high amount of personal information, and therefore, privacy attack such as location and data privacy stands as a major threat of information leakage. Information leakage of user's lifestyle and linkability between various bits of information such as location, time, user-identity and data threaten the well-being of a user in terms of safety [2]. Furthermore, privacy is an important problem within OSN sites, particularly when a genuine OSN user identity and account can be easily accessed publicly via other search engines by simply using the index his/her profile. In short, there is no certainty of user trustworthiness towards the OSN technology which leads to the aim of the paper which is to study in depth the non-trivial trust persona.

In theory, trust refers to the willingness of a party to go through risk taking and to reduce doubt to the lowest degree of confidence [1,3,4]. Trust is fundamentally based on experiences [1,4] and the ability to provide annotations of trust with confidence and without constraint. In the area of computer science, a lot of studies have been conducted revolving trust management, computational algorithms, and trust models. Various trust models in multiple domain have been proposed such as User-Centric Personalized Trust model, TISoN, regret, and Spares and Marsh's trust model. [1, 5, 6].

This research will adopt the trust concept of Quinn's multi-faceted model to capture the subjective view and meaning of trust across large populations in OSN. Trust synonyms selected as the trust concept in the core of Quinn's model are honesty, faith, belief, confidence, competency, credibility, reputation, and reliability. This multi-faceted trust model was found successful for users in the application of OSNs. Chieng, *et al.* [1, 23, 24] findings show the user acceptance of this model through the usage of a prototype namely MiniOSN. However; the findings, which were based on data gathering and analysis of survey suffer from flaws due to the imbalance and undefined trust features accordingly. The core of Quinn's [12] model is honesty, faith, belief, confidence, competency, credibility, reputation and reliability. However; the representation and ranking of these features is yet to be determined. There are no indication or ranks of importance for these attributes listed in multi-faceted model. For instance, in the context of trust, the attributes of confidence should be more important than belief attributes. Non-ranking attributes are reflected in the reliability of the overall trust model.

Hence, this research includes three main objectives: i) to provide descriptive reasoning by determining the ranking of importance for each trust attribute of multi-faceted model[1] statistically; ii) to propose Enhanced Action-based Trust (EABT) algorithm and Enhanced Multi-Facet Trust with Context Recommender Mathematical Model (EMF –CRMM) as computational trust models that input the weightage obtained in objective ; and iii) to evaluate and benchmark both trust computational model techniques implicitly and intrinsically. Enhanced Action-based Trust (EABT) algorithm is the outcome of the author's Multi-faceted trust model with an existing computational algorithm [9].Enhanced Multi-Facet Trust with Context Recommender Mathematical Model (EMF –CRMM) is the outcome of hybrid between the author Multi-

facet trust model with an existing computational algorithm [17]. The contribution of this research is to provide a novel means of trust attributes ranking and two hybrid computational based trust which can be employed in the OSN.

The rest of the paper is organized as follows. Section 2 describes the related work. Next, Multi-facet ranking based on correlation is described in Section 3. Section 4 includes the proposed EABT algorithm and its user-acceptance. Section 5 discusses the proposed EMF-CRMM model and the user-acceptances on it. Finally, a section on conclusion and future work is presented.

II. Related Work

In this section, some literature on the related subject will be given.

A. Online Social Networks (OSNs)

According to Boyd and Allison [7], the key elements of any OSNs are allowing individuals to construct a public or semi-public profile within the service, to articulate a list of other users with whom they share a connection and to view and traverse their list of connections and those made by others within the service. In 1997 [8], the first OSN was SixDegrees which allowed users to create profiles, list and message their friends and traverse friends listing, thus suiting the definition of an OSN defined by Boyd and Allison. Besides messaging, SixDegrees did not provide other functionality, hence, it finally shut down in 2000 [8]. Currently, OSNs sites offer wide functionality beyond simply listing and browsing friends. Contemporary OSNs like Facebook, LinkedIn, and Twitter besides allowing users to create a network to represent their social ties, also facilitate uploading of multimedia content, various ways of communication, and allow many users to share aspects of daily life with friends. As users share these private content, they must trust the OSNs service to protect their personal information. The main target in a social network is to enjoy the benefits of social networks while mitigating the security issues. However, benefits aside, the potential privacy risks or threats to user of OSNs are often underestimated or ignored [8]. Some of these personal information would not be valuable by itself, but having a clear picture of everything about a person can give attacker ideas and information required to perform others attacks such as credit card fraud or identity theft. Although security standards and practices are an increasing subject of attention, participants still reveal great amounts of sensitive information in the Web 2.0 environment. The risks of privacy and security are the concern of a user engaged in OSNs. Hence, online social networking takes place in a context of trust as trust is a very important aspect of human life.

B. Trust Management in current OSNs

OSNs have contributed to substantially increase the interest on trust in this area. Trust has been recognized as the important factor for successful gaining user's heart to use the sites as trustworthiness in OSNs has decreased due to all the security and privacy issues noticed today in OSNs [1]. However, in OSNs, despite all measures taken for privacy and security, there is no certainty of trust in social networks. For protecting their reputation before making decisions, users can consider trust as a very significant information [9]. Trust is also of significance in attracting users to use sites receive recommendations, sort and filter information and develop a context in a community regarding whom to trust and why. In order to ensure the users and make them disclose and share their personal information in sites, a specific level of trust is required. The properties of trust can be examined below [1,12]:

- Asymmetry: As two friends have different belief and may have seen different behavior from each other, so trust is not identical.
- Transitivity: If A trusts B and B trusts G, it does not necessarily follow that A has to trust G.
- Context Dependent: Trust level towards an individual can be varied based on time, situation and experience.
- Personalized: Trust is subjective. One can have different opinions regarding the trust level towards a same person.

Currently, the features below are adopted in the trust model in social networking [1,12]:

Single-faceted:Among many trust concepts, only one of them has been used to explain and define trust and to form a single-faceted model of trust so that it can back trust based on decision making that is too general, while many other significant notions of trust have been neglected.

Not personalized: Trust in the authentic world relies on context and people are not judged by others similarly as the weight of trust traits are different too. Nevertheless, no personalized concept is prevented in the nature of the current trust model. In this concept, subjective nature and the opinions about human's trust toward people in a large population is noticed.

Trust level cannot be annotated and calculated: In the present OSNs, friendship has not been considered in an appropriate category. Therefore, it is not possible to give a good explanation about the trust level towards various people in a context. It is not possible to compute it either. Hence, the trust value on each 'friend' is being uniformity with lists or categories, while it cannot be distinguished based on the percentage of trustiness and the way the user weighted the importance of trust traits.

