

# MULTI-FACET TRUST MODEL FOR ONLINE SOCIAL NETWORK ENVIRONMENT

Liu Ban Chieng<sup>1</sup>, Manmeet Mahinderjit Singh<sup>1</sup>, Zarul Fitri Zaaba<sup>1</sup>, Rohail Hassan<sup>2</sup>

<sup>1</sup>School of Computer Sciences, University Sains Malaysia, 11800 Penang

<sup>2</sup> Universiti Teknologi Petronas, Tronoh, 31750, Malaysia.

## ABSTRACT

*Online Social Network (OSN) has become the most popular platform on the Internet that can provide an interesting and creative ways to communicate, sharing and meets with peoples. As OSNs mature, issues regarding proper use of OSNs are also growing. In this research, the challenges of online social networks have been investigated. The current issues in some of the Social Network Sites are being studied and compared. Cyber criminals, malware attacks, physical threat, security and usability and some privacy issues have been recognized as the challenges of the current social networking sites. Trust concerns have been raised and the trustworthiness of social networking sites has been questioned. Currently, the trust in social networks is using the single- faceted approach, which is not well personalized, and doesn't account for the subjective views of trust, according to each user, but only the general trust believes of a group of population. The trust level towards a person cannot be calculated and trust is lack of personalization. From our initial survey, we had found that most people can share their information without any doubts on OSN but they normally do not trust all their friends equally and think there is a need of trust management. We had found mixed opinions in relation to the proposed rating feature in OSNs too. By adopting the idea of multi-faceted trust model, a user-centric model that can personalize the comments/photos in social network with user's customized traits of trust is proposed. This model can probably solve many of the trust issues towards the social networking sites with personalized trust features, in order to keep the postings on social sites confidential and integrity.*

## KEYWORDS

*Online Social Network, Trust, Multi-Faceted Model, Trust Management, Usable Security.*

## 1. INTRODUCTION

Online Social Network (OSN) can be defined as a free online platform, with high availability that serve as a digital representation of the users stay connected in the virtual environment that provide data sharing, semi- public profile creation, and messaging services [1,2,3,4] Online Social Network (OSN) such as Facebook, Twitter and Myspace have experienced a bullet's speedy growth in recent years. Despite the social hierarchy, almost everyone, with an online device, will have at least one account in any of the social network sites. A survey done by [1] has demonstrated that the users of social networking site from 2005 - 2012, consist of people from different age group, ranging from 18 to 65 and above. The number of OSNs users has increased in all age groups over the years. The main problem in the current OSN is the generalization of trust in OSN. Friends in a group are assumed to be trusted equally. Take for example, on Facebook and Twitter; they have grouped all friends under one level of the

category in which they tend to trust them all the same. Although they can group friends into “Close Friends” and “Family” like in Facebook, the categorization is still in a big group but not personalized and specific. However, in real-life, it is impossible to do so as trustworthiness is context dependent and need to be personalized [5, 6]. Some friends are likely to be more trustworthy compared to the rest. For example, Alice wants to share a private message in the Facebook only with certain friend in the ‘Close Friends’ group. However, trust level can be varied according to the times, experiences and individual. Moreover, the person you trust before not necessary to be trusted by you in your entire life. As an account owner, have no right calculate your trust level too and the trust level is assumed to be general for all. This research aims to answer the questions of whether a multi-faceted model of trust that is personalisable and specialisable be welcomed in OSNs, would an application of the model satisfy user needs when expressing their subjective views on trust in the OSN environment, and would the proposed solution address issues we found in the literature review. The main aim of this research paper is to tackle the lack of personalization in term of trustworthiness in the current OSN. The objectives of this research paper are stated as below:

1. To study the security, privacy and trust issues in current social network and explore various trust traits and users requirement that is essential to the users.
2. To demonstrate a taxonomy of security and privacy attacks occurring on various type of online social network.
3. To present the outcome of the questionnaires and to solve the issue of single level trust adopted in the current social network by introducing a miniOSN which adopts multi-facet trust approach.

This paper is organized as follows; Section Two introduces the concept of OSN, the categorizations as well as a brief history of them. It provides an analysis of the state of the art in trust and its characteristics, and current trust mechanisms used in notable online social networks. Section Three present the gap of the existing online social networks. This chapter also discusses about the trust identification in current OSN. Section Four concentrates on a survey designed to gather user opinions of current trust management approaches being used, and presents our findings as well as analysis of the results and future works. And finally, we come out with a conclusion, discussing the extent to which the original objectives and goals were achieved during this research project.

## **2. BACKGROUND**

In this section, we will present the related section regarding our study such as social network and the trust mechanism in current social network.

### **2.1. Social Network (OSN)**

Online Social Network not only serves as a communication tool but also act as an application source and online community builders [1, 2 3]. Face to face interaction is eliminated in OSNs [4, 7]. It was the most popular internet sites mushrooming in the past few years and today having billions of users with a wide demographic range. Nowadays, the users of OSNs are spread over all age groups despite their backgrounds. The first recognizable OSN is the SixDegrees.com with the initial purpose creates profiles and listing friends in 1997. OSN experienced various evolutions from 1997 till now, with the addition of function, improvement of the interface and the availability of OSN simultaneously with the increment of the popularity of OSNs [8].

## 2.2. Trust Mechanism in Current OSN

Network in OSNs has become more and more diversify since social sites bring together people, often from different type of social ties; consisting of thick bonding and weak bonding [4]. Hence, forming a different level of trust among “friends” in the social networking sites. “Thick trust” is formed among those sharing common interests in offline interaction while “thin trust” is formed across strangers. He claimed that mixing of social circles in OSN could gradually lead to social distrust [4]. Hence, privacy management should be examined together with the trust model in OSNs. OSNs have been believed to generate many security and privacy issues, and thus, trustworthiness in social networks has been doubted after all. However, trust is an important concept in obtaining the user’s heart to use the sites. This is because, a certain level of trust is needed in order to make the user willing to use the sites and share their private data on the sites. The characteristic of trust can be concluded as [1].

- i) Trust is asymmetric: Trust is not identical; A might trust B fully but A doesn’t necessary to trust with the in the same way.
- ii) Trust is transitive: A and B trusts each other well and B has a common friend C, that A might not know where A might trust C because of B. However, A might not trust D, a friend of C since their network linkage is getting far.
- iii) Trust is context dependent: In other words, trust level towards an individual can be varied based on time, situation and experience. Depends on the context, people tend to trust each other differently.
- iv) Trust is personalized: Which means trust is subjective. Two persons can have different opinions regarding the trust level towards a same person.

