International Journal of Energy, Information and Communications
Vol.6, Issue 1 (2015), pp.45-58
http://dx.doi.org/10.14257/ijeic.2015.6.1.05

A Social Network Model with Privacy Preserving and Reliability Assurance and its Applications in Health Care

Chunming Gao[1] and Noriyuki Iwane[2]

[1]School of Technology, Michigan Technological University, USA
[2]Faculty of Information Sciences, Hiroshima City University, Japan
[1]chgao@mtu.edu, [2]iwane@hiroshima-cu.ac.jp

Abstract

Social media has become a platform to provide big data services. In healthcare applications, online E-health platforms have enabled patients to obtain useful references on the Internet, as well as to share information and exchange experiences among people with similar diseases. Such social networks also enable researchers and marketers to conduct studies or advocates on targeted groups of patients. However, how to protect user privacy while assure user and data reliability at the same time remains a challenge in practice. This article tackles the problem by exploring trust-engagement mechanism and developing a dynamic multi-trust model integrating multilevel access control, credible anonymity, and mutual rating mechanism for a multi-purpose healthcare social network. The social network model we presented in this study mainly focuses on the purpose of big data privacy preserving, and user and data reliability assurance. We discuss the mechanism of the model and present practical implementation designs on achieving the goals. We also apply the model in the healthcare social network to elaborate how electronic health records (EHRs) and personal health records (PHRs) can work together to support a social health record (SHR) network which enables privacy preserving and user and data reliability.

Keywords: *big data; social network; trust model; health care; privacy; user and data reliability*

1. Introduction

Big data on social network has been valuable resources to online users, researchers, and marketing organizations. Input from users has contributed to the quick growth of online big data and in return the big data becomes potentially more useful. Social media has become a platform to serve big data service, such as user communication or information exchange in a specific online community. However, to make a multi-purpose social network to be practical, concerns must be addressed regarding data security, user privacy, user and data reliability, as well as how to promote user participation. While data security has been a constant research topic for decades, how to protect user privacy while assure user and data reliability at the same time is still a big challenge both in practice and in academic research on these social networks. The ability in retaining users is also one of the fundamental factors to the success of social networks. Various social network platforms, such as Facebook [1] and LinkedIn [2], have been successful in gaining substantial popularity among participations by providing services, *i.e.*, social connections and professional connections respectively. Online healthcare social networks such as PatientsLikeme [3] gather people in the same interest in dealing with healthcare issues. In healthcare applications, online healthcare social network platforms have enabled patients to obtain useful references on the Internet, as well as to share information and exchange experiences among people with similar diseases. Such

ISSN:2093-9655 IJEIC

social networks also enable researchers and marketers to conduct studies or advocates on targeted groups of patients. These healthcare social networks can also provide platforms for researchers to survey and study self-reported patient data [3-9]. Meanwhile, studies have raised concerns similar to any other social network regarding data security, user privacy, user and data reliability. Innovative new network models have been summoned for further studies [10]. Our work addresses these concerns as trust-engagement and develops a dynamic multi-trust model integrating multilevel access control, credible anonymity, and mutual rating mechanism for a multi-purpose healthcare social network.

The social network model we presented in this study mainly focuses on the purpose of big data privacy preserving, and user and data reliability assurance. We discuss the mechanism of the model and present practical implementation designs on achieving the goals. We will also apply the model in the healthcare social network to elaborate how electronic health records (EHRs) and personal health records (PHRs) can work together to support a social health record (SHR) network which enables privacy preserving and user and data reliability. The main contribution of this work is to develop a multi-trust model integrating public key encryption, access control, pseudonymous authentication, and mutual rating mechanism for a multi-purpose healthcare social network. We will also explore the design domain for practical implementation of the model, for the purpose of user privacy preserving and user and data reliability assurance.

The rest of the article proceeds as follows. Section 2 introduces an overview of a generic multi-trust social network model. Section 3 presents a dynamic implementation of the model and the mechanisms to assure privacy and user and data reliability. Section 4 discusses the applications of the model in the healthcare social network domain. Section 5 evaluates the model and the applicability in health care. Section 6 discusses related work. Section 7 concludes and discusses future work.