While reviewing trust management systems in computer science, Quinn, *et al*. [12] found that utilizing only one trust attribute in a single-faceted approach is an inadequate model of trust for use in internet environments. Current trust model "tend to use a single synonym, or definition in the use of trust can only provide a generic, non-personalised trust management solution". To address this problem of the lack of potential for personalizing trust management, a multi-faceted model of trust that is both personalisable and specialisable was proposed by Quinn, *et al.* [12] which can satisfy large and board population. In [12], myTrust Trust Management system defined trust as a concrete concept and abstract concept with the attributes of its own, where the former includes credibility,

honesty, reliability, reputation and competency attributes, and the latter includes belief, faith, and confidence attributes. Ratings are then given to each of the eight attributes, and trust is calculated as the weighted average of these ratings. In Figure 1, a number is associated with each of the eight trust concepts, these numbers are referred to as concept weights which based on the algorithm from Kleinberg's 'Hypertext Induced Topic Selection' (HITS) [13].

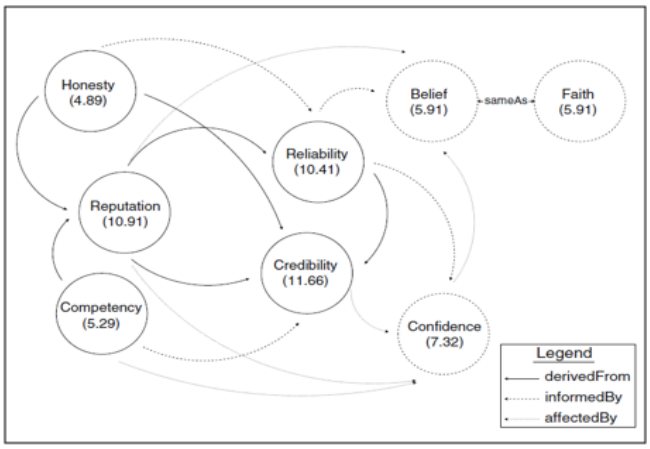

Fig. 1. Illustration of Personalized Model in myTrust [1, 12]

In addition, Quinn, *et al.* [12] work has been extended by Chieng, *et al.* [1] in which the author demonstrates the adoption of Multi-facet model for the application domain of social networks. The ties of the friendship are set according to the eight trusts attributes consist of competency, confidence, credibility, reliability, reputation, faith, honesty and belief. The range of each trust attributes is range from 1 to 10, where the greater the number indicates that the more trust is given to a specify friend. However, there is not a trust value to be computed in this model, and attributes of trust concept might cause some confusion and misunderstanding to the users, the selected of attributes of trust should be defined.

C. Privacy and Security Issues in OSNs

When users collaborate in a Web 2.0 setting, they generally share a lot of personal information which allows users to upload different types of content. A privacy breach occurs when information shared with a party for whom it was not intended, when information is abused for a different purpose than was intended, or when information is accessed after its intended lifetime [8]. One of the most common threats is identity theft or fake identity. When a user becomes the target of an attacker, the attackers are able to collect enough personal information from the person's social network profile to fake his identity or the identity of his contacts. Even a few personal details may provide attackers with enough information to guess the answer to security or password reminder questions for email, credit card, or bank accounts [14].

Unsolicited messages (Spam), cross site scripting (XSS), viruses and worms have capitalized on the exponential growth of OSNs and the free traffic they provide [15]. OSNs are also vulnerable to social engineering techniques which exploit low threshold to trusted networks and to scripting attacks which allow the automated injection of phishing links. On many OSNs, it is even possible to use scripts to invite friends. Attackers who want to have the most impact with the least effort by just creating a virus and embedding it in a website or third party application, then rely on users to share the malicious links with their contacts [16].

D. Computational Trust Models in OSNs

- Online Reputation Models

The reputation mechanism used in most online marketplaces like eBay or Amazon [5] is based on the ratings that users perform after completion of a transaction. The reputation value is computed as the sum of those ratings over the last six months for eBay. Similarly, Amazon [5] also uses a mean of all ratings to assign a reputation value. They do not provide explicit mechanisms to deal with users that provide false information. The only way to increase the reliability of the reputation value is through a tremendous number of opinions that reduce false or biased information.

- Marsh Trust Management [24]

The trust model proposed by Marsh [24] only considered direct interaction. It differentiates three types of trust which are basic trust, general trust, and situational trust.

- Basic trust. Models the general trusting disposition independently of who is the agent that is in front. It is calculated from all the experiences accumulated by the agent. Good experiences lead to a greater disposition to trust, and vice versa. The author uses the notation $Tx\ t$ to represent the trust disposition of agent x at time t.

- General trust. This is the trust that one agent has on another without taking into account any specific situation. It simply represents general trust on the other agent. It is noted as $Tx\ (y)$ representing the general trust that agent x has on agent y at time t.

- Situational trust. This is the amount of trust that one agent has in another taking into account a specific situation. The utility of the situation, its importance and the 'General trust' are the elements considered in order to calculate the 'Situational trust'. The basic formula used to calculate this type of trust is: $Tx\,(y, \propto)\ t = Ux\,(\propto)\ t\ t \times Ix\,(\propto)\ t \times Tx\,(y)\ t\hat{}$ where x is the evaluator, by the target agent and α the situation. $Ux\,(\propto)\ t$ represents the utility x gains from situation α, $Ix\ (\propto)\ t$ is the importance of the situation α for agent x and $Tx\ (y)\ t\hat{}$ is the estimate of general trust after taking into account all possible relevant data with respect to tax (y, α) in

TABLE I.

Model Name	Context dependent	Formula of model
eBay [5]	No	N/A
Marsh [24]	Yes	$T_x(y,\alpha)^t = U_x(\alpha)^t \times I_x(\alpha)^t \times \widehat{T_x(y)^t}$
Multi-context trust [11]	Yes	$T_x = \frac{S.T_s + N.T_c + F.T_F + P.T_p + G.T_G + L.T_L}{S+N+C+F+P+G+L}$
TISoN [6]	N/A	For TIM: $t_{o\to s} = s_{MTP} \times t_{a_{nMTP}\to s}$
Action-based trust[9]	N/A	Shown in Fig 3 and Fig 4.
Trust network based Context Aware recommender system[17]	Yes	$P_{c,i} = \bar{r}_c + \frac{\sum_{p\in M} sim(c,p)(r_{p,i} - \bar{r}_p)}{\sum_{p\in M} \lvert sim(c,p)\rvert}$ $T_{c(p,i)} = 1 - \frac{\lvert P_{c,i} - r_{c,i}\rvert}{Z_{MAX} - Z_{min}}$ $WT_{(c,i)} = T_{(c,i)}\left[X + Y.\frac{\sum_{q=1}^{m} W_q}{\sum_{q=1}^{r} W_q}\right]$

the past; that is, if t is the current time, x will aggregate all situations $\mathcal{T}x\,(y, \sigma)\,\mathcal{T}$, with $\theta < T < t$ and σ similar or identical to the present situation α. θ and t define the temporal window that the agent is considering. Only the experiences within that window will be taken into account for the aggregation.

