Online Social Network for Recommendation System using SVM

Sandeep Konjere
Sinhgad Institute of Technology,
Lonavala,
Pune, India

V. N. Dhawas
Sinhgad Institute of Technology,
Lonavala,
Pune, India

ABSTRACT

To connected with world online communication and sharing information using the social network sites become a very famous in recent days. But it's very challenging job for social network site to provide the privacy and security. However, users need to become new friends to increase their social connections as well as to get information from specific group of people. Many online social networks (OSNs) using the past Friend recommendation method and which is very popular now days. There is a huge requirement to implement privacy-preserving friend recommendation methods for social networks as user privacy is the main motive nowadays. Online Social Networks(OSNs), not only get the focused from millions people to spend their time every day on social networks but also incredibly implement OSN clients social circles by using companion suggestions. This paper is motivated by need of friend proposal without showing privacy and security when using social networks. The goal in implementing of our system is to support users of OSN by securely creates trust with a stranger which is accomplishing by multi-hop recommendation process. Active OSN user privacy protection by using proposed method which is allowing them to enhanced their social networks. To carry out the secured social directed coordinating, existing framework use the secure kNN plan. Yet, with the help of KNN, distance based learning is not clear which sort of distance to use and their component to use to give the best results and calculation expense is very high. To overcome on this limitation and increased the outcomes precision, proposed framework utilizes SVM classifier for secure social coordinate matching. Through security analysis and trial outcomes, we demonstrate that the security, feasibility and precision of the proposed method is to have superior to anything existing one.

Keywords

Online, social network, multi hop relationship, trust value, privacy.

1. INTRODUCTION

Online social networks (OSNs) are widely used to connect with our friends circle. For example, Facebook, MySpace, and Twitter motivate users to keep in touch with their contacts, reconnect with old colleagues, and generate the new contacts with recommended users in view of shared components, for example, groups, leisure activities, intrigues, and covers in fellowship circles. From the previous few years we have seen tremendous increment in the utilization of OSNs, with about 300 OSN systems collect the data from more than an expansive part of a billion enrolled customers. Accordingly, OSNs stored an enormous scope of perhaps delicate furthermore, private data on clients and their associations. This data is typically private and expected the people are watching our collected information. Another way, the notoriety of OSNs keeps in unwavering clients as well as gatherings with rather antagonistic intrigues too. The enhancing and difficulty of design and utilization examples of OSNs unavoidably present security intrusion to all OSN clients as a consequence of data trade and publicly sharing on the Internet. It is within these lines not astounding that stories about security divided by Facebook and MySpace display over and again in standard media.

The Internet generates the various kind of information sharing systems, such as the Web. Now days, online social networks increased the strong popularity and are nowadays become the one of most popular sites on the Web. Online sharing network (OSNs) have been got tremendous growth in recent years such as Facebook, YouTube, twitter, and LinkedIn, which is generates huge amount of social data including personal and private data about each individual users. Security and privacy are main key parameters of online social network which produce the some limitation on sites. However, users want to make new friends to enlarge their social connections as well as to get the information from thousands of people. Extensively in the recent past Friend recommendation is a very important application in many online social networks (OSNs). Online social networks are organized around users not like the Web, which is largely organized around content. Social network analyses have enhance the research in developing various recommendation algorithms.

Various experts focused from different computer science disciplines have attempted to solve some of the issues that arise in OSNs and propose a different range of privacy solutions, including software tools and design principles. Some old methodologies have to ID-base recommendation, propose a friend by giving back a binary answer, ”yes” or ”no”, which bring down the probability of discovering friends of friends. Social networks are looking for; the majority of this sort of methods will neglect to amplify friendship more than two hopes. The homophily concept, OSN users are have social attachment with one another in small of their identical attributes. From one perspective, specifically asking proposals to outsiders or a non-dear friend uncovers Alice's identity, as well as uncovers her health condition and medical data. Surprisingly more terrible, traditional recommendation approaches offering personality to recommend to outsiders will shows OSN users social connections to the community, which hinder patients from using it, furthermore decreased the chance of arrange the multi-hop trust chain if one of OSN users on the chain gives back a wrong result. Then again, current methodologies can't afford the fine-grained and context-aware results automatically, because of the way that OSN users call for to decide the suggested companions in light of their own decisions on the recommendation request. As in our sample, Alice would need to request assistance from her companions who work in a hospital, yet not a truck driver. To overcome on this problem, we design system which think about how possible it is of using OSN users social attribute to implement the multi-hop trust chain in the presence of each context aware 1-hop trust relationship, where the greater part of trust connections are formed and strengthened by the shared social attributes.

Online social networks (OSNs) provide separate and simple techniques to correspond with each other's and obtain new friends on the social network. Badly, privacy of user and their data concerns brought up in the recommendation process obstruct the development of OSN clients companion circle. Some OSN clients want to secure their private information from the unaware users and show their companions' data to the general domain. To overcome on this issue, use privacy-preserving trust-based friend recommendation scheme for online social networks, which boost two outsiders design a trust connection in light of the multi-hop trust chain. For classification existing system uses KNN algorithm. To enhanced the performance of system, our system implements SVM algorithm for classification.