2. Overview of a Generic Multi-Trust Social Network Model

In this section, we present a generic network model (Figure 1), which can serve as a social network platform. Using this platform, a virtual community can be formed where users take part in the activities anonymously or by using pseudonyms. However, this virtual community is not isolated. It is connected with real entities which hold users' true identities and can therefore endorse users' attributes on the virtual community. In this way, although users are anonymous in the social community, their endorsed attributes are trustworthy. Hence users or third party researchers and marketers can put trust on the targeted users for information exchange, research, or study based on those trusted attributes. Users can put trust on the platform regarding their privacy on participating in the virtual community activities. This multi-trust social network model includes the following components:

- Virtual-network Control Center (VCC)
- Participating Organizations (POs)
- Service Requesters (SRs)
- User Interface (UI)
- Users

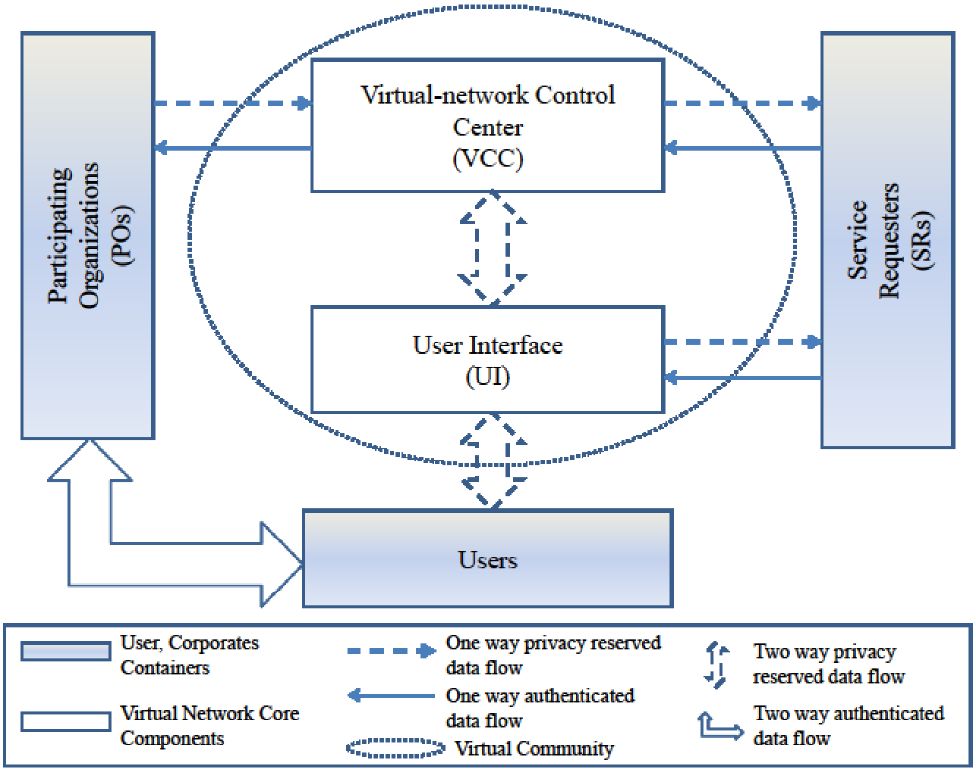
Virtual-network Control Center (VCC)
User Interface (UI)
Participating Organizations (POs)
Service Requesters (SRs)
Users
User, Corporates Containers
Virtual Network Core Components
One way privacy reserved data flow
One way authenticated data flow
Virtual Community
Two way privacy reserved data flow
Two way authenticated data flow

Figure 1. A Generic Multi-Trust Social Network Model

VCC maintains the central database for pseudonym-based accounts and trust control. The User Interface (UI) is to provide a platform for the users to activate their virtual account on VCC and register on the virtual network, as well as for the users to retrieve information, interact with others, and take part in the activities requested by SRs, or for the SRs to request services on VCC. POs are the trusted organizations which hold valid user identifications and official user data. In order to join the network and enable their valid users to participate, POs first create unique numbers (UNs) and temporary pass codes for their users. POs then transfer the UNs and pass codes along with trust-necessary attributes TA($a_{1,}$ $a_{2,}$ …, a_i) to VCC. TAs($a_{1,}$ $a_{2,}$ …, a_i) are the essential attributes to categorize users to serve the purpose of the virtual network, but using these attributes alone cannot reveal users' true identities. Users then use their UN and pass code to activate and register on VCC. When registering, users will create their login name and password. They may also create their pseudonym and virtual profile according to their preference. Once registered, users can selectively publish their TAs. Partial or whole TA($a_{1,}$ $a_{2,}$ …, a_i) will become published attributes PA($v_{1,}$ $v_{2,}$ …, v_j), which will be revealed to public for other users to identify similar users. Login names are unique on VCC. Users can change their login name, password, and other profile information at any time. Login names will not be revealed, while pseudonyms and virtual profiles are publicly shared.

SRs may request survey, advocates or commercial services on VCC, targeting some specific users based on users' TA($a_{1,}$ $a_{2,}$ …, a_i), which could only be updated by POs, and categorized by VCC. VCC is responsible to provide the targeted groups to SRs and provide the options for users to opt for participation. Users will not reveal their real identities by taking part in such activities. VCC is responsible to manage bookkeeping of users' participation activities by using UNs. The service requesters may provide incentive rewards, such as monetary credits or gift cards to participants. VCC is responsible to pass these rewards to the users through the UN issuers, *i.e.*, the correspondent POs.