Currently, the trust model in social networking adopts the following characteristic:

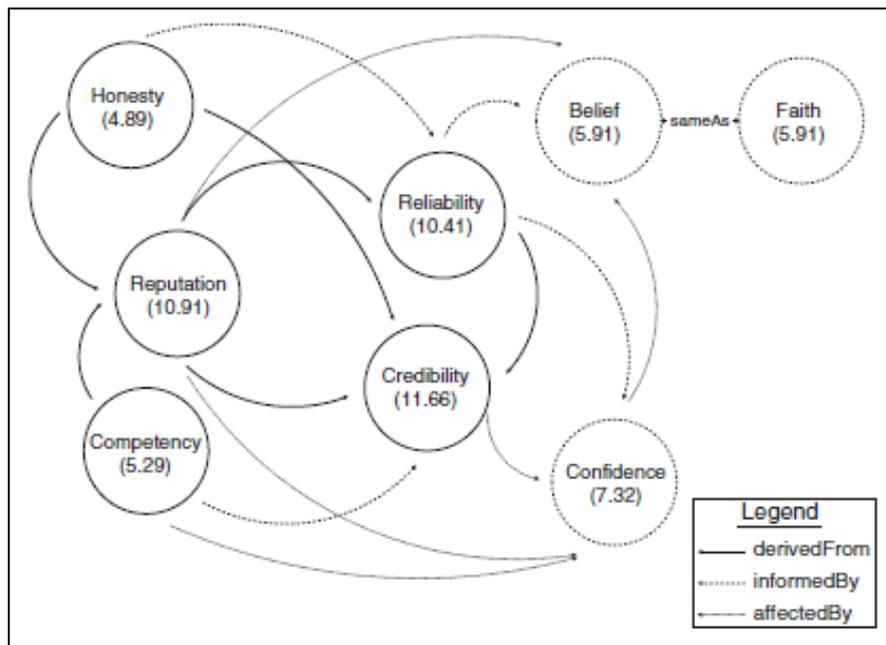
- a) Single- faceted: The current trust model focus only on one trust characteristic, which is an inadequate model of trust since the Internet environment is so broad and the population of users is wide. It is too general in term of trust beliefs and it has ignored a lot of other important trust concepts such as reputation in their model [5, 6]. Dishonesty can happen [5]. However, trust concepts are very useful in considering the relationship between peoples and it should not be unitary but diverse [7].
- b) Not personalized: Trust model should be personalized and conjunction with the domain specific model [5, 6]. However, current trust model itself does not inhibit a personalized concept, which take-in consideration of the subjective nature and the views of human’s trust towards peoples across a large population [6]. In the real world, trust is context dependent and peoples tend to judge people differently with different weight of trust traits. However, current social networking sites cannot specify the trust level based on the user’s customized trust traits on specific individuals.
- c) Trust level cannot be annotated or calculated [6]: Friendship is not well- categorized in the current social networking sites [1]. Hence, the trust level towards different individual cannot be explained in context and yet cannot be calculated accordingly [6]. Thus, the trust value on each “friend” is being uniformity with lists or category, but not differentiated according to percentage of trustiness and how the user weighted the importance of trust traits.

## 2.3 Related Work on Trust Management

The Trust Management Model [5] such as the Marsh’s trust model is one of the pioneers to introduce computational concepts of trust and has represented trust in scalar form while SECURE makes it in a range from including the measure of uncertainty. There are also some

simple trust calculation in some of the online community like eBay and Amazon, to enable the members to understand the statements and guide them for purchasing and moreover send feedbacks. However, it is based on single-faceted approach and dishonesty can still happen as mostly they will tend to avoid negative comment [5, 6]. Many other trust management systems such as REFEREE, SULTAN, Advogato and Film Trust applied the single- faceted approach, which means they do not inhibit the subjective nature of trust in their users [6].

However, my Trust, Trust Management Service (as shown in Figure 1) has been using a personalized model in conjunction with a specific domain model to provide the user a personalized- trust based services. myTrust has adopted an internal trust multi-faceted management system, TRELIS, with the trust calculation mechanism based on rating. myTrust has been designed to enable users to annotate trust in term of the traits of trust, share the trust information and the calculate trust. The model is modelled through 4 unique models: Upper Ontology provides generic traits of trust, Meta model, Domain Specific model and personalized model [6].The multi-faceted idea has utilized the subjectivity of trust nature and view found among the large population. The trust concept such as: honesty, reputation, competency, credibility, confidence, reliability, belief and faith are recognized as the core of this multi-faceted model. Besides that, multi-faceted model is able to support personalization and is context dependent. The multi-faceted of trust and the relationship between the trusts concepts are utilized to reflect the subjectivity of human being into the model [6].



**Figure 1:** Illustration of Personalised Model in myTrust [6]

Moreover, a multi-faceted management interface that is applicable to both operational and contractual operations [9]. The heterogeneous web services with different levels of capabilities and characteristics can be managed with this multi-faceted interface. There are basically three facets of web services: No management, operational management and contract management. The web services might exist in different domain with different controllers too makes it harder to be manageable. Standard exists for operational management. However, ROAD framework is used to implement the management interface for self-managed mechanism.

Since we have noticed that there are a lack of flexible and personalised trust management features within current OSNs and we believe that such features are important to protect the privacy of users, so we decided to explore whether the multi-faceted model of trust proposed by [6] that enables personalization and the flexibility of annotating trust subjectively would be utilized in OSNs. We also interested to know the desired functionalities of the trust management model to be implemented into OSNs. Based on the research questions, we developed an online questionnaire protocol that included 12 closed-ended questions on four topics: (a) general usage patterns related to content sharing, (b) experiences regarding privacy that are related to content sharing, (c) how and with whom the people share content, and (d) the perceptions of social trust and the desired trust traits requirement.

## **2.4 A Review on Usable Security in OSN**

In view of an increasing threat landscape, today's users face an increasing requirement to use applications, security tools and interact with related system functionality. However, a significant challenge in many cases is posed by the usability of the technologies, with the consequence that users can face difficulties in understanding them correctly and utilizing them effectively. Therefore, Online Social Network (OSN) also facing the similar challenges. Security and usability (Usable Security) are two different domains which become the concern in viewing the OSN. In order to design usable technologies, it must be designed with a secure applications and interface so that end-users would be able to comprehend the functions provides for them [10]. Nowadays, most researchers have started to focus on this issue and also the privacy and identity albeit users do not want to reveal the information as they wanted [11]. Most of the OSN products provides with security settings which offer from basic to advanced security protection for their end-users. However, most of the end-users would apprehend the default settings which had been provided once they installed the application in their computer rather than having some tweak on the settings for better protection. The main question that can be highlighted here is why the end-users would do that. There are some concerns on how current security settings have been implemented on each application or products which make it cumbersome to be used. By relying upon the default setting is not an adequate solution given the facts that single default level of security unable to serve to all level of users. The developers should not put the end-users in baffle situation where they need to deal with it without a proper guide. In this context, the presentation and usability plays an important role to ensure that end-users able to understand how to manage their security functionality.

Usability can be viewed as a quality attribute that evaluates how user interface is being used [12]. Thus, in order to deliver the information and meet the purpose of one particular system, the end-results of application must be user-friendly and be presented with a correct Human Computer Interaction (HCI) aspects. Many HCI guidelines have been implemented to guide the developers to provide a meaningful manner and understanding system functionality (i.e. interface, security features, etc) [13, 14, 15, 16]. At present, there are not very much focus has been given to improve the usable security of Online Social Network (OSN). As the social networking quickly become popular means of communication, there are corresponding needs to ensure that end-user would be competent and easy to interact and to use the application. However, for this current work, the authors make an early observation to compare six types of Online Social Network (OSN) in respective of usability as a template filled with useful template data in a general sense as shown in Table 1. It is expected that the developers able to re-asses this template to fill in with more detail and concrete data via fully implementation of usability evaluation methods which also become our future works.