- Multi-Context Trust [11]

The mathematical core of this model leans on a theory, distributed by Marsh in his founding thesis [11]. This theory introduces so-called contexts of trust which represent the fields in which the authors are capable of trusting the entity. To explain this term in a simplified example, "I trust my brother to drive me safely to the airport, but I would feel very insecure if he were to go by my plane." Dividing trust into contexts is the only reasonable way to comprise a thing as complex as trust while maintaining the possibility of flexible changes and further development. Every context is normalized into the interval from 0 to 1 to facilitate future aggregation. There are seven different trust contexts stand on functionality provided by Facebook that discussed in [11]. Among the context are i) Interaction time span (S); ii) Number of interactions (N); iii) Number of characters (C); iv) Interaction regularity (F); v) Photo tagging (P); vi) Group membership (G) and vii) Common interests (L).

These seven contexts should be aggregated in a way which allows us to establish an order relation. The equation below is introduced in this model to serve as a priority vector of number where Tx represents the priority for given context.

$$P = (TS, TN, TC, TF, TP, TG, TL)$$

The final value of trust can be calculated with this formula below:

$$Tx = \frac{S.Ts + N.TN + C.TC + F.TF + P.Tp + G.TG + L.TL}{S + N + C + F + P + G + L}$$

This method of aggregation enables us to attribute each context with its importance. If, for instance, we find a context less contributing to overall trust in our recent findings, we simply decrease the level of importance in the priority vector. Similarly, a completely new context may be added to the existing set and this expansion is also planned in the nearest future in [11].

- TISoN [6]

One of the computational trust models like Trust Inference for Social Networks (TISoN) [6] was introduced a hybrid model which implementation are based on algorithm and mathematical model. Hamdi et.al [6] introduce TISoN model to generate and evaluate trust value helps user and allow them to rate each other without any interactions. [6] designed a novel Trust Path's Searching(TPS) algorithm to discover the reliable trust path in a large social network then use trust inference measure(TIM) to decide how much the user will trust another. Table 1 demonstrates the computational trust models classification done in OSNs.

- Action-based Trust

In [9], authors proposed a new trust model based on what type of content user disclosure in OSN and what action performed by the user, examples like commenting, liking, sharing a post, and tagging on an image, posting a video and so on. An algorithm is designed to calculate trust values on the basis of the actions performed by the user which lead to users from being aware in sharing sensitive content in OSNs. If the trust value of a user is showing a constant low value over some period of time, then he is suspected to be involved in malicious activities. This algorithm would be amended to consider Quinn multi-faceted trust model in OSN in order to discover an appropriate way to compute the trust.

- Context Aware Recommender Model [17]

Based on the research in [17], Dutta et.al designed a trust based recommender systems leveraged by context attributes, recommender system aims at solving the problem of information flooding and is emerging as a widely used tool for web applications. The recommender system proposed by [17] is a trusted network based context aware recommender system, this type of recommender system takes into considerations trustworthiness of the recommending partners and context information such as time, location and company of a person along with the user and item. According to the author, the accuracy of the recommender output enhanced when the most relevant contexts are selected and their weightages are appropriately taken incorporates with aspects of dynamic trust. In this case, trust is dynamic in nature and not a static parameter. In this research; both Action-based

trust and Context-aware recommender model will be adopted and enhanced further. The fundamental of multi-facet trust model with ranked features will be embedded into the enhanced algorithm.

E. Analysis of Quantitative Variables with Correlation Analysis

Mathematically described, correlation quantifies the extent which two quantitative variables, X and Y, "go together"[19]. When high values of X are associated with high values of Y, a positive correlation exists.When high values of X are associated with low values of Y, a negative correlation exits.The resulting value called the "correlation coefficient" shows if changes in one variable or item will result in changes in the other.

When comparing the correlation between two items, one item is called the "dependent" item and the other the "independent" item. The goal is to see if a change in the independent item will result in a change in the dependent item [20]. The strength of the linear association between two numerical variables in a population is determined by the correlation coefficient, ρ, whose range is −1 to +1. A coefficient of +1.0, a "perfect positive correlation," means that changes in the independent item will result in an identical change in the dependent item. A coefficient of -1.0, a "perfect negative correlation," means that changes in the independent item will result in an identical change in the dependent item, but the change will be in the opposite direction.

A low correlation coefficient (e.g., less than ±0. 10) suggests that the relationship between two items is weak or non-existent. A high correlation coefficient (i.e., closer to plus or minus one) indicates that the dependent variable will usually change when the independent variable changes. The direction of the dependent variable's change depends on the sign of the coefficient. If the coefficient is a positive number, then the dependent variable will move in the same direction as the independent variable; if the coefficient is negative, then the dependent variable will move in the opposite direction of the independent variable [20].

III. Correlation Analysis for Trust Attributes in Multi-Faceted Model

The sample size for correlation is 83 and the data were collected based on the prototype. When participants sign up an account and login to the proposed prototype known as MiniOSN 2.0 and accept friends request, they are required to edit the friendship which is the trust level with the friends, according to that eight trust attributes, then all the data were stored within the database of the prototype [23]. The data is then extracted from the database to a mathematical tool that help to process the data and to perform the correlation analysis [23]. The result is listed below

TABLE II. Correlation Coefficient of each Trust Attribute [23]

Trust Attribute	Correlation Coefficient
Honesty	+0.76
Competency	+0.81
Confidence	+0.91
Reputation	+0.88
Faith	+0.92
Belief	+0.90
Reliability	+0.86

When comparing the correlation between attribute of trust and value of trust, a high positive coefficient (> +0.70) means a change in the trust attribute will usually predict a change in the trust value. So the higher the values of correlation coefficient, the stronger the strength association between trust value and trust attributes. In Table 2, the value of correlation coefficient of all the trust attributes together with trust value shown very high positive correlation (>0.8). Correlation coefficient for faith is the highest among other trust attributes which is 0.92, followed by confidence and belief which is 0.91 and 0.90. The different of a correlation value between reputation and credibility is merely 0.01 that is 0.88 and 0.87; followed by 0.86 and 0.81 which are reliability and competency. The lowest correlation value among these attributes are honesty which is 0.76. The value of correlation coefficient for all trust attributes with trust value is very close with each other.