In the model, multi-trust is engaged in terms of data security enforcement, user privacy control, participant credibility control, and rewarding mechanism. The main concern on data security is regarding communication channels among the network components. This could be enforced through public key encryption so that the participating parties and users get appropriate authentication and verification when necessary. User privacy is fully enforced through levels of access controls. First, users need to consent so that their unidentifiable attributes may be transferred to VCC from POs. Second, users need to activate their accounts on VCC and selectively publish their attributes. Third, users create their virtual profile freely and may make any changes any time. Fourth, only POs can link real user identities through UNs. User credibility is fundamental for SRs and other users to trust the participants and related data input. This is addressed by requiring that participants must be valid users in POs, and the users' TA($a_{1,}$ $a_{2,}$ …, a_i) can only be updated through POs. Furthermore, users can be rated by other users based on their participations. Users' change of pseudonyms will not affect their ratings. In this way, a user's reliability can be kept consistent. To encourage users' participations, incentives may be necessary. A reliable reward mechanism is through VCC's bookkeeping of user participation and inverse information passing via UNs to corresponding POs. SRs pass the rewards through VCC to POs. The POs will disburse the reward to the real users through real-world channels.

In the next section, we discuss a dynamic implementation of the proposed network model and discuss the mechanisms to preserve privacy and data reliability.

3. Dynamic Designs and Implementations

3.1. Dynamic Designs

In reality, the number of network components such as POs and SRs is not limited. It will be dynamic that any components could join the network or leave the network. The network model should be flexible in maintaining varying number of components and accepting new components. Core component of the network model is VCC, which is responsible for maintenance of virtual user accounts, applications, and management of real time big data. To extend the model further, there can be multiple VCCs (Figure 2) on the network, which is a better reflection of real world scenario. In this case, users can decide which VCCs to join based on their interests. VCCs and POs, VCCs and SRs could authenticate each other using a trusted agency's certificate.

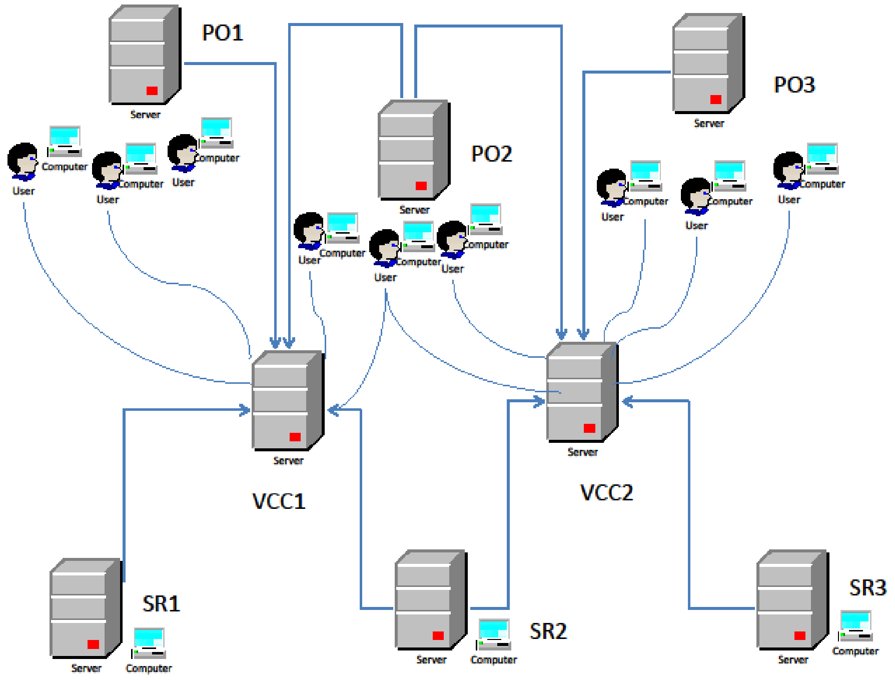

Figure 2. Dynamic Implementations

In order for users to join a VCC, a PO needs to obtain unique universal identifier numbers for each user. This unique number cannot be created locally on PO. Instead, VCC will be responsible to provide UNs for the trusted POs. Depending on the network implementations, it does not matter whether there is only one VCC or there are multiple VCCs, there should be one dedicated agent for UN creations. VCC or VCCs apply UNs from UN creation agent and maintain a UN pool. Similarly, a PO applies for UNs from one of the VCCs and maintains a UN pool locally. Whenever UN pools are low, the system will automatically apply new UNs. This is true for VCCs as well. When the UN pool is low with a VCC, the VCC will apply more UNs from the UN creation agent.