Table 1. General analysis of popular Social Network based on usability criteria.

| <b>OSN Types</b>  | <b>Effectiveness</b>  | <b>Efficiency through Guiding Interface</b>  | <b>User Satisfaction</b>   |
|-------------------|---|--|--|
| <b>Facebook</b>   | High if the user takes some time to learn (i.e. technical explanation and terminology in two separate tabs) | Guiding user through question and answers with detail explanation which includes different signal cues | Easy for advanced users as it involved some technical terminology. Novice users might face some difficulties to understand (Depend on the usefulness and clarity of questions) |
| <b>Twitter</b>    | Medium (i.e. simple explanation in combination security & privacy tab)                                      | Guiding user through useful tabs with basic explanation  | Simple and easy to understand as the security features is basic (Limited choices)  |
| <b>YouTube</b>    | Medium (i.e. simple explanation in privacy tab)   | Guiding user through simple tabs with limited explanation  | Limited information and explanation. However it is easy for all level of users.(Limited choices)   |
| <b>Google+</b>    | High if the user takes some time to learn (i.e. technical explanation and terminology in Privacy tab)       | Guiding user through long list of information.   | Long list of information provided. More suitable for advanced user rather than novice (Learnability will take some time)   |
| <b>Pixnet.net</b> | Medium (i.e. basic explanation in settings)   | Guiding user through useful tabs and help queries function.  | Easy for advanced users as it involved some technical terminology. Novice users might face some difficulties to understand (Depend on the usefulness and clarity of questions) |
| <b>Myspace</b>    | Medium (i.e. simple explanation in privacy tab)   | Guiding user through useful tabs with limited explanation  | The security tab listed in a small font at the bottom with a very limited information and explanation (Problem with visibility)  |

This study using a similar approach to compare user help techniques based on usability as a new platform by providing some general ideas on the evaluation of each technique [17]. All of these will be evaluated using Usability evaluation Methods (UEM) via inspection, user testing or inquiry. However, with this particular study, the authors made an early observation and general comparison rather than evaluate it in further details. It is expected that the software designer will be able to know elements that can be enhanced or formulated to make their application works better. Usability includes three main attributes such as effectiveness, efficiency and user satisfaction [18]. Effectiveness was measured by looking at whether user able to understand the usage of security settings provided in timely manner. Efficiency focused on whether user able

to complete the tasks after learning how to use one particular application while user satisfaction focused on whether the application that user used is pleasant to gain full satisfaction.

#### **4. A GAP STUDY OF SECURITY & PRIVACY ON CURRENT OSN**

A few Social Networks are studied carefully and the gap of current trust social networks is investigated. The comparison among the Social Networks in terms security and privacy aspects have been studied and compared and the result is tabulated in *Table 2*. It shows that in all of the social networking sites, the profile settings by default are public to all and it has to be manually set by the user. This can lead to a confidential problem where the private data can be leaked unintentional. Since an email address is used to identify the user's identity in the virtual world, multiple identities are always inevitable. This can indirectly affect the Integrity and Identification. In Pixnet.net, strangers are allowed to be the readers of the bloggers; while in YouTube, even strangers can subscribe to ones channels and be updated with his shared videos. All these can affect data integrity too. Moreover, Facebook and Twitter has affected the data privacy because of the photo tagging features.

Online devices such as Smartphones, Tablets and Desktop have provided high availability of the Social Network sites. People can be easily stay connected to their OSN accounts. Meta tags in Pixnet.net have made user's blog post to be easily searchable by the public and highly available to others [25]. The official account in Facebook and Twitter can affect accountability since the person who share/ post something through the account are not known [21, 22]. Besides that, friendship on Facebook and Twitter are not well differentiated, but in a general list [21, 22], while on YouTube, subscribers can be strangers that one never knows [26], and on Pixnet.net, visitors can appear as anonymous, again, affecting accountability.

Next, Facebook, Google +, Myspace and Twitter has inhibit location based features affecting data privacy. Twitter and Google + can affect the data privacy with the Harsh Tag features [23, 24] and YouTube affect data privacy with the freely downloadable and sharing video features [26]. Pixnet. Net can harm data privacy through Meta tags as the tags helped to promote their blog entries to the public with common tags [25]. Besides that, one's online status can be easily shown even he "Appear to be Offline", because of the "Seen" features, affecting user privacy. Facebook, Twitter, YouTube, Google Plus, Pixnet. net and Myspace reveals user's data such as current profile picture, cover photo and account name to the public by default, affecting both user privacy and data privacy.

#### **5. SURVEY FINDINGS**

To gain insight into different practices regarding trust in Online Social Network, the questionnaire groups participants into three categories as follows, people who are currently using OSNs, people who have used OSNs before but are no longer active, and people who have never signed up in any OSNs. In total, 213 people took part in answering the questionnaire. However, only about 200 samples are taken due to the validity and completeness of the survey result return from each participant. Among which, 117 were female, 83 were male. Mostly from age ranges from 23 to 25. Among all the 200 participants that contributed in this survey, there are 179 active OSN users, 12 people that are no longer active in OSNs and 9 people who never or will not sign up in any online social networks. Among the 179 respondents who are currently using OSNs, the majority of the profiles are set to be viewable by the friends that are directly linked through the users' networks. This indicated that the OSNs users are more comfortable to share their data to people that they know than exposed everything to the public. We then asked

the question of whether these users are happy with the available ways of controlling access to their profiles.

Table 2: Security and Privacy concern in some popular Social Network

|                   |   |  |                 |  |  |  |                 |   |                       |
|-------------------|---|--|-----------------|--|--|--|-----------------|---|-----------------------|
| <b>Google+</b>    | - Manual Profile Setting [Google, 2013]<br>- Publicly available info is searchable in Google. [Google, 2013]<br>- Circle's name is private behind scene. [Google, 2013] | - Multiple identities<br>- Ease of adding people into circle.<br>- Share things within circles or to certain peoples | - Similar to FB | - Similar to Twitter   | - Password Authentication<br>- Email notification.<br>- Text message. [Google, 2013] | - Timeline features.<br>- Last sign-in time.<br>- Identity of person who "+1" or share post.<br>- Details about person in circles behind the scene. [Google, 2013]                   | - Similar to FB | - Google photos reside in a Picasa account.<br>- Harsh tag features.<br>- Location-based like in twitter.<br>- Restrict downloading of photos from setting.   | - Similar to Twitter  |
| <b>Pixnet.net</b> | - Manual Profile settings [Pixnet.net, 2013]<br>- Stranger as readers.<br>- Restrict viewing by setting. [Pixnet.net, 2013]<br>- Meta tags. [Pixnet.net, 2013]          | - Multiple identities.<br>- Reader can be strangers.<br>- "friend" upon approval [Pixnet.net, 2013]                  | - Email address | - Online Device.<br>- Personal Domain name. [Pixnet.net, 2013]<br>- Meta tags feature gained popularity [Pixnet.net, 2013] | - Password Authentication<br>- Email notification. [Pixnet.net, 2013]                | - Monthly based grouping of blog posts.<br>- Number of people read the posts.<br>- Last login session. [Pixnet.net, 2013]<br>- "appear to be anonymous" hide the commenter identity. | - Similar to FB | - Nickname<br>- Blog visitor identity.<br>- The personal information.<br>- Restrict photo downloading by "disabled right clicked". [Pixnet.net, 2013]<br>- Tag features. [Pixnet.net, 2013]<br>- Third Party application. [Pixnet.net, 2013]<br>- Meta tags. [Pixnet.net, 2013] | - Similar to Twitter  |
| <b>Myspace</b>    | - Manual profile settings.  | - Multiple identities.<br>- Manual approval setting [Myspace, 2013b]   | - Similar to FB | - Online devices.  | - Similar to Twitter.  | - Timeline features<br>- "Highlights" features.  | - Similar to FB | - Location based features.<br>- Personal details.<br>- Connection activity<br>- Third party. [Myspace, 2013a]   | - Similar to Twitter. |

