International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 3: March 2016, pp 22-25. www.aetsjournal.com ISSN (Online) : 2394-6237

An Expectation Based Privacy Conserving for OSN

P. Chithraichelvi , M. Balamurugan

Abstract— An Expectation-Based Privacy-Conserving for Online Social Networks which enable two strangers create trust associations based on the existing 1-hop friendships. The anonymous close friend authentication scheme to protected the communication among OSN users. Apply the secure k-anonymity and collaborative filtering algorithm as the consecutively protocol to derive the encrypted social coordinate profile matching results. To develop the objective trust level and a result to evaluate the average trust level as the transitive whole value without cooperating each individual's trust level.

Index Terms— Online Social Networks (OSN), K-anonymity, Collaborative Filtering Algorithm, Security.

I. INTRODUCTION

Social networking on social media websites involves the use of the internet to connect users with their friends, family and acquaintances. Social media websites are not necessarily about meeting new people online, although this does happen. Instead, they are primarily about connecting with friends, family and acquaintances you already have in real life. The most well-known social media sites are Facebook, Twitter, Instagram and LinkedIn. These sites allow you to share photos, videos and information, organize events, chat, and play online games.

Often, each of your "friends" (Facebook) or "followers" (Twitter) will be connected to each other. Just like in real life, the connections between people aren't just one-on-one, but a network of connections. This online social network is useful for spreading information, pictures and videos and generally staying in touch with people you wouldn't normally get to interact with all the time. For example, you can easily set up a Facebook page with details and pictures of an event you might be planning, such as a school fete. The page allows you to easily send out invitations to other users of the social media site.

Just like other technology, for example mobile phones, social media is a very effective tool for connecting with people. However, there are a few privacy and security issues worth keeping in mind.

Social media sites have a variety of privacy settings you can adjust. This means you can control who sees your profile page and other information you share on the site. Some people do not mind having their personal information available for anyone to view online. However, we strongly recommend that you don't publish your home address and be mindful of posting other personal information about yourself (including your birthday), or others especially if you don't have their permission.

It's worth keeping in mind that if malicious parties have access to your full name and date of birth and using other available information – for example which suburb you live in - it is possible that you could fall victim to identity theft. Just as you wouldn't give your mobile number or bank details to anyone who asked, you should guard access to all the details of your social networking account.

Some people who use social media prefer only to allow people they have officially become friends with to see their profile and other information. It is important to note that for most social media sites (including Facebook) the default privacy setting is not to hide your information when you sign up. If you don't want your profile and other information to be seen by people who aren't a "friend" or "follower", you will have to check these settings and adjust them accordingly after you sign up.

The whole point of joining social media websites is to be in touch with your friends and family. "Friends" in the context of social media and Facebook in particular, has a specific meaning. For example, for you to interact online with a friend, family member or acquaintance either one of you must first send a "friend request" to the other and then have that request accepted. Once accepted, the technology recognizes you as "friends" and you can interact with each other online, so you can view the other person's profile page, see their pictures, and send them messages.

On the whole, nearly all the interactions that occur on social media sites are safe. However, you need to be conscious of your safety and the information you share. Everyone using social media should remember these safety tips:

- You are not obliged to accept a friend request from someone you don't know or do not want to be in contact with.
- Be respectful of the privacy of others when posting photos or videos of them, or mentioning them where others might read about it.
- Be aware that you can remove someone as a "friend" and/or block them from interacting with you even after you have "accepted" their friend request.
- Change your privacy settings so that only your friends can see your profile page and interact with you.

P. Chithraichelvi *(PG Student)*,Department of Computer Science and Engineering , Sri Sai Ram Engineering College, Chennai, India.

M. Balamurugan *(Assistant Professor)*,Department of Computer Science and Engineering , Sri Sai Ram Engineering College, Chennai, India.

1) Common Features of Social Networks

- *The ability to create a Profile page*–this is your main "home" on the network. Different networks offer varying abilities to personalize your page in terms of look and feel. They may also differ in terms of the types of information you would include, such as name, location, education, etc. Facebook, for example, asks for your relationship status (because it's more "social"), while on LinkedIn, which is primarily for professional use, does not.
- *A way to find and link to "friends" or connections*–The purpose of a network is connections, so facilitating a members' ability to find and connect to other people is important. Each network offers different types of search capabilities and once you've located a potential friend, you must send an "invitation" to invite them into your personal network.
- *Privacy Controls*–In most networks, your ability to access more detailed information about a person is based on their status as one of your connections; "friends" can see much more information than those who are not your "friends." You can control who is actually in your personal network by effectively managing who you invite into your network and whose invitations you accept.
- *The ability to send public and private messages*–In Ning and Facebook, you can communicate with your connections either by sending a private message or "writing on their wall." On LinkedIn, you communicate via person-to-person messages. Ning also provides Forums where members can interact with one another on specific topics (you're reading this in one of the Ning forums).

II. SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then the next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

The major part of the project development sector considers and fully survey all the required needs for developing the project. For every project Literature survey is the most important sector in software development process. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

A. Efficient Identity-Based Signatures Secure in the Standard Model

The only known construction of identity-based signatures that can be proven secure in the standard model is based on the approach of attaching certificates to non-identity-based signatures. This folklore construction method leads to schemes that are somewhat inefficient and leaves open the problem of finding more efficient direct constructions. We present the first such construction. Our scheme is obtained from a modification of Waters' recently proposed identity-based encryption scheme. It is computationally efficient and the signatures are short. The scheme's security is proven in the standard model and rests on the hardness of the computational Diffie-Hellman problem in groups equipped with a pairing.

B. Probabilistic Routing in Intermittently Connected Networks

We consider the problem of routing in intermittently connected networks. In such networks there is no guarantee that a fully connected path between source and destination exists at any time, rendering traditional routing protocols unable to deliver messages between hosts. There do however exist a number of scenarios where connectivity is intermittent, but where the possibility of communication still is desirable. Thus, there is a need for a way to route through such networks. We propose PROPHET, a probabilistic routing protocol for such networks and compare it to the earlier presented Epidemic Routing protocol through simulations. We show that PROPHET is able to deliver more messages than Epidemic Routing with a lower communication overhead.

C. PSAD: A Privacy-Preserving Social-Assisted Content Dissemination Scheme in DTNS

Content dissemination is very useful for many mobile applications, like instant messaging, file sharing, and advertisement broadcast, etc. In real life, for various kinds of time-insensitive contents, such as family photos and video clips, the process of content dissemination forms delay tolerant networks (DTNs). To improve the data forwarding performance in DTNs, several social-based approaches have been proposed, most of which leverage mobile users' social information, including contact history, moving trajectory, and personal profiles as metrics to design routing schemes.

However, although the social-based approaches provide better performance, the revealing of mobile users' information apparently compromises their privacy. Moreover, users' contents may only be shared with a particular group of users rather everyone in the system. In this paper, we propose the PSAD: a Privacy-preserving Social-assisted content Dissemination scheme in DTNs. We apply users' verifiable attributes to establish their social relationships in terms of identical attributes in a privacy-preserving way. Besides, to provide the confidentiality of contents, our approach enables users to encrypt contents before the dissemination process, and only allows users who have particular attributes to decrypt them. By trace-driven simulations and experiments, we show

the performance, privacy preservation, and efficiency of our proposed scheme.

D.Enforcing Access Control in Web-Based Social Networks

We propose an access control mechanism for Web-based Social Networks, which adopts a rule-based approach for specifying access policies on the resources owned by network participants, and where authorized users are denoted in terms of the type, depth, and trust level of the relationships existing between nodes in the network. Differently from traditional access control systems, our mechanism makes use of a semi-decentralized architecture, where access control enforcement is carried out client-side. Access to a resource is granted when the requestor is able to demonstrate of being authorized to do that, by providing a proof. In the paper, besides illustrating the main notions on which our access control model relies, we present all the protocols underlying our system and a performance study of the implemented prototype.

III. PROPOSED SCHEME

Apply the secure k-anonymity algorithm as the running protocol to derive the encrypted social coordinate profile matching results. To derive the objective trust level, a solution to calculate the average trust level as the transitive overall value without compromising each individual's trust level. Through security analysis and experimental evaluation, it has shown the security and feasibility of the proposed scheme.

- It spread existing relationships to multi-hop trust chains without cooperating recommender's identity privacy.
- Using polynomial secret sharing.
- Collaborative filtering and KNN classifier algorithm used for profile matching that is give the more security for personal data.