There are two options to form a UN number. One option is to design the number into meaningful sections. One example is by using an area code and a sequential number like the formation of a phone number. While the advantage of this design is easy to categorize the UNs based on area code, on the other hand, it would make the creation of UNs complicated. The main reason is that VCCs are developed not based on the geographic regions. Instead, they are developed based on domains of applications. The other option to form UNs is to make UN a pure unique sequential number. One cannot derive anything from a UN itself. In this case, categorization of UNs will have to rely on individual attributes which are associated with UNs. VCCs will be responsible for such management. For example, VCC can categorize the UNs based on which PO a UN belongs to.

3.2. Privacy Protection Mechanism

Users' PO accounts are first created and maintained in trusted organizations, where users' identities are verified. Users' attributes on POs are maintained as trusted data sources. User privacy in these organizations is enforced via local access controls and PO's security and privacy policies, which is beyond the scope of this study. Our focus is on how user privacy is preserved when participating on VCC. Following the dataflow paths in Figure 1, we will first examine the access controls when user information is transferred to VCC from PO. On a PO site, users will decide if they want to join a VCC. There could be two design options for implementation considerations. One design option is opt-in, for which the default is for the users not participating on VCC. Users have to explicitly consent to enroll in the participation list so that UNs can be created for them. The other design option is opt-out, for which the default is for users to participate on VCC automatically unless users explicitly decide not to. Either ways, users need to be clearly informed and users have the authority to join or not to join. If a user decides to join a VCC, a UN will be assigned and the appropriate information will be transferred to the VCC.

If a user has accounts on multiple POs, it is possible that when the user is offered to either opt-in or opt-out to a VCC on a PO site, the user might have already joined the VCC previously. In this case, the user will be asked to provide his/her UN so that any new attributes will be related to the account on the same VCC. If it is on a different VCC other than the previously joined, it does not make much difference if the user is assigned a new UN number. However, for universally consistency considerations, it is best to keep one UN for each user at all times. In the case that a user forgets his/her UN, the user can either find it by logging on to the VCC site, or the original PO could find it out at the PO site. If a user could not have access to any of these resources, a new UN will be necessary for the user to join a VCC. However, the new UN will not link to the account related to the old UN and the old account on VCC becomes stagnant account. When this happens, there can be various ways to deal with. One effective method is for a PO to send an invalidating signal to VCC when the PO identifies an old UN for a user. On the VCC site, the stagnant account can be set as invalid if it has been inactive for a designated period of time. By doing this, users will be given the authority to decide when to terminate the VCC account.

UNs assigned to user accounts at PO site are mapped to the correlated user accounts. This is the only place where a UN could be mapped to the real user by the proposed network system. A UN is transferred to a VCC along with de-identified user attributes and initial sign-on pass codes. When a user registers on VCC using UN and pass code, the user will create a login name and password. After that, the account will not be able to be accessed through the UN anymore. A user will have full control of the virtual account by using VCC login name and password.

VCC login names are unique on each VCC site and they are not revealed to public. Instead, users' virtual names are public. There are no restrictions on what could be taken for virtual names and these virtual names can be changed freely. Therefore, multiple users could take same virtual names and users have to be distinguished from each other by using other means such as virtual profile pictures and other virtual public attributes.

Other than their virtual profiles, users also have full control of their posts on to the VCC site. For their previous posts, they have the privileges to either edit or remove. Hence users have the rights to dynamically safeguard their confidentiality and privacy on VCC sites.

3.3. Reliability Assurance of Virtual Users

On VCC, users can decide what virtual identifies to use and what attributes to reveal to public, as well as to post messages, questions or comments freely. However, to make a social network to be meaningful, a mechanism to promote trustworthy must be maintained and the accountability of user activities will have to be ensured. One purpose of the proposed network model is to help assure user and data reliability.

First, user accounts, user posts, and user activities are related to their UNs even though UNs are not revealed to public. Although VCCs do not obtain real user identities, user activity information could be presented to their POs. This is important because it provides a reliable channel to ensure user activity accountability. This feature enables applications such as for the users to get reward or to get evaluations for their virtual world activities and performance.

Second, users are rated by their peers on VCC. This rating will be attached to the user accounts no matter how a user changes his/her profile information. The ratings can be simple. One practical way is like the rating method adopted by Amazon.com, which is to state the percentage of positive ratings in a recent period of time and the number of total ratings. By looking at this, other users can obtain some trust level of a user who participates on VCC. In addition, the rating on a user should be a reflection of the user's participations and posts. Therefore it should be a derived value from all factors related to the user. One main factor can be individual ratings on all the individual posts. In that way, any individual post is rated separately. In this case, a user's rating is not necessarily completely related to an individual post's rating and valuable posts could be retained even if in the case of a poor rating of the user.

Third, VCC categorizes users by using their TAs, which are provided by POs. These attributes are considered verified and reliable information regarding users although users might not decide to publish some or all of them. This categorization is for the purpose of third party (SRs) activities such as surveys targeting a group of users with similar attributes. VCC informs the categorized users about SRs' requests and the informed users decide if they want to take part in the SRs' activities. Through this process, SRs can be assured that users are valid in a targeted group.