| OSN Type/ Security Keys | Confidentiality  | Integrity   | Identification   | Availability  | Authentication   | Accountability  | Authorization  | Privacy  | Non-repudiation  |
|-------------------------|--|---|--|---|--|---|--|--|--|
| <b>Facebook</b>         | - Manual settings [Facebook, 2012]<br>- Friend lists are visible only if permitted [Facebook, 2012]<br>- Followers are same status as public. [Facebook, 2012] | - Multiple identities<br>- "like" features [Sophos, 2011]<br>- Friend adding features. [Sophos, 2011]       | - Email address [Facebook, 2012]<br>- Telephone no. [Facebook, 2012]<br>- Trusted contacts. [Facebook, 2012] | - Online Device.<br>- Do not have Domain name. [Pursalu 2012] | - Password Authentication<br>- Email notification. [Facebook, 2013]<br>- Trusted contact. [Facebook, 2012]<br>- Text message. [Facebook, 2012] | - Timeline features.<br>- "Download a copy of your Facebook data". [Pursalu 2012]<br>- Real-time communication [Facebook, 2012]<br>- Private group. [Facebook, 2012]<br>- Invite suggest features. [Facebook, 2012]<br>- "official" profile [Facebook, 2012]<br>- Active session. [Facebook, 2012]<br>- General "Friend lists". | - Security code identify the user is human being or not.   | - Commenter identity.<br>- Photo tagging<br>- Location based features<br>- Personal details [Pursalu 2012]<br>- Online Status is "Seen"<br>- Third party application [Pursalu 2012]<br>- Ads.<br>- Download/ copy paste. | - Codes will be sent via SMS to user or Trusted contact when user forgotten password/ username. [Facebook, 2012] |
| <b>Twitter</b>          | - Manual Setting of profile and follower approval.<br>- Profile visible upon setting.  | - Multiple identities<br>- "favorite" or retweet feature<br>- "verified" flag for celebrity [Twitter, 2013] | - Email address [Twitter, 2013]<br>- Telephone no. [Twitter, 2013]   | - Online Device.<br>- Do not have Domain name. [Pursalu 2012] | - Password Authentication<br>- Email notification.   | - Timeline features.<br>- Real-time communication.<br>- "official" account<br>- Retweeter/ Mentioner identity.<br>- Do not have groups like in FB<br>- General "Followers" lists.<br>- "Favorite" features  | - Security code identify the user is human being or not<br>- Settings changes saved after password verification. | - Retweeter or commenter identity.<br>- Harsh tag features.<br>- Personal information. [Twitter, 2013]<br>- Location-based features. [Twitter, 2013]<br>- Download/ copy paste.  | - Codes will be sent via SMS when user has forgotten password/ username. [Twitter, 2013]                         |
| <b>YouTube</b>          | - Browsing of unregistered users is limited.<br>- Profile is linked to Google account [YouTube, 2013]  | - Multiple identities<br>- "Subscribe", "like", "dislike" or share feature [YouTube, 2013]                  | - Google account login   | - Similar to FB   | - Google Account   | - Commenter identity.<br>- Do not have private groups like in FB<br>- General "Subscribers" lists. [YouTube, 2013]  | - Similar to FB  | - Commenter identity.<br>- Uploader identity.<br>- Download videos through various platform. [YouTube, 2013]   | - Similar to Twitter.  |

We found that most people are pleased with current access control methods; they can share their photos and other contents without doubts. Most of them think that the settings are automated with the previous settings and are easy to control too. Most of the users also think that their privacy is protected in OSN and feel safe when using current OSN. Similarly, most of the users believe that OSN will not use their information for other purpose. They feel safe using OSN for content sharing. We found that most people are pleased with current access control methods; they can share their photos and other contents without doubts. Most of them think that the settings are automated with the previous settings and are easy to control too. Most of the users also think that their privacy is protected in OSN and feel safe when using current OSN. Similarly, most of the users believe that OSN will not use their information for other purpose. They feel safe using OSN for content sharing.

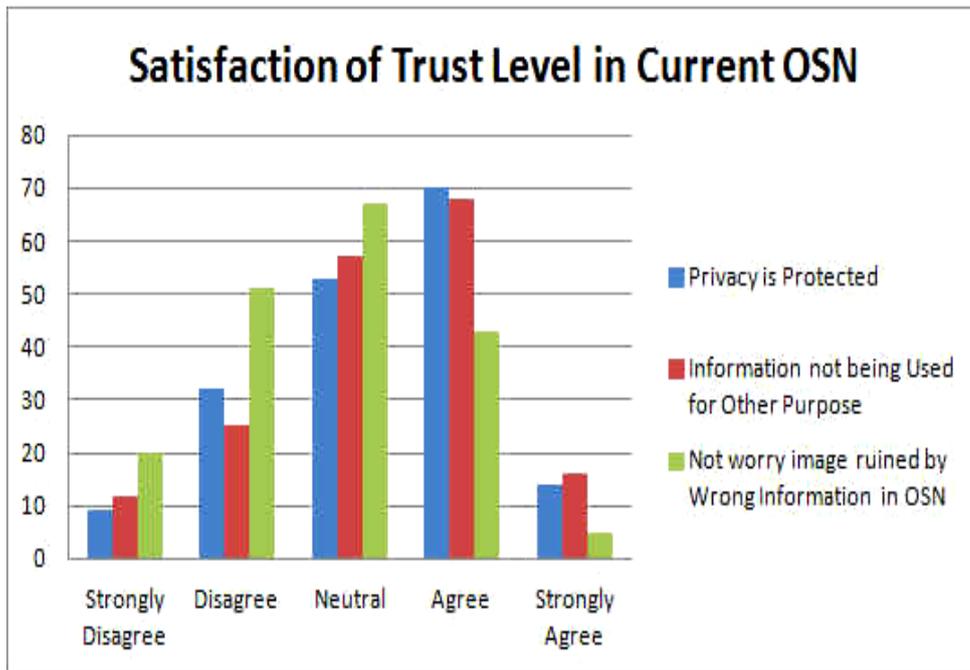


Figure 2. User satisfaction towards current access control methods- Category One

Most of the users also think that their privacy is protected in OSN and feel safe when using current OSN as indicated in Figure 2. There are only less than 40 of the peoples that always doubt about their privacy in OSNs. Also, there are about 55 of people standing neutral instead of addressing concerned in it. Similarly, Figure 2. also indicated that, most of the users believe that OSN will not use their information for other purpose. They feel safe using OSN for content sharing. Only less than 40 of the participants think that it is not, while around 58 of people didn't point out their opinions but remain neutral. As Figure 2. implies also, despite relying too much on OSNs, most of the people are worried about their image is being ruined by wrong information posted in OSN, while about 68 of the respondents stand neutral for it. Only approximately 40 of people are not worrying about it. Since most of the people are satisfied with the current access control methods, we asked the question of whether they trust random strangers to view their profiles, as well as the question of whether access control really is necessary. The result has indicated that only 10 out of these people actually stated the fact that indeed, they do trust anyone and everyone, including random strangers, viewing their profiles.