In this paper a study about the related work and its background is done in section II, the implementation details in section III where we seethe system architecture, modules description, mathematical models, algorithms and experimental setup. In section IV we discuss about the expected results and at last we provide a conclusion in section V.

2. LITERATURE REVIEW

In this paper [1], author implemented privacy preserving trust-based friend suggestion plan for online social networks. It authorizes two outsiders to create the trust connections based on the current 1-hop companionships. For secure methods, systems first make for the mysterious close friend validation scheme to secure the communication within OSN clients. At that point, assign the secure kNN algorithm as the running protocol to derive the encrypted social direction coordinating results. To examine the objective trust level, author goal to answer for ascertain the normal trust level as the transitive general quality without bargaining every individual's trust level, Author sure for the security and feasibility of the proposed plan by security analysis and evaluation methods.

Author proposed online social network like Orkut, YouTube, and Flickr are among the most standard social webon the Internet [2]. Users of these locals shape an informal community, which provide a suitable technique for sharing, organizing and search object in addition, contacts. The notification of particular areas allows looking at the characteristic of online social framework graphs allover scale. Understanding these charts is critical, both of them to upgrade existing systems and to layout new uses of online social community. This paper proves a large-scale measurement study of the structure of different online social sites. Author look at information gathered from four well known online social networks: Flickr, YouTube, Live Journal, and Orkut. Author crawled the freely available client links on almost every site, putting a large section of each social community's graph. By the author point of\ view his paper is the first study to analyze different online social networks at scale.

In this paper [3] author suggested to make a large-scale study to find out exactly how uncompromising the security leakage problem is in Facebook. Asa contextual analysis, authors target on use birth year, which is a common attributes of any users. In some area, author gives suggestion to calculate the birth year of more than 1 million Facebook users in New York City. Author again look at the accuracy of proposed techniques for a few classes of users: (i) very private users, who don't make their friends list open; (ii) Users who conceal their birth years however make their friend list public.

In this paper [4], author proves that it is unsurely knew how protection method and trust impact social collaborations among individual to individual communication destinations. An online scenario of two surely understood individual to individual communication destinations, Facebook andMySpace, used for most of trust and protection concern, along with by ability to publicly display information and create new connections. People from both locals reported comparative levels of security concern Facebook people communicate altogether r more unmistakable trust in the Facebook and people using it and were more willing to share identifying information. Results give alert that is in online communication, trust is not as imperative in the generating new connections as it is in eye to eye encounters. They similarly expose that in an online webpage, the presence of trust and the status to share information don't subsequently interpret into new social communication. These study demonstrates online connections can obtain in locals where seen trust and security assurances are weak.

In this paper [5], they first acknowledge extraordinary substance of trust measurement differentiated and QoS-based directing measurement. They provide an organized examination of the relationship between trust measurement and trust-based distinguishing in order to keep conventions the important logarithmic properties that a trust metric must have putting in mind the final motive to work effectively and preferably with particular summed up division vector on the otherhand connection state directing conventions in WANETs.

In this paper [6], authors try to overcome on this issue by presenting a decentralized method that can look into the social neighborhood of a client by finding friends of friends. Instead of just executing data about the user on the framework, the techniques believe on real friends and satisfactorily address the emerging privacy issues. In addition, authors prove VENETA, a mobile platform which, with different features, design new friend of friend detection algorithm.

In [7] author sure that last few years have seen remarkable improvement in the reputation of interpersonal organization frameworks, with Facebook being a model case. The starting control perspective withthe security protection arrangement of Facebook is especially not the same thusly existing access control perfect models as Discretionary Access Control, Role-Based Access Control, Capability Systems, and Trust Management Systems. This model work ventures in widening the cognizance of this area control perspective, by giving an entrance control exhibit that formalizes and wholes up the assurance protecting segment of Facebook. The system shown byan instance into a couple of Facebook-style casual organization frameworks, every single with an unmistakably particular access control instrument, so that Facebook is yet one instantiation of the model.

How Confidentiality and data handling care of imperative issues for social network users proves in [8]. Author is sure about confidentiality and data handling. In a real world, access control generation depends not depend upon the large range social networking provider but rather depend to be under the control of the client. In this paper, author implemented a functional, SNS stage autonomous arrangement, for informal organization clients to control their information. They generates the ideas that are sufficiently general to portray access control limitations for various SNS stages. Our construction modeling utilizes encryption to enforce access control for clients’ private data in light of their security inclinations. Creator have actualized model as a Firefox extension.

In [9] author proves the Online social network (OSNs),for example, Face book, MySpace, and Twitter have encountered large development lately. These OSNs offer striking method for online social collaborations and correspondences, additionally increased protection and security methods. Author also reduce the various issues with creates for the safety of user information and protection of OSNs. They also find out design conflicts in the mid of these and the customary configuration objectives of OSNs, for example, ease of use and amiability. Authors also design the security and privacy problems created by the core operations of OSNs and showed a few chances of using social network theory to mitigate these design conflicts.