3.4. VCC Site User Interface Designs

VCC is the core of the virtual network. It is a hub for the users, POs, and SRs. It maintains virtual user accounts and keeps the semi-structured big social data. Above all, the interface makes everything meaningful. It must serve the purpose of essential functions of a social network, as well as to provide secure communication channels from VCC to POs and SRs. To serve as a social network interface, VCC must be user friendly and follow a user centered design for the login homepage and all the other linked pages. Usually a good login page should:

1) Briefly state the features of the site
2) Present the login window
3) Provide the initial sign up options

As demonstrations, we examine the user interfaces of the following social networks, *i.e.*, Facebook, LinkedIn, and PatientsLikeMe. On the login page of Facebook, it states that you can "Connect with friends and world around you" and "See photos and updates from friends", "Share what's new in your life", and "Find more of what you're looking for". On the login page of LinkedIn, it states that you can "Join the world's largest professional network". On the login page of PatientsLikeMe, it states the purpose is "Making healthcare better for everyone through sharing, support, and research" and you can "Learn from others", "Connect with people like you", and "Track your health". After logging in, users are provided the interfaces to conduct the activities to fulfill the purpose of the sites. A successful design is always user centered design which is for the convenience of users, in which case, Facebook, LinkedIn, and PatientsLikeMe all followed these design principles on their login pages. However, regarding user credibility, although Facebook and LinkedIn require that users are to use real identities, there are no solid mechanisms to verify or enforce this requirement. PatientsLikeMe asks users to self-claim and self-verify their identities hence there is no guarantee of the identities of members on the sites and there is no guarantee of the accountability of the data posted by the users. Our proposed social network model has tried to address these issues through POs verifications and peers' ratings as discussed in previous sections.

When there are multiple VCCs, the VCCs usually do not communicate with each other and they communicate with POs or SRs independently. Connections between VCCs and

POs or SRs can be built up through mutual authentication by using public key encryptions. Although VCCs maintain the database for anonymous accounts and provide user data sharing services, there are still confidential data such as UNs, unpublished user attributes, and identities of POs. All these data along with user public data should be secured to ensure data integrity on VCC sites.

Another issue which might post as a security and privacy concern is when users are requested to take part in SRs' service, a network redirection might happen. In this case users should be alerted that they are going to be redirected and they need to watch out for what they have to reveal themselves on SRs' sites. While on VCC, users conduct their own privacy practices when communicating with other users on the site. Therefore, users should be informed to practice their own privacy and respect others' as well.

4. Applications on Healthcare Social Network

This section demonstrates how the multi-trust social network model could be applied on a healthcare social network and what kind of services this network can provide.

In an online healthcare social network, hospitals, clinics, and medical institutes serve as POs which hold authentic records for patients and healthcare providers. VCCs are independent organizations which can act as special-purpose business associates of the POs. VCCs will be responsible to provide healthcare information sharing service for users. Users could include patients, nurses, and doctors. In some applications, medical schools could also serve as POs. In this case, medical students will be special users on VCC who can practice medical consulting and gain real-time medical experience in the virtual community. When hospitals and medical schools join VCC of the healthcare social network, they transfer the attributes of user status accordingly. A user might have dual status, *e.g.*, the user could be a patient and a healthcare provider, or could be a patient and a medical student. Other attributes to be transferred to VCC include important factors which are used to categorize patients, such as types of diseases that patients have experienced, and the types of medications a patient once took. On the PO side, patients are provided the option whether to take part in activities on a VCC. On the VCC side, patients and other users create a virtual profile along with a pseudonym and selectively publish their medical attributes. Hence, from a user's pseudonym and the published attributes one can tell if the user is a doctor, a nurse, a student, a patient and what diseases the person might have experienced.

This healthcare social network (Figure 3) based on the multi-trust social network model could serve multiple purposes. We discuss a few applications in this section.