Most people, however, claimed that they do not, while also a small portion of people are not bothered by it at the same time.

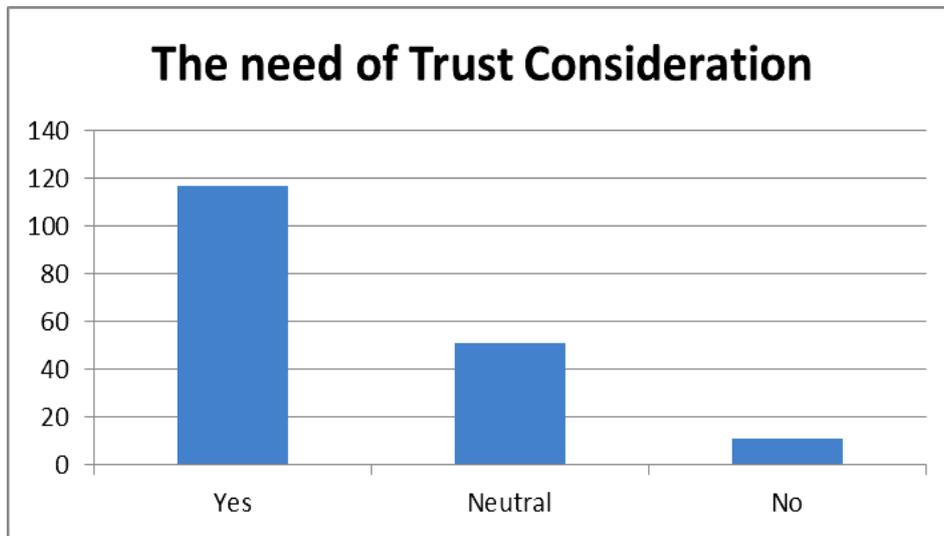


Figure 3. Necessity of access control in OSNs - Category One

We have found a similar contradictive response regarding the necessity of considering the trust level when sharing contents in OSNs, as shown in Figure 3, only less than 10 of these people think it is not necessary, while most people, nearly 120 of the respondents believe that considering the trust level in OSN when sharing something is necessary, and around 50 of people do not care about having control over their profiles and remain neutral. During their memberships of the 12 respondents who are no longer active in OSN, 9 of the participants had set their profiles accessible by directly linked networks, while only less than 1 of them allowed friends of a friend to access their profile. There are only another one of them that set their accessibility to anyone or searchable by search engine. When asked about why you have stopped using OSNs, for instance, a lot of people lost interest in OSNs, mostly due to they are not really happy with the access settings. In our survey, approximately 5 of the participants in this category have lost trust on OSNs most probably due to some unpleasant experiences during their membership. There are around 4 of them who don't dare to post their private data online, as they are doubt for the confidentiality of their data. When asked whether they think access controls of profiles are necessary in OSNs, this group of people had a similar response to category one. On the other hand, among 9 respondents that never signed up in any OSN, some had no interest, some dislike the idea of having private information on the Internet and none of them have never heard of OSNs.

### 5.1. Desired Trust Features and Opinions on the Proposed Solutions

In contrast, when we asked the 200 people the question whether they would trust all their directly linked friends to view all parts of their profiles, most of the respondents only trust some of their connected friends but not all. Most of the people also feel safe when sharing content but only applied to sometimes, while about 30 of them are doubt about the data confidentiality and only less than 20 of them feel definitely comfortable on content sharing. There are only about 10 of them who don't really care about it. We have found a similar contradictive response regarding the necessity of considering the trust level when sharing contents in OSNs, only less than 10 of these people think it is not necessary, while most people, nearly 120 of the

respondents believe that considering the trust level in OSN when sharing something is necessary, and around 50 of them do not care about having control over their profiles and remain neutral. We would like to find out if a multi-faceted model of trust that calculates a weighted average of the eight trusts attributes: credibility, honesty, reliability, reputation, competency, belief, faith and confidence, is to be integrated into OSNs, would that be welcomed?

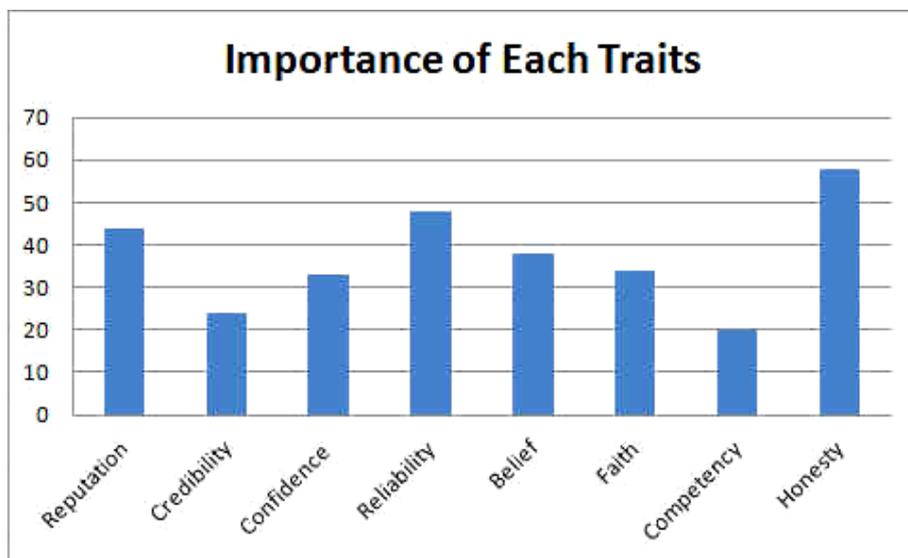


Figure 4. Importance of the 8 Trust Traits

We would like to know is ranking of the eight traits can represent the subjective views of trust in OSNs as well. To do so, we have asked 200 participants who of those eight attributes of trust are most important in their opinions, as shown in Figure 4. Honesty appears to be the most important factor, closely followed by reliability and reputation as well as credibility. Many of them think that rating friends in OSNs seem cruel. However, since privacy is an issue they are willing to take the chance, if there is such a setting.

## 5.2 Analysis of Survey

Several issues have been discovered during the survey, as discussed within this section:

### i. Current trust mechanisms need to be refined.

We find out that, in current OSNs, a single faceted mechanism is used, where user can selectively set their profiles accessibility to anyone or specified groups. Even though the users trust each member in a specific group differently, they are not able to state the trust level for each friend separately. Although mostly they are satisfied with the current access settings in OSNs, a large number of people are worried for wrong information spread through OSNs about them. There should be a multi-faceted mechanism that allows users to express their various degrees of trust in a person, or a group of people context-specifically since the main problem in the current system is that, users cannot express their subjective views on trust freely, and the fundamental trust characteristics mentioned in section 2.4 are not utilized in OSNs.