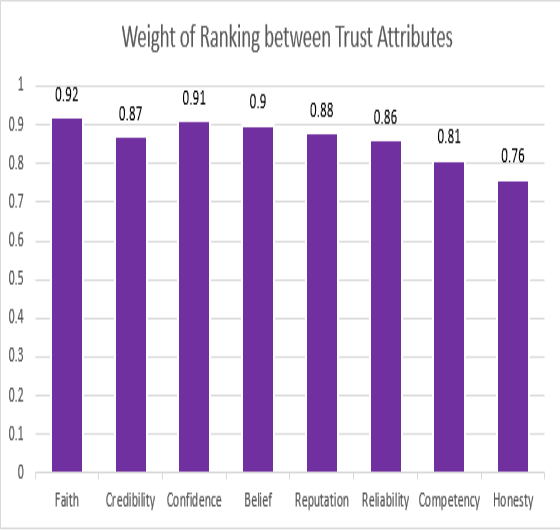

Fig. 2. Ranking of importance among all Trust Attributes

From the result in the Table 2, Chin and Mahinderjit Singh [23] conclude that faith is the most important in multi-faceted model of trust, confidence ranked second important. As seen in Figure 2, the values of coefficients for each attribute are in a symmetric pattern, the coefficient scores of each trust attributes were laid between the scale of 0.76 to 0.92 which show the scores are relatively large and strongly tight between the attributes and overall trust value. Faith is shown the highest coefficient value among all other attributes, for those who responded to this survey, higher trust rated scores were correlated with higher overall trust value scores, are = 0.92, which can be considered a large effect. Without running a test for significance, the authors are not able to infer the same correlation to the rest of the population from which our sample was drawn. From the result of this correlation coefficient, among eight of the trust attributes, faith have the most impact to the users when rating a friend, and followed arranged in an ascending order of ranking, which are confident, belief, reputation, reliability, credibility, reliability, competency and honesty respectively. As in Chieng [1] research work, trust attributes in multi-faceted model as influenced by Quinn [12] considered the wattage for each attributes is equally important in which the wattage are set as the default value. However; the findings of this research demonstrates otherwise. Different attributes have different importance, ranked and weighted.

IV. Proposed Enhanced Action-based Trust (EABT) Algorithm

Action-based Trust algorithm [9] is chosen as it calculates the trust value on the basis of the actions performed by the user which lead to users from being aware in sharing sensitive content in OSNs. Based on the proposed computational algorithm, the value of trust for a user in OSN depends on every each action that he performs for example, like a photo, share, post a status, etc., then compute the value of trust for a user, this value referred as a trust factor by authors in [9]. The trust factor of a user may increase or decrease depending on the category of content the user interacts with, which are classified as sensitive or not sensitive. Gambhir, *et al*. [9] used weight as the measurement for each of the actions the user performs in OSN. *Wa* represents weight for action, and *Wp* represents weight for post; Wc and Pc are weight for category and credibility of a post. *Wa, Wp, Wc* and *Pc* were taken into consideration as the parameters while computing the trust factor. Table 3 below illustrates the idea of using different weight that simulating the algorithm in different test case scenarios as follows:

TABLE III. Different weightage used in Action-based Trust algorithm

Weight for action, W_a		Weight for post, W_p		Weight for category, W_c	
Share	.008	**Photo**	.003	**Sensitive**	.009
Like	.006	**Video**	.002	**Non-**	.001
Comment	.007	**Link**	.001	**Sensitive**	
Dislike	.006	**Message**	.003		
Tagging	.005				
Post	.008				

Figure 3 shows the Action-based Trust algorithm of computation of trust factor. Here, *Pc* determines whether the message which is to be posted is of right commitment or not. In other words, Post Credibility is the measure of the kind of message which is to be posted. It is used in the calculation of Trust factor only when the action performed is Post (If (Type(*Wa*)==POST)). It is incremented by a factor of .001 if the message being posted is categorized in a non-sensitive category (e.g., academics, music, etc.); and gets decremented by a factor of .009 if the message is categorized in a sensitive category (alcohol, violence, etc.). The existing algorithm is extended and enhanced further by integrating multi-factor trust attributes which has been ranked according to [23].

```
Algorithm CAL_TRUST_FACTOR (username, password, action, post)
Input: username, password, action, post
Output: Trust Factor of user.
Login from openid

While (true)
  {
      Calculate Weight for Action (Wa).
      Calculate Weight for post (Wp).
      If (Type(Wa)==POST) then
   {
      Wc=0
      Call Matching_Process (Input, CAL_SEL)
      If (Flag == 0)
      Calculate Pc = Old(Pc) + .009; //Every right commitment
      Else
      Calculate Pc = Old(Pc)-.009; //Every wrong commitment
   }
      Else
      Calculate Weight for category (Wc)
      Calculate Es = Wp + Wc +Wa
      If (Type(Wa)==POST) then
      Calculate Trust factor (Tf ) = old (Tf) + Pc + Es
      Else
      Calculate Trust factor (Tf) = old (Tf) + Es
  }
```

Fig. 3. Exisiting Action-based Trust algorithm[9]

Figure 4 below shows the Enhanced Action-based Trust (EABT) Algorithm

```
Algorithm CAL_TRUST_FACTOR (username, password, action, post)
Input: username, password, action, post
Output: Trust Factor of user.
While (true)
{
      Calculate Weight for Action (Wa).
      Calculate Weight for post (Wp).
      Calculate Weight for catergory (Wc).
      // = .001 assume all is non sensitive content
      Calculate Es = Wp + Wc +Wa
      If (Type(Wa)==POST) then
      Calculate Trust factor
       (Tf ) = old (Tf) + Pc + Es //assume Pc = .001
      Else
      Calculate Trust factor (Tf) = old (Tf) + Es
}
```

Fig. 4. Enhanced Action-based Trust (EABT) Algorithm

Before computing the trust factor, the seed values of T_f has been compute with the trust rating value given by a user and the weight of trust attributes, also the value is assumed to be up to three decimals place. If seed value is assumed to be integer, the range of the trust factor will get very large which will be very difficult to analyze. Seed value of T_f is calculate as the rating value of a user towards a friend which also another user within same social network site.

$$T_f = \frac{(\text{User's Rating Value}.\sum_{i=1}^{i=8} Weight\ of\ Trust\ Traits)}{8} \quad (1)$$

After T_f is calculated, this value will become the seed value of a user's friend and it also referred as Old (T_f) in the algorithm.