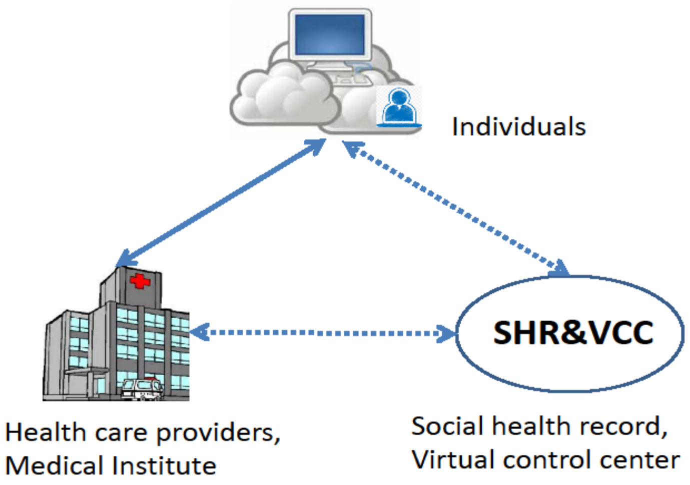

Figure 3. Components of Multi-Trust Healthcare Social Network

4.1. A Platform for Patients to get Second Opinion

When people get sick, they think about seeing doctors. However, when they have to suffer for an enduring time because of chronic diseases and conditions, they tend to seek second opinions from all available resources. Needless to say, the online resources in the format of public EHR (electronic health record) systems and online forums are becoming attractive. Especially the interactive sites which could enable communications among users embrace potentials because they can also satisfy people's social needs. Unfortunately one obstacle to hinder user participations are concerns over privacy and reliability. People wish to participate might want to keep privacy. While some sites such as PatientsLikeMe [3] can provide anonymous participations, reliability of users and data then becomes an issue. The multi-trust healthcare social network model (Figure 3) can provide a platform to address this dilemma.

On VCC, users keep anonymous by using pseudonyms. Their initial social health records (SHR) including the trusted attributes (TAs) are transferred from authority organizations such as hospitals and clinics. After user registration on VCC, users can publish their TAs based on their privacy preferences. Using the published attributes (PAs), patients can identify others with similar diseases and share experiences with each other. They can also consult online volunteers who are specified as medical professionals or medical students. Since users are rated, patients can put informed level of trust on the second opinion of the source.

4.2. A Platform for Education of Volunteering Medical Students

An online virtual healthcare social network will provide pre-med college students and medical school students a real-time medical environment for them to gain experience and even practice consulting. Since they participate as special users, their ratings can serve as evaluation of their study and practice, which will help them to obtain new knowledge and enhance skills in patient treatment.

When student records are transferred to VCC, they are marked as medical students. After students activate their accounts, they can post or comment other users' posts. Their posts will be rated by other users. Since their activities and ratings are related to their UNs, these data can be transferred to their home institutes for educational evaluations.

4.3. A Platform for Targeted Surveys and Commercials

Healthcare researchers could request VCC for experimental studies on targeted groups of patients. Similarly, healthcare related businesses could also conduct advocates or commercials on targeted groups of people with similar diseases. Although it is in a virtual environment with people using their pseudonyms, TAs($a_{1,}$ $a_{2,}$ …, a_i) on VCC can assure the targeted groups are valid users with similar diseases. Also because of the reward-enabled feature, patient participation could be reasonably assured.

To encourage patients' participation in the surveys, rewards can be used as incentives. Using the proposed platform, users will still keep anonymous while taking part in these events. VCC will keep a record of user participations. The rewards are provided by the SRs, which could be research institutes or commercial organizations. The rewards can be conveniently in monetary credits, which can be transferred to VCC and VCC will further transfer it to the hospitals or clinics which host the users. These participating health organizations will deliver the rewards to their patrons who are rewarded on VCC.

5. Evaluation

This section analyzes how the objectives are achieved to preserve user privacy and assure user and data reliability. We also discuss the practicability of applying the model in healthcare.

5.1. Privacy Preserving

The objective to preserve user privacy is by giving users multiple levels of access control and full CRUD privilege (create, read, update, and delete) on the social network. We can see four levels of access control which have been adopted in the model.

First level happens in a participating organization (PO) where users' real identities have to be involved. At this place users are offered to either join or not to join a social network. Only with users' permission, their de-identified information can be transferred to the social site (VCC).

Second level access control happens at the VCC site, where users decide either to activate or not to activate their social account. Their UN number and initial pass code are only used once at registration time. Examining Figure 1, it is clear that using UN will not be able to retrieve any real identity information from POs.

Level three is requesting users to use login name and password to login, but the login name and password are not revealed to public. Instead, pseudonyms are used for others to identify users. Further, the pseudonyms can be changed freely at the users' free will.

Level four is to provide users the authority on their virtual profile and their own posts. Since users' posts are the hard-to-control sources that could reveal their real identities, also because users could have various levels of comfortable about their posts, giving users full control is important to satisfy the requirement of privacy preserving.

Through multiple levels of access controls, real identities of users are hidden deep at participating organizations. In order to obtain identities of users, adversaries would have to break into the VCC first. Even if the adversaries might get UNs on VCC, since there is no linkage information, they still cannot retrieve users' real identities. However, a vulnerable place of privacy preserving is at the posting site on VCC. Adversaries might take advantage of a user' posts to derive the real identity. The model is to leave it to users' discretion on how much to reveal while informing users about privacy preserving.