## ii. Need of better control on the accessed of profiles

As our findings have contradictive found that, a large number of users do not trust anyone and everyone to view all parts of their profiles, and believe controls are indeed necessary in OSNs. This means that, the existing trust mechanism in OSNs has not achieved user satisfaction, hence, refinement of trust management is needed in OSNs.

## iii. Users are unsure about a multi-faceted model of trust with rating features.

Other contradictive findings in this survey are that, users think that trust level should be refined in OSNs, but on the other hand, users have not agreed with the rating features. They find it hard to rate someone they know personally and been rated by others too. Such opinions could be the result of a lack of understanding regarding the proposed solution, as for a large percentage of candidates, since the word rating is so open to be interpreted, it would be very hard for them to simply imagine what ratings could be like without having the rough ideas of how it is going on.

## 6. SYSTEM DESIGN AND IMPLEMENTATION

With influences from Quinn's trust model and considerations for user requirements, we introduce miniOSN, an online social network with a trust rating feature implemented. miniOSN is a web based system that has functionalities of a basic online social networking website, it allows users to create accounts for themselves with a username and password. Users of miniOSN can then confirm a friend request, edit their friendships, upload photos, post status, as well as edit the trust requirements for their content shared.

MiniOSN is developed using PHP programming language and hosted in miniosn.comyr.com, as a free web site. By using miniOSN, users can view a list of his/her friends and edit the friendship accordingly. As illustrated in Figure 5, the user can specify the trust towards his/her friend. The user can rate each of the connected friends differently according to the trust between them based on the eight trust traits, namely honesty, reliability, reputation, credibility, confidence, competency, faith and belief. The rating is made by default zero value, and is range from 1-10. The larger the number, the higher the rating it is.

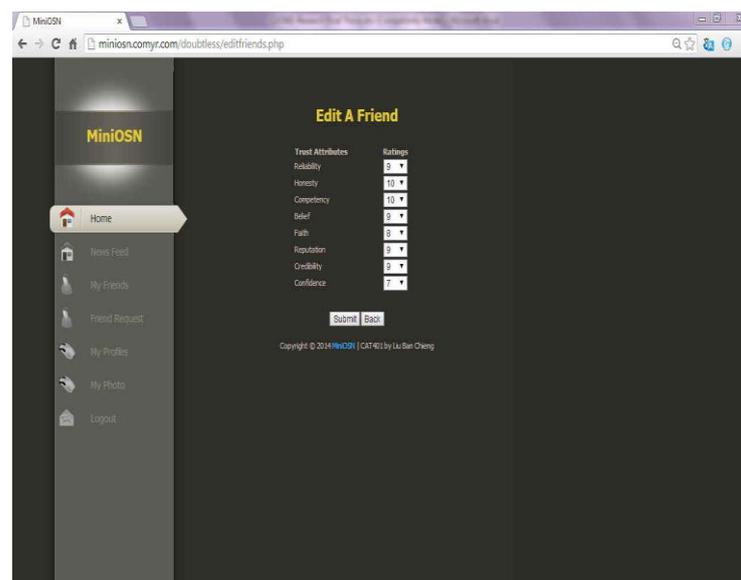
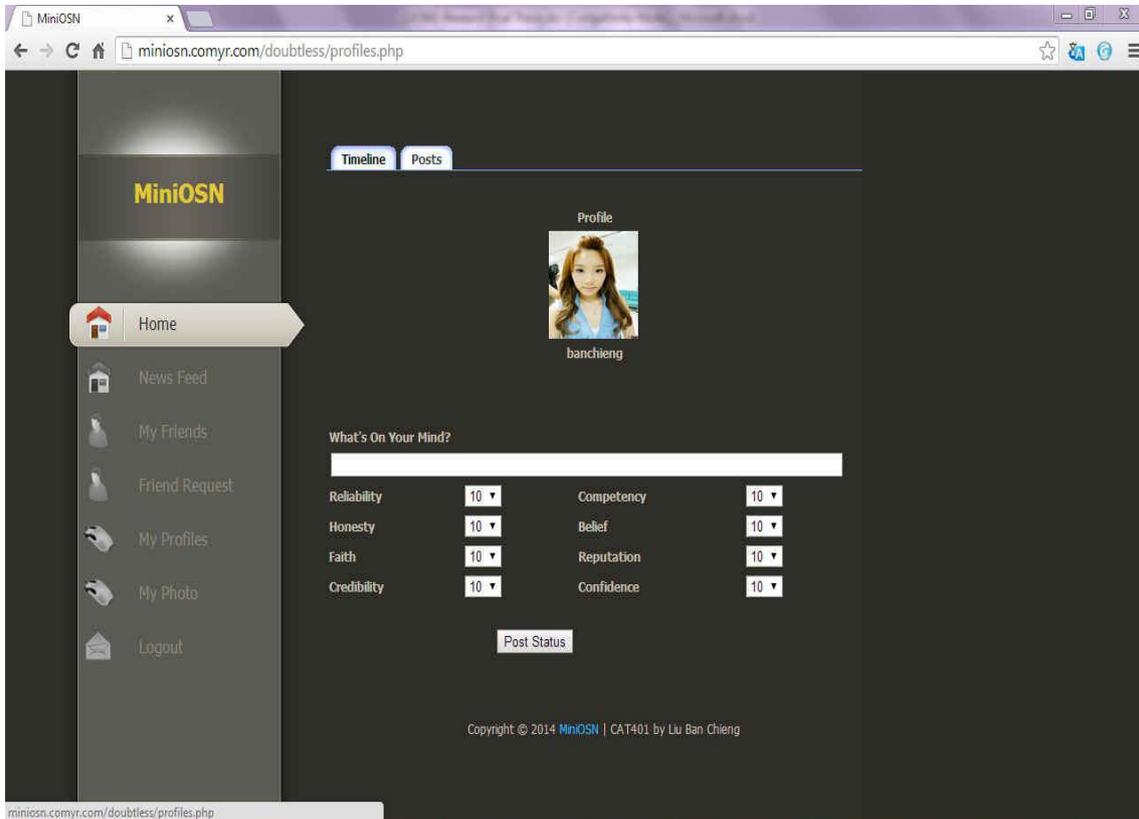


Figure 5. Edit Friendship

MiniOSN enables users to post a status and a photo. Figure 5. shows the timeline of the user profile if the user clicks “My Profile”. User is able to post a status under “What’s On Your Mind?” At the same time, the user can set the weight of each trust traits accordingly in order to adjust the accessibility of the post he/ she want to share.

Figure 6. Profile Page



## 7. EVALUATION

In order to find out what users think of the design and functionalities of miniOSN in relation to expressing various subjective views on trust, we chose to conduct another survey targeting the active OSN users from the 1st survey and gather their opinions on the proposed solution.

Our purpose of the evaluation survey is to find out:

- Whether the user accept the idea of expressing various degrees of trust among connected friends
- How well the trust characteristic found in the literature review helps users of minors to express trust towards friends
- Is the proposed rating feature helpful in gaining better control of user profiles and the content shared?
- The limitation and weaknesses of the mini OSN.

Similar to the 1st survey method, as we are still aiming at a large audience, therefore, Google Docs was again chosen to host the survey on the 5th of May, 2014, over a period of one month time. Invitations to take part in the survey were sent out through email and private message in

Facebook. However, this time, we are targeting on the active OSN participants from the previous survey to answer our questionnaire.