A. *Proposed Trust Prototype with Enhanced Action-based Trust (EABT) Algorithm*

User will be required to register an account for the proposed Trust Prototype with Enhanced Action-based Trust (EABT) Algorithm; which is known as MiniOSN 2.1. Once the user has registered and signed in into MiniOSN 2.1, he/she requires to confirm the friend request. After friendship being confirmed, the rating value user holds for a friend would be stored into the system database, the rating value of a friend could be varied from time to time based on the subjective views of users, which the authors declared as personalize and context dependent. The higher the value represents the more the feeling of trust express from user to friend. An illustration of these actions is shown in Figures 5 and 6.

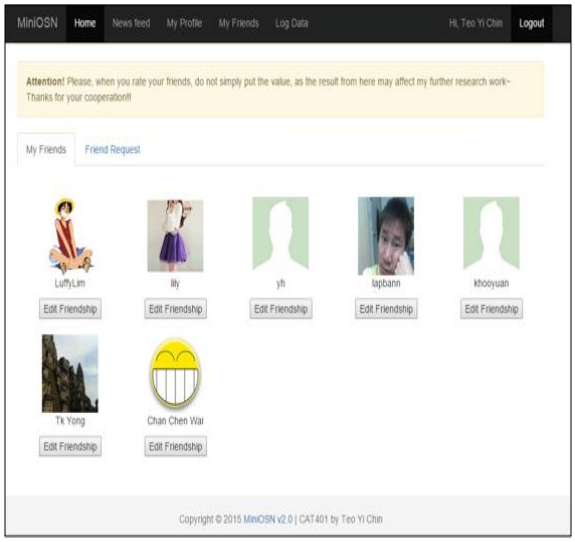

Fig. 5. MiniOSN 2.1's Friend List

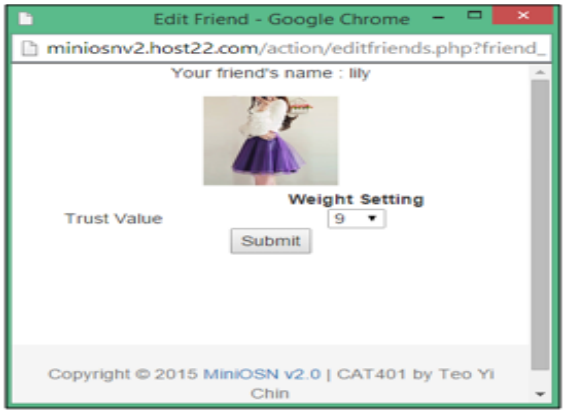

Fig. 6. MiniOSN 2.1's Edit Friendship feature

In Log Data page which is shown in Figure 7, the table displayed on the page showing the result of Trust Value, Seed Value (old (Tf)), Post Message and Post Photo for all the friends of a user, respectively. When the rating value of a friend was assigned by user, system will generate these values automatically based on the enhanced Action-based trust computation algorithm running background in the system.

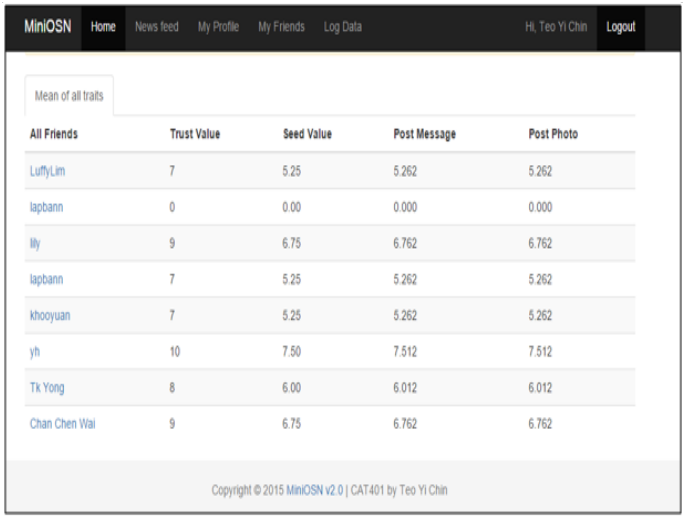

Fig. 7. MiniOSN 2.1's Log Data page

B. *User Acceptance of MiniOSN 2.1 with EABT Algorithm*

The aim of this user-acceptance survey is to evaluate user acceptance of the rating idea used within EABT algorithm. A total of 28 participants who are actively using OSN were interviewed. Most of the candidates have IT knowledge, background and fall within the age range of 20 to 24 years old.

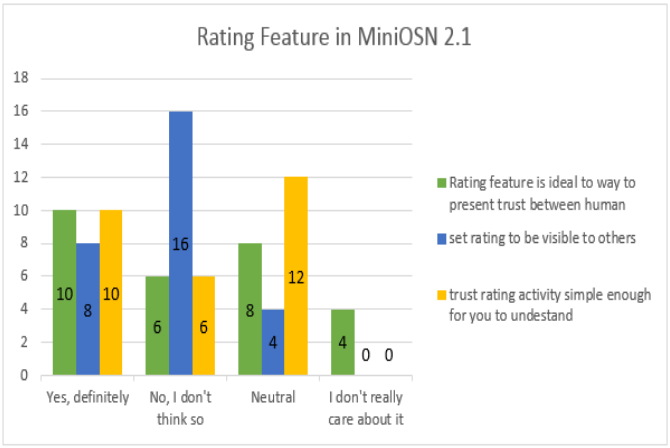

Fig. 8. Rating Features in MiniOSN 2.1

Based on the data interpreted in Figure 8, most participants stated that the rating feature in MiniOSN is an ideal way to present trust between human. On the contrary, most of the participants are unwilling to set rates to be visible to others, this might due to the human physiological factor to avoid any hard feeling or unnecessary misunderstandings to people or friend in social media. The enhanced algorithm also helps participants to learn more relate to privacy and confidential of oneself when being personal information is being exposed in social media sites. Participants hope that the rating is confidential and it only use to guess the users' behavior characteristic. Through rating, user can choose to preserve confidentiality more effectively. On the other hand, few of the participants refuse to use it, as the rating is time consuming for those who tend to have a lot of "friend" in social networking sites. Similarly, some users are not specifically familiar with the calculation of the Trust Factor (seed values, Tf). Nevertheless, the whole concept is rather basic and simple to understand for the user. It is common to be compared to other online social networks, because trust values are part of the functionality in which online social network should take into account.