5.2. Reliability Assurance

One objective of the model is aimed to make user activities accountable. In this way, it will assist to further reinforce user activity reliability and user input reliability. Although users only reveal virtual identities and virtual profiles on the social network site, their attributes are verified, which present to be reliable. Although users might post anything at their free will, their activities are linked to their UNs at background. Although they cannot be identified on VCC, technically their activity can be reported back to the participating organizations. In real applications, policies can be developed regarding what should be expected on users' activities, and what consequences might incur if policies are violated.

The fact that all the users on VCC are authentic users from participating organizations along with verified attributes forms the foundation of user and data reliability. Furthermore, through user rating methods, the credibility value of individual posts and users will be attached to a user account and posts respectively. Even though users may change their pseudonyms, these ratings will be always attached. Therefore, users and services may reasonably assume a certain level of trust on the user activities and user input.

5.3. Practicability of Application in Health Care

In the United States, health care related service providers are regulated by HIPAA law (Health Insurance Portability and Accountability Act). Under this law, de-identified patients information can be transferred to business associates for research purposes. On the other hand, meaningful use of electronic health records (EHR) is encouraged and still under development. Under reasonable belief, the desire of patients to share experiences with people having similar diseases will eventually require the social networks to connect with health service providers. Our proposed social network model would support both the requirement of law and the service demand of users.

6. Related Work

R. Steele [11] summarized potential capabilities of health-related social media in five categories based on relations of participating parties. The five relationships are patient-patient, clinician-patient, public health-consumer, researcher-patient, and corporate-patient. In patient-patient category, patients are mainly to communicate with other patients, like on PatientsLikeMe [3]. In clinician-patient category, healthcare providers can communicate with patients through online applications such as the systems hosted by hospitals. In public health-consumer category, patients can obtain general health information online through health organizations' websites, such as CDC website [12]. In researcher-patient category, researchers can conduct targeted surveys or clinical tests on the patients through the online channel. In the corporate-patient applications, marketers can advertise their products to the targeted group of patients. However, to make a healthcare social network which can serve multiple purposes to be practical, concerns must be addressed regarding data security, patient privacy, quality and reliability of data, participant accountability, and promotion for participation. While it is common practice to enforce data security, how to protect privacy and to provide accountability at the same time still embraces further research [13-15]. There exist inherent conflicts between preserving of security and privacy and the design goals of social network [10]. Ref. [10] argues that asking users to register with their government issued identity cards can prevent identity forging hence enhancing user and data reliability, but unfortunately user privacy cannot be guaranteed. It further challenges more creative designs of social networks to address this problem. In our study, we aim to develop a network model to address this dilemma.

Ref. [16] studied the limitations of healthcare social media and argued that a monitoring mechanism for the quality and reliability of data is required. In our proposed model, we conducted a different approach to enhance quality and reliability of data by adding participant rating of individual messages and participant rating of individual users. Ref. [16] also argued that social media users should be educated on using online resources to protect their confidentiality and privacy. Ref. [17] aims to preserve patients' privacy of electronic medical records by giving the authority to patients through patient controlled encryption. It proposes that all records stored in data center are encrypted and the encryption keys are created by patients and saved by patients. Patients send encryption keys to caregivers so that their records could be accessed. The communications between patients and caregivers are through public-key encryption so that they are confidential. As the authors stated, this mechanism can be functional, but it requires the responsibly of patients and caregivers to store their private keys locally. Similarly, Ref. [18] proposed a mechanism to protect Electronic Health Record (EHR) data security in a cloud environment by requiring a trusted authority to issue encryption keys. The data are encrypted and stored on a cloud server. Patients authorize access to users and users obtain the private keys through trusted authority. It also suggests that the private key can be revoked and the data could be encrypted using a different private key. In our model, users do not need to store their keys locally. Instead, data security is assured through trusted servers in trusted organizations and levels of information revelation and levels of access control. In our social network model, the social network platform only holds virtual user information while all the identifiable information will stay within the trusted organizations. We may also put the social network platform on cloud servers. However, since the main functions are to enable user information sharing, encryption of these data are not essential. Instead, privacy, reliability, and accountability will be the main concerns. Some studies [19, 20] seek to preserve privacy through authentication based on users attributes and set various levels of privacy. By enforcing levels of privacy, the least information could be revealed in attributes matching. In our proposed model, similar to this level controlled privacy, users have the control over which attributes to reveal to the public. Ref. [21] discusses a mechanism which cut off the linkages to users' previous posts while maintains the trust through voted reputation values. In this way, users' privacy can be preserved against linkage attacks. Our design uses a similar rating mechanism while provides users with fully control on their posts. We also aim to address this issue through flexible virtual profiles.