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

IV. ARCHITECTURAL DESIGN

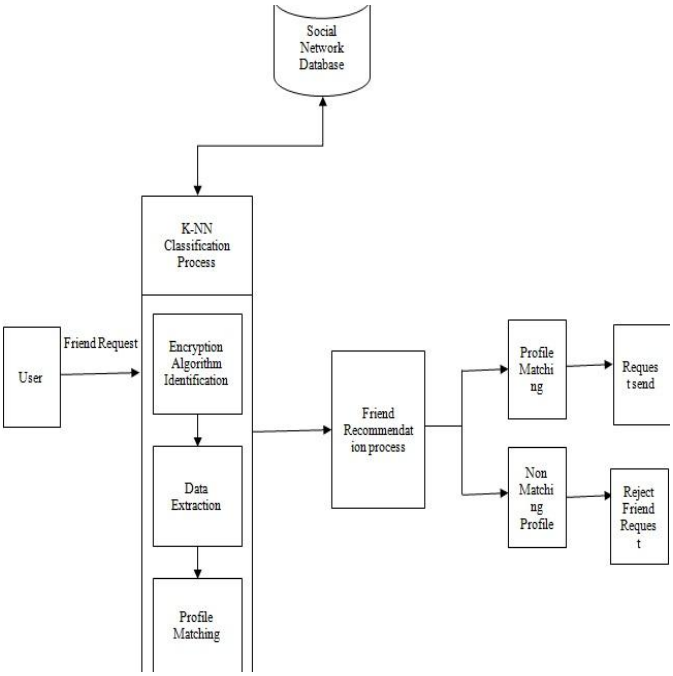

Fig.1 System Architecture

The major part of the project development sector considers and fully survey all the required needs for developing the project. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations. Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those

components, the relationships (e.g. the behavior) between them.

Design is a multi- step that focuses on data structure software architecture, procedural details, algorithm etc… and interface between modules. The design process also translates the requirements into presentation of software that can be accessed for quality before coding begins. Computer software design change continuously as new methods; better analysis and border understanding evolved. Software design is at relatively early stage in its revolution.

Therefore, software design methodology lacks the depth, flexibility and quantitative nature that are normally associated with more classical engineering disciplines. However techniques for software designs do exit, criteria for design qualities are available and design notation can be applied.

V. METHODOLOGY

Following are the most frequently used project management methodologies in the project management practice:

1. Data Collection
2. Lifestyle Analysis and Indexing
3. Friend Matching
4. User Impact Ranking
5. Feedback Control

1) Data Collection

I am collecting the data's from the social networks such as their habits, lifestyles etc…The collecting data's put into the server for further process.

2) Lifestyle Analysis and Indexing

Extracting the person lifestyles by implementing the k-anonymity algorithm and the user's lifestyle are analyzed based on their queries. After analyzing the lifestyle to be stored in the database. First the user can see the lifestyles of the user and then only they can see the user name (or) any other detail.

3) Friend Matching

After extracting the lifestyles from the Social Networks. We represent the similarity of other user's one by one in a graph construction method.

4) User Impact Ranking

Based on the graph method, ranking method will be displayed according to the user's Knowledge.

5) Feedback Control

By implementing all those above activities. We are adding a feedback mechanism to gather the user's query and further improve the friend recommendation process.

VI. CONCLUSION

A privacy-preserving trust-based friend recommendation scheme for online social networks, which enable two strangers establish trust relationships based on the existing 1-hop friendships. For privacy concerns, we first design the anonymous close friend authentication scheme to secure the communication among OSN users. Then, we apply the secure k-anonymity computation as the running protocol to derive the encrypted social coordinate matching results. To derive the objective trust level, we propose a solution to calculate the average trust level as the transitive overall value without compromising each individual's trust level. Through security analysis and experimental evaluation, we have shown the security and feasibility of the proposed scheme.

REFERENCES

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Syst., vol. 43, pp. 618–644, Mar. 2007.

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

[3] A. Squicciarini, F. Paci, and S. Sundareswaran, "PriMa: A comprehensive approach to privacy protection in social network sites," Ann. Telecommun., vol. 69, nos. 1/2, pp. 21–36, 2014.

[4] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 521–530.

[5] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1–6:38, Nov. 2009.

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

[7] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and my space," inProc. 13thAmer.Conf.Inf.Syst. 2007, p. 339.

[8] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks,"IEEE Commun. Survey Tutorials, vol. 13, no. 4, pp. 562–583, Dec. 2011.

[9] P. W. L. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems," in Proc. 14thEur. Conf. Res. Comput. Security, 2009, pp. 303–320.

[10] R. Dhekane and B. Vibber, "Talash: Friend finding in federated social networks," inProc. Linked Data Web, 2011, pp. 1–8.