V. Enhanced Trust Network based Context Recommender Mathematical Model

In order to obtain a better understanding of how Trust Network Based Context Recommender Mathematical Model [17] can be integrated in OSN as trust computational mechanism, the understanding on how recommender system works as a tool for web applications is essential.

Figure 9 describes the flow of prediction calculation of trust network-based context aware recommender system. Trust parameters and selection & weighting of relevant context are used to build a neighborhood for the target user. The task in the trust network-based context aware recommender system is to predict the ratings of a particular user which we refer to as the target user.

Rating Database: We need a database of votes or ratings from a population of users' friends. Each rating in the database corresponds to the rating from a single user on specific friend.

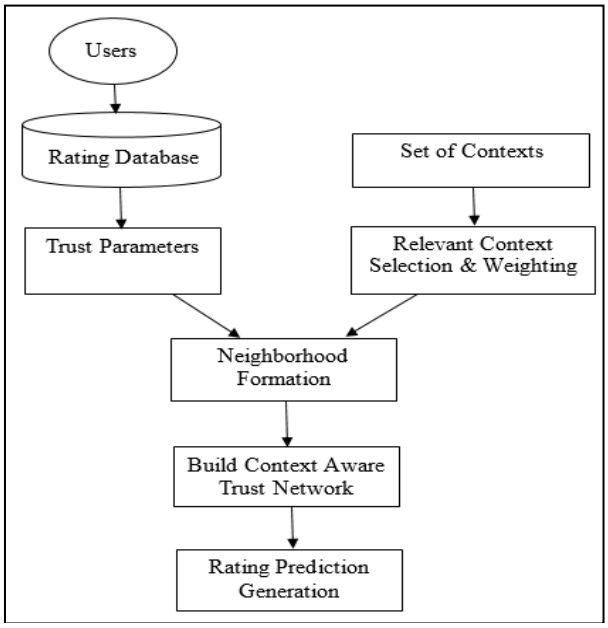

Fig. 9. Prediction calculation for Context Aware Recommender System

Trust parameters: Trust parameters are used to build a neighborhood for the target user, it is used as the input for trust calculation to generate trust values between rating values of a pair of users given towards a specific friend.

Set of contexts: Referred as trust attributes in this research, which are reputable, reliability, confidence, competency, credibility, honesty, belief and faith.

Relevant contexts selection & weighting: Eight trust attributes are selected as our relevant contexts and weights of each of eight trust attributes are used as parameters to build neighborhood for the target user as well.

Neighborhood formation: Neighborhood formed when the trust value of a friend is being calculated or updated. Trust values represent the trust that the target user holds for a specific user. The overall trust value will be updated each time the target user provides a rating to a new friend or recommended friend.

Build Context Aware Trust Network: Trust network is built when trustworthiness of each of every friend of target user is being generated, then its target users.

Rating Predication Generation: Rating prediction is being generated for a target user using the target user's neighborhood and applying the context weighted trust formula.

In [17], trust is defined as the ability of a user to provide accurate recommendations. Trust values are calculated between in pair of users and trust values are asymmetric. Dutta et.al [17] has proposed the prediction calculation for a trust network based context aware recommender system which was modified from [18] formula to generate rating prediction where user p is the sole contributor instead of all users in the neighborhood contribute to the rating prediction. $\bar{r}_c$ or $\bar{r}_p$ refers as the average friends' rating value of user c or user p.

$$P_{c,i} = \bar{r}_c + \frac{\sum_{p \in M} sim(c,p)(r_{p,i} - \bar{r}_p)}{\sum_{p \in M} |sim(c,p)|} \Rightarrow P_{c,i} = (\bar{r}_c - \bar{r}_p) + r_{p,i} \quad (2)$$

(Resnik's formula)

where

$P_{c,i}$ = *Predicted rating for target user c on a specific item i,*

$\bar{r}_c$ = *Average rating of user c,*

$\bar{r}_p$ = *Average rating of user p,*

$r_{p,i}$ = *Rating of user gave to friend, i.*

$T_{c(p,i)}$ represent the friend-level trust value,where p is the user who provided the rating prediction on friend I, and c is the target user. Target user, c refers to the user profile receiving the friend recommendarion, and user *p* refers to the profile that has been selected as a recommendation partner for user c. In multi-facet environment which uses the range of 1 to 10 rating scale, Z_{max} would be 10 and Z_{min} would be 1. The result for friend-level of trust range from [1,0], where a larger value means the prediction was more accurate.

$$T_{c(p,i)} = 1 - \frac{|P_{c,i} - r_{c,i}|}{Z_{MAX} - Z_{min}} \quad (3)$$

where

$T_{c(p,i)}$ = *Trust of target user c for p for a specific friend i,*

$r_{c,i}$ = *Target user's actual rating on friend i,*

Z_{max} = *Top of rating scale,*

Z_{min} = *Bottom of the rating scale.*

The trust value which a target user holds for all other users will vary time; this represents the personalized trust. Because the dynamic of trust needs to be infused in the recommender system to enhance the accuracy, incorporation of relevant context parameters in the trust network will be resolved this issue. In order to take context weightings (important factors) into consideration, for equation in (3) is modified again to $WT_{c,i}$ as shown in (4) below.

$$\mathbf{WT_{(c,i)}} = T_{(c,i)} \left[X + Y . \frac{\sum_{q=1}^{m} w_q}{\sum_{q=1}^{r} w_q} \right] \quad (4)$$

where

$WT_{c,i}$ = *context weighted trust value.*

X,Y = Two real number such that X+Y = 1,

m = number of matching contexts,

r= number of relevant contexts selected, $r \geq m$.

Equation in (4) takes into consideration, the effect of relevant contexts on the trust value and derive the context weighted trust value. In this research, the weightage of trust attributes will be inhabit into the equation in (4). *r* is the number of relevant contexts selected, *r* is equal to 8 because we are using all eight weighted trust attributes to calculate trustworthiness of a user. In this approach, both user rating and user's friend rating will be considered as the parameter to compute the trust value. *m* refers to the matching contexts between target user *c* and user *p* given the rating value towards eight trust attributes in the prototype. *X* and *Y* are the real number such that *X* + *Y* is equal to one, different combination value of *X* and *Y* will produce varies weighted trust score. In our case, the value of *X* and *Y* would be 0.5, based on the experiment carried out by the authors in [17], MAE of each of different set of *X* and *Y* were captured to measure the accuracy of prediction. MAE known as Mean Absolute Error to measure the average absolute deviation between predicted ratings and users true ratings. If MAE is small, it indicates high prediction accuracy. A combination of value of 0.5 for both *X* and *Y* generate the smallest score of MAE among all different combinations.