7. Conclusions and Future Work

Our study contributes by developing a generic multi-trust network model integrating security, privacy, accountability, and credibility through multi-level access control, pseudonymous authentication, and mutual rating mechanism. We demonstrated its applications for a multi-purpose healthcare social network which bears the feature of promoting user participation. By adding the dimension of promotion for user participation, we believe a new research area is revealed and the solutions will have broad impacts in real world practice. However, further research needs to be conducted to address new challenges. As one open question, while a reliable rewarding mechanism is useful to promote online patients participation, how can a system prevent or detect falsification on self-reported data? Our future work also includes an implementation of the proposed network platform in a clinical environment to test its feasibility and explore further development possibilities.

Acknowledgements

The authors would like to thank the anonymous reviewers and the editor for their constructive and encouraging comments.

References

[1] Facebook. Online at https://www.facebook.com/.

[2] LinkedIn. Online at https://www.linkedin.com/

[3] J. Brubaker, C. Lustig and G. Hayes, "PatientLikeMe: empowerment and representation in a patient-centered social network", CSCW Workshop, USA, **(2010)**.

[4] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou and R. H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, **(2013)**.

[5] J. Pearson, C. Brownstein and J. Brownstein, "Potential for Electronic Health Records and Online Social Networking to Redefine Medical Research", Clinical Chemistry, vol. 57, no. 2, **(2011)**, pp. 196-204.

[6] J. Huh and M. Ackerman, "Using Collective Intelligence for Supporting Diabetes Patients", ACM Group 2010 Clorg Workshop Position Paper, **(2010)** October 8.

[7] M. Swan, "Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking", Int J Environ Res Public Health, vol. 6, no. 2, **(2009)** February 5, pp. 492–525.

[8] C. Brownstein, J. Brownstein, D. Williams, P. Wicks and J. Heywood, "The power of social networking in medicine", Nature Biotechnology, vol. 27, no. 10, **(2009)** October, pp. 888–90.

[9] P. Wicks, T. E. Vaughan, M. P. Massagli and J. Heywood, "Accelerated clinical discovery using self-reported patient data collected online and a patient-matching algorithm", Nature Biotechnology, vol. 29, no. 5, **(2011)**, pp. 411–4.

[10] C. Zhang, J. Sun, X. Zhu and Y. Fang, "Privacy and security for online social networks: challenges and opportunities", Network, IEEE, pp. 13-18.

[11] R. Steele, "Social media, mobile devices and sensors: Categorizing new techniques for health communication," Fifth International Conference on Sensing Technology (ICST), **(2011)**.

[12] CDC: Centers for Disease Control and Prevention. Online at www.cdc.gov.

[13] Y. Tong, J. Sun, S. S. M. Chow and P. Li, "Towards Auditable Cloud-Assisted Access of Encrypted Health Data", IEEE Conference on Communications and Network Security (CNS), **(2013)**.

[14] S. S. M. Chow, Y.-J. He, L. C. K. Hui and S. Ming Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment", ACNS, **(2012)**.

[15] C. Gao and N. Iwane, "Developing a Multi-trust Model for Multi-purpose Healthcare Social Networks", IEEE CCNC Workshop, **(2014)**.

[16] S. A. Moorhead, D. E. Hazlett, L. Harrison, J. K. Carroll, A. Irwin and C. Hoving, "A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication", Med Internet Res., vol. 15, no. 4, **(2013)**, pp. e85.

[17] J. Benaloh, M. Chase, E. Horvitz and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records", Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09), **(2009)**.

[18] S. Narayan, M. Gage and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure", Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10), **(2010)**.

[19] M. Li, N. Cao; S. Yu and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks", INFOCOM, 2011 Proceedings IEEE, **(2011)** April 10-15, pp. 2435-2443.

[20] L. Guo, C. Zhang, J. Sun and Y. Fang, "PAAS: A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks", IEEE 32nd International Conference on Distributed Computing Systems (ICDCS), pp. 224-233, **(2012)** June 18-21.

[21] J. Bethencourt, E. Shi and D. Song, "Signatures of reputation", Proceedings of the 14th international conference on Financial Cryptography and Data Security (FC'10), Radu Sion (Ed.). Springer-Verlag, Berlin, Heidelberg, **(2010)**, pp. 400-407.

Authors

Chunming Gao, Ph.D, is an Assistant Professor in the Medical Informatics Graduate Program at Michigan Technological University (MTU). He received his degrees of Masters and PhD in Computer Science at MTU in 2004 and 2011 respectively. Dr. Gao's areas of expertise are efficient algorithm designs, data management and security, and innovative HCI designs. He serves as a reviewer for a variety of IEEE and ACM conferences, such as SIGCHI, INFOCOM, and GLOBECOM. He also serves as an editorial board member of International Journal of Information Science and an editorial board member of Journal of Advanced Computer Science Technology.

Noriyuki Iwane, Ph.D, received the B.S., M.S. degrees from Hiroshima University in 1983 and 1986, respectively, and PhD from Kyushu Institute of Technology in 1997. He is currently an Associate Professor at Hiroshima City University. His research interests include human-computer interaction, learning science and educational engineering for human interface software.