There are three parts of the survey questions, the first part aimed to find out whether the system meets the functional requirement. The second part is to find out do users feel the need to express their various levels of trust among their connected friends and the participants' opinions on how they felt about the usage of proposed trust management solution and how well can users in mini OSN express their subjective views of trust personally and context-dependently. And finally, we asked participants on how well they understand about the 8 trust traits we implemented in mini OSN and how they felt about the trust rating feature. From all this aspects, we are able to defined possible refinement of miniOSN.

### 7.1 Evaluation Results

From the first part of the questionnaire, all of the respondents are satisfied with the functions implemented where their content shared which included photos and status are only visible to the trusted friends only. All of the respondents agree that miniOSN works properly without any technical issues. In the second part of the questionnaire, we found that when asked whether participants felt that they could express trust transitively depending on the context, most of the candidates felt that this is indeed the case. Although one of them felt that miniOSN is not modeled well and doesn't help much in expressing trust depending on context and another one of them felt that there is not much different with the existing OSN. However, almost all of them felt that miniOSN help them to express trust personally with only about 20 of them felt that there is no much difference with the existing OSN.

In the third part of the questionnaire, we found that when asked whether participants felt that rating is an ideal way to preset trust between human, most of the candidates felt that this is indeed the case. Although there are also 38 of them who felt that rating is not a good way to express trust and 20 people remains neutral in this case. However, we found that there is a contradictive view as shown in Figure 7, regarding whether to set the rating to be visible to others or just the user. Surprisingly, among 57 of the participants felt that, rating should be made visible to others while 45 of them think in the other ways and a few of them remains neutral or doesn't pose any concern on it.

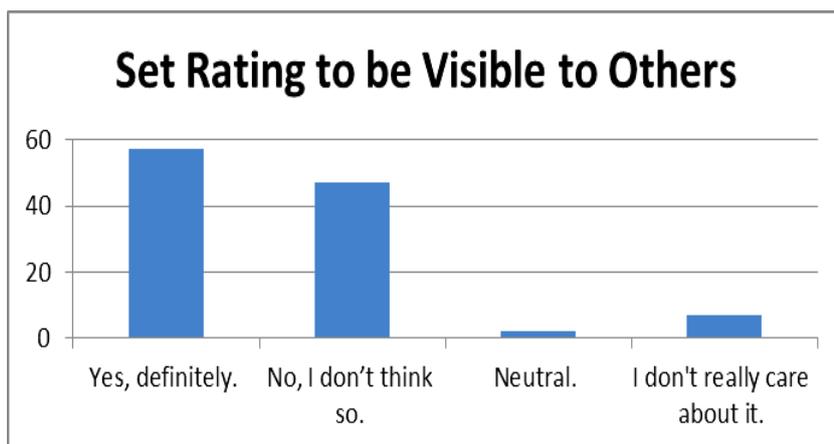


Figure 7: Rating should be Set Visible to Others

When issuing some questions regarding the usage reliability and satisfaction of the trust mechanism, most of the participants felt that miniOSN indeed helps them to shares without any doubts anymore. They felt that their privacy of private information is protected in miniOSN where the weight settings features with preview are convenient for them as it is automated with the previous settings too. However, there is also about 10 of them who do not agree with that, where they found that it is hard to shares without any doubts and they didn't find that the settings helps much. Most of the candidates indicated that miniOSN is easy to use and the rating feature is very helpful in the sense of restrict accessibilities of content shared. However, there are less than 21 out of them think that it is hard to use miniOSN and the rating feature is complicated. Majority of the participants will prefer using miniOSN in the future frequently. In contrast, only two of them will never use miniOSN again. Similarly, all of the participants are confident to use the websites without any doubts and said to be can imagined that most people can use the miniOSN very quickly.

Besides that, we would like to explore the user-friendliness of miniOSN. Figure.8 indicated that about half of the participants think that miniOSN is unnecessarily complex in the sense of the structure and mechanism of rating. They felt that the system become unnecessarily complex and should be modeled in a more simple way that at the same time captured trust mechanism effectively. Only about 30 of them think that it didn't create any difficulties for them in term of complexity. We also found that there is a contradictive view regarding the need of technical support. Majority of the participants felt that they can use the system without any technical assistant, probably because the instruction of using the system are already stated in the homepage that can lead them to use the system easily. Only 22 of them felt that they still need a technical support to assist them in using the system. Moreover, most of the candidates felt that miniOSN is not cumbersome to use and is still considered convenient for them although the structure itself is complex. Only about 10 of the participants felt that miniOSN is not well organized which make it not user-friendly. They might think that the work load has made the simple posting become complicated. When asked whether they need to learn a lot before they can use miniOSN, the responses appear to be dispersed. About half of the total of them felt that it is indeed, while the other half of the participants felt the other way.

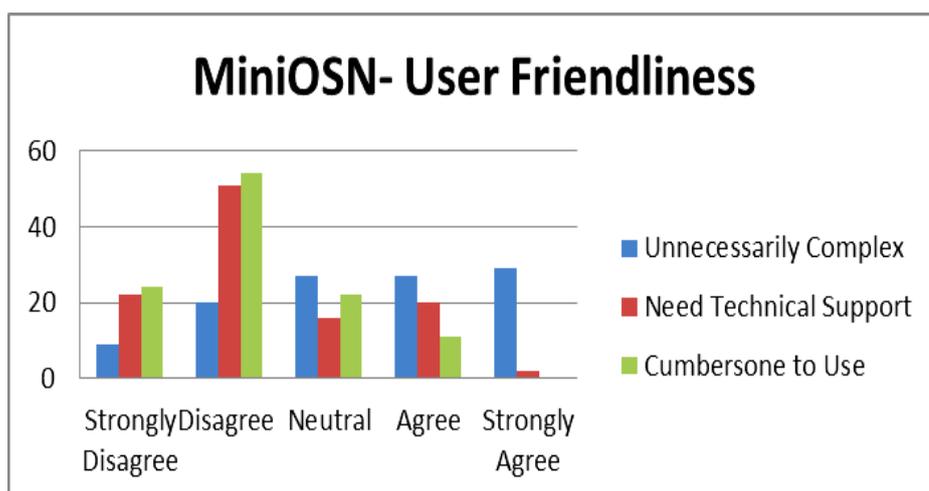


Figure 8. MiniOSN - User Friendliness

Overall, more than half of the participants felt that the trust mechanism implemented in miniOSN did help users to express various degrees of trust, and it also helped users to gain a

better control over their resources in online profiles. However, it was mentioned that the rating system in miniOSN seemed to be over-complicating the situation earlier, most probably because some of them found that it is difficult to understand the attributes. Again, they might think that the work load has made the simple posting become complicated. However, overall, most of them think that the concept is okay for them and is easily understood.

## 7.2 Evaluation Analysis

From the evaluation results, we have found that most people would like to express their subjective views of trust among connected friends depending on the context in the OSN. Most of them felt that the proposed solution would help users to gain a better control over the resources in online profiles. However, some enhancement and modification should be done especially on the structure and design of miniOSN. Since the trust traits concept might cause some confusion and misunderstanding to the users, the selection of trust traits should be defined. Besides that, the management problem is also crucial. Although the users might have a full control over the trust settings of their connected friends, which works well on a one-to-one basis, however, when one has to manage a large number of friends, it becomes difficult for the user to keep track of various sets of numbers.