A. *Proposed Trust Prototype with Enhanced Multi-Facet Trust with Context Recommender Mathematical Model [EMF –CRMM]*

With influences from multi-faceted trust model and ranked weights trust attributes in the author first findings, MiniOSN2.2 is proposed with trust computation mechanism different from miniOSN 2.1. Rating feature will be demonstrated in MiniOSN 2.2 as well, rating activities are part of the process of trust computation, in MiniOSN 2.2 trust rating of another user takes into consideration as one of the important factors to calculate trust. User needs to enter the rating value of each trust attributes. Rating value range from 1 to 10, when trust value is being calculated, the system will look up for a matching rating value of these trust attributes between the user and recommender partner.

B. *User Acceptance of MiniOSN 2.2 with EMF –CRMM*

The aim of this user-acceptance task is to evaluate user acceptance in term of the applicability of trust network based context recommender mechanism is applicable in OSN. All participants who are active in OSN and with some knowledge of practice of online social network are chosen.

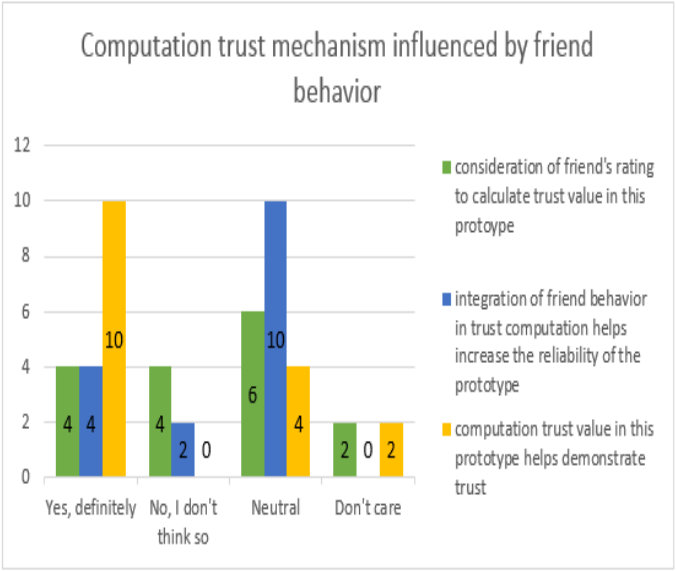

Fig. 10. Computation trust mechanism influenced by friend's behavior

In MiniOSN 2.2, trust rating value of a friend is taken into account for trust value calculation (see Figure 10). In this research, implementation of trust computation mechanism

with trust network-based context recommender model in MiniOSN 2.2 aims to help users to express trust, 62.5% of participants' respondents the prototype successfully demonstrated the trust. Generally, participants described the ideal experience from this prototype are showing a good response. Despite the issues in the design of the user interface and the ambiguity of navigation in the prototype, enable trust rating from a recommender partner to a friend in this prototype which is said to be able to increase the trust and privacy awareness among social users in this survey finding. There are mixed opinions provided by participants when the question asked participants to compare the social network of incorporating rating and trust computational mechanism with other online social networks. Some of the participants responded that this is the first time experience obtained from a participant have this rating feature with computational trust system and is not familiar for them to be seen on other social network sites. While some participants responded it was good to bounce ideas off other social networks, which acts like feedback from customer on shopping sites like Lazada.

C. Comparison between MiniOSN 2.1 & MiniOSN 2.0

From the evaluation results, the authors found that most people felt that the trust computation mechanism of recommender model would be more transparent compare to action-based trust model. The result showed that most people are keen to express subjective views of trust depending on the context among connected friends in OSN. Also the result showed most people felt that both mechanisms help them to gain a better control over the resources in an online profile. However, some enhancement and modification should be done, especially on the structure and design of both prototypes.

Overall, EABT algorithm has better reviews in term of user-friendly in system, this is due to the workload of rating friends is much easier and convenient. In MiniOSN 2.2, users need to go through additional process or step while rating friends, there is users need to send a request to a recommender friend providing he/she own rating based upon confirmation of friend request. This makes the rating process in OSN take a longer time, which means lack of user friendliness thereby reducing the effectiveness of the computation of the system if there is any delay in responding for providing rating value from a recommender friend. Another downfall in recommender model is the need for human contact or support in providing feedback rating continuously from time to time for the user would make the system look clumsy. An efficient system should prevent or reduce occurrence of human intervention. In order to provide a reliable trust rating and a computational mechanism within OSN, user needs to understand each setting correctly. There should still be standard to follow by the user to avoid any argument when rating a friend. Based on the comparison and evaluation of both models, the authors demonstrate that EABT algorithm takes a preemptive than the recommender model in term of efficiency. In conclusion, from all the results of these surveys, trust needs to be taken into account in OSN. As most of the active OSN users believe that OSN should provide a better control on user own resources or profiles that are personalize-able by integrating element of trust. Implementation the concept of trust and computational mechanism in OSN is expected by most of the users. Trustworthiness of OSN needs to be guaranteed in order to protect user privacy and to win the user's heart.

VI. CONCLUSION& FUTURE WORKS

The current OSN is suffering the lack of trust or confidence in the opinion expressed in the web-based social network where the degree of trust among the users is absent. Current trust mechanisms used in OSNs are limited to simple privacy settings where users can control who can view their profile and interact with them or can include them in some community. Trust propagation does not manifest itself as a physical phenomenon in nature, but only exists at the mental and cognitive level. It is therefore difficult to assess whether computational models for trust propagation are adequate and reflect the way people reason about trust. Throughout the study, the author discussed that how the multi-faceted model of trust based on eight trusts attributes that implemented into OSN, where the trust concerns are taken based on the eight important traits: honesty, reputation, competency, credibility, confidence, reliability, belief and faith [1, 12]. The author next we set the weightage and by using statistical means, ranking of each attribute is determined [23].

Secondly, the input of [23] is then applied together into the proposed EABT algorithm and EMF–CRMM model. The simulation of prototype of these two models has been developed to use it as the mean to collect the data joint with the web-based questionnaire for this evaluation. Rating feature is demonstrated in both proposed computational trust models in the social network for most of our evaluation participants felt that it helps users to obtain a better control over their online resources in a profile which enable them to express their trust depend of the context and personally in OSN. Evaluation regarding the functionalities and acceptance of MiniOSN 2.1 and MiniOSN 2.2 are examined based on user opinions and overall satisfaction towards the developed prototype seems through second survey and third survey which targeting only active OSN users. Overall the proposed conceptual framework received positive reviews from participants, however opinion seems still to waver if it is integrated into current OSN. People tend not to judge people by those values generated by a machine rather they judge from the abstract aspect, such as sensitivity or feeling they felt for others. The authors suspect that such a proposed model would work well in an e-market environment, where users do not have previous relationships offline and are building trust for each other from scratch.

However, there is also no standard tool or method to measure the accuracy of trust value being generated by computational trust mechanism that integrated in OSN. Despite all the privacy and security issues in OSN, trust must be enforced to increase the trustworthiness of a social network site in order draws back the heart of the user to use it. Where there is the high levels of trust, people are more willing to provide support and take risk in information exchanges. In future, more research focusing into computational trust for inputting feedback ratings in OSN must be done. As for future work, trust calculation algorithm or mathematical model that is resistant to attacks such as Sybil attack, and is applicable to the Quinn's multi-faceted model [12] of trust in this research could be implemented and evaluated.

Such an algorithm should highlight because it could enhance the trust management service in OSN by providing accurate recommendations. Another focus would be to study the effect of distrust in the multi-facet model.

REFERENCES

[1] Liu Ban Chieng , Manmeet Mahinderjit Singh , Zarul Fitri Zaaba, Rohail Hassan, *Multi- Facet Trust Model For Online Social Network Environment*, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1, January 2015

[2] Gross.R, Acquisti.A, *"Information Revelation and Privacy in Online Social Networks(The Facebook case)",* WPES '05 Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71 – 80, doi:10.1145/1102199.1102214

[3] Johnson.H et.al, *"On the Concept of Trust in Online Social Networks",* Trustworthy Internet, Springer Milan PP. 143-157, [online] http://link.springer.com/chapter/10.1007/978-88- 470-1818-1_11#.

[4] Ruohomaa.S et.al (2005). *Trust Management Survey*. *Lecture Notes in Computer Science.* Springer Berlin Heidelberg.Vol. 3477, pp 77-92 [online] http://link.springer.com/chapter/10.1007%2F11429760_6#

[5] Sabater.J, Sierra.C; "*Review on computational trust and reputation models*"; IIIA-CSIC, Campus UAB, Bellaterra, Barceloana, Spain; September 18, 2003.

[6] Hamdi.S,Bouzeghoub.A, Lopes Gancarski.A, Ben Yahia.S, "*Trust Inference Computation for Online Social Networks*", TRUSTCOM, 2013, 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013

[7] Boyd, D.M., Ellison, N.B.: *Social network sites: definition, history and scholarship*. J. Comput. Mediat. Commun. 13(1), 210–230 (2007).

[8] Beye, M., Jeckmans, A. J., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). *Privacy in Online Social Networks.* In Computational Social Networks (pp. 87-113). Springer London.

[9] Gambier, M. N Doja, and Moinuddin, "*Action-based trust computation algorithm for Online Social Network*", Proc. of 2014 Fourth International Conference on Advanced Computing & Communication Technologies, Rohtak. N.p., 8-9 Feb. 2014.

[10] Lu.G et.al (2009). "*A Review on Computational Trust Models for Multi-Agent Systems".* The Open International Science Journal, 2009, 2, Pages 18-25.

[11] Savec.T, Samek.J (2013). "*Trust evaluation on Facebook using multiple contexts*". *DECEUR Workshop Proceedings.* 2013, vol. 2013, no. 997, pp. 23-32. ISSN 1613-0073. Available from: http://www.ceur-ws.org/Vol-997/trum2013_proceedings.pdf

[12] Quinn.K et.al. (2009). "*An analysis of accuracy experiments carried out over of a multi- faceted model of trust"*. International Journal of Information Security. Springer-Verlag. Vol. 8, Issues 2, pp 103-119 [online] http://link.springer.com/article/10.1007%2Fs10207-008-0069-7

[13] Kleinberg, J.: "*Authoritative sources in aHyperlinked Environment*." In: Proceedings of the 9th ACM-SIAM Symposium on Discrete Algorithms (1998).

[14] Salama, M., et al., "*Computational Social Networks: Security and Privacy, in Computational Social Networks"*. 2012, Springer. p. 3-21.

[15] Karuppanan, K. (2012). *"Security, Privacy, and Trust in Social Networks. In Computational Social Networks (pp. 23-53)".* Springer London.

[16] McDowell, M., Morda, D.: *"Socializing securely: using social networking services".* United States Computer Emergency Readiness Team (US-CERT), Washington, DC (2011)

[17] PallaDutta et.al; *"A Novel Approach to Trust Based Recommender Systems Leveraged by Context Attributes"*. International Journal of Engineering and Technology(IJET). Vol 6 No 3 Jun-Jul 2014, pp 1480-1486.

[18] Kristen Mori. *"Trust Networks in Recommender Systems".* 2008. Masters Project, San Jose State University.

[19] Gerstman B. (Sep 2004). Online lecturer note of San Jose State University: Chapter 14 Correlation. Retrieved http://www.sjsu.edu/faculty/gerstman/StatPrimer/correlation.pdf

[20] Steven B. Achelis. Technical Analysis from A to Z. Retrieved From: http://www.metastock.com/customer/resources/taaz/?c=3&p=44

[21] Raj Gunesh. Online lecturer note: Statistic Correlation Analysis. Retrieve From: http://pages.intnet.mu/cueboy/education/notes/statistics/pearsoncorrel.pdf

[22] Mahinderjit Singh.M, Liu.B.C, Hassan.R , Zaaba.Z.F, "*Friends Personalization of Trustworthiness forPrivacy Perseverance in Social Networking",* Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I WCECS 2015, October 21-23, 2015, San Francisco, USA.

[23] Chin Teo Yi, Manmeet Mahinderjit Singh , "*Multi-Facet Trust Factors Ranking With Correlation Analysis Technique: A Case Study on Online Social Network (OSN)* ", 26th International-Business-Information-Management-Association, Madrid, Spain Nov11-12, 2015 VOLS I - VI, 2015 pp: 1812-1822

[24] Stephen, M. (1994). Formalising trust as a computational concept. Ph. D dissertation. University of Stirling, scotland.