The design and structure of the miniOSN should also be simpler in the sense that it doesn't complicate the usage of social networks. miniOSN do allowed users to clearly see a list of all their connected friends and their given trust ratings, for easy comparison and readjusting. However, the trust traits number controlling the accessibility should be reduced in the sense to reduce confusion and complication of the overall system. The proposed solution addresses the problem of a lack of personalization when modeling trust in OSNs; however, a common view that trust level decreases as the link between nodes grow longer is not being captured well at the moment. Also, the major problem to be solved is indeed the unnecessary complicated structure of trust mechanism design.

## 8. CONCLUSION

This paper discussed about the challenges faced in online social networks nowadays. Research has proved that the current issues can be classified into security and privacy which can give a negative impact on the trustworthiness and integrity of social networking sites. The security impacts include cybercriminals, identity theft and social phishing, stealing the information of the users affecting data integrity and confidentiality [19, 20]. Malware attack could harm the data availability while physical threat can harm the user's life or reputation. Third party application and advertisement can dig user's data through the social networking sites API. Leakage of data can lead to privacy threat such as identity, user and data privacy. Current trust model in social networking sites using the single- faceted approach is said to be not well differentiate the categorization of friends and the trust value is not personalized and specified. Throughout the comparison and contrasts, a multi-faceted model of trust is proposed by adopting the idea from [6].

Based on the outcome of this research, we have extended our work. We have designed a miniOSN, where the trust concerns are taken based on the eight important traits: honesty, reputation, competency, credibility, confidence, reliability, belief and faith [6]. This model is user-centric, personalized and context dependent, which believes can fit the entire trust requirement of the users. On the other hand, we intend to investigate further the assessment on usability elements via effectiveness, efficiency and user satisfaction. We have conducted a

second survey based on Usability evaluation Methods (UEM). From the evaluation result, MiniOSN is said to provide users with better control over their online resource but refinement is indeed needed to reduce the complexness of the concept which support our hypothesis by using a multi-facet trust model for media social such as Facebook.

## 9. ACKNOWLEDMENT

This paper is supported by Project Grant by the School of Computer Sciences, Penang Malaysia.

## REFERENCES

- [1] Johnson.H, Lavesson.N, Zhao.H & Wu.S.F (2011), "On the Concept of Trust in Online Social Networks", Trustworthy Internet, Springer Milan PP. 143-157, [view online] [http://link.springer.com/chapter/10.1007/978-88-470-1818-1\\_11#](http://link.springer.com/chapter/10.1007/978-88-470-1818-1_11#).
- [2] Zhang.C, Sun.J, Zhu.X & Fang.Y (2010) "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol.24, no.4, PP.13.
- [3] Gunatilaka. D (2011), "A Survey of Privacy and Security Issues in Social Networks." Retrieved From: <http://www.cs.wustl.edu/~jain/cse571-11/ftp/social/index.html>
- [4] Brandtzæg. P.B, Lüdersa.M & Skjetnea. J.H. (2010), "Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites," International Journal of Human-Computer Interaction, 26:11-12, PP.1006-1030.
- [5] Ruohomaa, Sini, and Lea Kutvonen. "Trust management survey." Trust Management. Springer Berlin Heidelberg, 2005. pp 77-92.
- [6] Quinn, Karl. A Multi-faceted Model of Trust that is Personalisable and Specialisable. Diss. School of Computer Science & Statistics, Trinity College, Dublin, 2007.
- [7] Chen.X & Shi.S (2009), "A Literature Review of Privacy Research on Social Network Sites," Multimedia Information Networking and Security, 2009. MINES '09. International Conference, vol.1, PP.93-97, 18-20 Nov. 2009.
- [8] Boyd.D.M. & Ellison.N.B (2008), "Social Network Sites: Definition, History,and Scholarship," International Communication Association, Journal of Computer-Mediated Communication 13, PP. 210-230.
- [9] King, Justin, and Alan Colman. "A Multi Faceted Management Interface for Web Services." Software Engineering Conference, 2009. ASWEC'09. Australian. IEEE, 2009.
- [10] Smetters, D. K. & Grinter, R. E. (2002) "Moving from the design of usable security technologies to the design of useful secure applications", Proceedings of the 2002 workshop on New security paradigms. Virginia Beach, Virginia: ACM, PP. 82-89.
- [11] Hart, J., Ridley, C., Taher, F., Sas, C. & Dix, A. (2008). "Exploring the Facebook Experience: A New Approach to Usability," Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges, ACM. PP. 471-474.
- [12] Nielsen, J. (2003) "Usability 101: Introduction to Usability". Retrieved from: <http://www.useit.com/alertbox/20030825.html>.
- [13] Johnston, J., Eloff, J.H.P & Labuschagne, L. (2003) "Security and human computer interfaces", Computers & Security, Vol. 22, no 8, PP. 675-684.
- [14] Nielsen, J. (1994) "Ten Usability heuristics". Retrieved from: <http://www.nngroup.com/articles/ten-usability-heuristics/>.
- [15] Norman, N. (2014) "The first principles of human computer interaction". Retrieved from: <http://asktog.com/atc/principles-of-interaction-design/>
- [16] Shneiderman, B (1998) "Designing the user interface: strategies for effective human-computer interaction, Menlo Park, CA: Addison Wesley
- [17] Herzog A. and Shahmehri, N. (2007) "User help techniques for usable security", Proceedings of the 2007 symposium on Computer human interaction for the management of information technology, March 30-31, Cambridge, Massachusetts

- [18] Hertzum, M. (2010). "Images of Usability" *International Journal of Human-Computer Interaction*, 26(6), PP.567-600.
- [19] Sophos (2011). *Social Networking Security Threats: Understand Facebook security threats*. Retrieved From: <http://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx>
- [20] Brandt. A. (2010). Five Reasons You Should Always "Stop. Think. Connect." Retrieved from: <http://www.webroot.com/blog/2010/10/04/five-reasons-you-should-always-stop-think-connect-2/>
- [21] Facebook. In Facebook [Policy Page] Retrieved October 16, 2013, Retrieved from: [https://www.facebook.com/full\\_data\\_use\\_policy#publicinfo](https://www.facebook.com/full_data_use_policy#publicinfo). (2012).
- [22] Furnell, S. M. "Why users cannot use security", *Computers & Security*, vol.24, 4, PP. 274-279. (2005).
- [23] Gunatilaka. D, "A Survey of Privacy and Security Issues in Social Networks." Retrieved From: <http://www.cs.wustl.edu/~jain/cse571-11/ftp/social/index.html>. (2011).
- [24] Hart, J., Ridley, C., Taher, F., Sas, C. & Dix, A. "Exploring the Facebook Experience: A New Approach to Usability," *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*, ACM. PP. 471-474. (2008).
- [25] Pixnet.net. In Pixnet.net [Control Panel Page]. Retrieved October 18, 2013, Retrieved from: <http://panel.pixnet.cc/account>. (2013).
- [26] YouTube. In Youtube [Account Setting Page]. Retrieved October 18, 2013, Retrieved from: [http://www.youtube.com/account\\_privacy](http://www.youtube.com/account_privacy). (2013).