3. IMPLEMENTATION DETAILS

3.1 Problem Definition

Some OSN users refuse to uncover their personal information and their companions’ data on the social website so to follow the privacy system propose a trust-based privacy preserving companion proposal plan for OSNs, in which any user can utilize their attributes to discover finding a friend, and set up social connections with outsiders by means of a multi hop trust chain. The main aim of protect is:

1) Find matched friends based on requested attribute.

2) Generate social relationship with strangers via multi hop chain.

3) Enhanced the security and privacy preserving.

4) Recommended friends are obtained with higher performance and security compared with other algorithms.

5) This algorithm gives higher efficiency and faster computation of friend recommendation process.

3.2 System Overview

The implementing goal of our proposed system is to assist OSN users by constitute of trust with strangers securely. It is accomplish by multi-hop recommendation process. The proposed method allows OSN users to enhance social circles with maintaining their identity privacy. As shown in Fig.1, system having various number of OSN users and central authority. Central authority is liable for parameter distribution. System maintains the secure communication channels between CA and each OSN users. These secure channels between OSN users and central authority are established by authentication and key exchange schemes. This scheme keeps the security of information distributed by CA. For the security purpose it keeps the public private key sets for OSN frameworks for all OSN users. The trust level in framework is the reliability trust with propagative property. These are binary values which generated by OSN server between Pairwise OSN clients, where 0 indicates less trust level and 1 speaks about most elevated amount with full trust. It is a context-aware trust, in which OSN users transmit proposal to different friends based on different context-aware queries. OSN users act the various numbers of roles in the system such as queried, friend, recommender, and destination users. Each user having different kind of social attributes that is social coordinates such as age, gender, designation etc., which are keep in vector at CA. For the proposed system we utilized the SVM scheme for to improve the performance and accuracy of the system. To achieve the secure social coordinate matching, existing system uses the kNN scheme. But with KNN, distance based learning is not clear which type of distance to use and which properties to use to get the best results and it has quite high computation cost. To overcome this limitation and improve the results accuracy, proposed system uses SVM classifier for secure social coordinate matching.

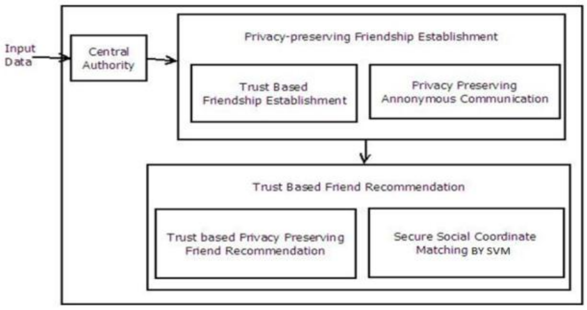
Input Data
Central Authority
Privacy-preserving Friendship Establishment
Trust Based Friendship Establishment
Privacy Preserving Annonymous Communication
Trust Based Friend Recommendation
Trust based Privacy Preserving Friend Recommendation
Secure Social Coordinate Matching BY SVM

Fig.1. System Architecture

3.3 Mathematical Model

System S = {U, P, R, G, PP, SP}
Input:

Browse Dataset:-

U = {u1, u2, u3,...un }

Where, U is a set of number of related papers and u1, u2, u3,....un is the number of papers.

Process

Central Authority

P = {P1, P2, P3,....Pn }

Where, P is represented as a set of Central

Process and P1, P2, P3Pn are the number of

central authority process.

Privacy Preserving Friendship Establishment

R = { r1, r2, r3,...rn }

Where, R is represent as a set of Privacy

Preserving Friendship Establishment Model

and r1, r2, r3,.....rn are number of Privacy

Preserving Friendship Establishment.

SVM Classifier

G = {g1, g2, g3,.....gn }

Where, G is represent as a set of SVM Classifier

and g1, g2, g3,.....gn are number of SVM

Classifier.

Trust Based Friend Recommendation

PP = {pp1, pp2, pp3,....ppn }

Where, PP is represent as a set of Trust Based Friend Recommendation and pp1, pp2,pp3,....ppn are number of Trust Based Friend Recommendation.

Output:

Final Output:-

SP = {sp1, sp2, sp3,....spn }

Where, SP is represent as a set of Final Output and sp1, sp2, sp3,....spn are number of finaloutput.

3.4 Algorithm

Algorithm1 Trustbased privacy preservingfriend recommendation

```
for$i$=1→$max\{hop\}$do
if$p_{i+1}$<$p_i$then
abort;
else;
$Q$→$R_i(F)$:Matching request;
 $R_i(F)$→Q:returnencrypted$\Psi_{Ri(F).Q:}$
Q → CA : Certificate $c_{D.S}$, encrypted$\Psi_{Ri(F).Q}$
$8:CA$→Q:Social coordinates
  $B_{Ri1}^{-1} Q_D^{-[1]}, B_{Ri2}^{-1}\ Q_D^{-\{2\}}$
:$Q$→R$_i$(F):Commitment $\tau_{Ri.Q'}$
  $B_{Ri1}^{-1} Q_D^{-[1]}, B_{Ri2}^{-1}\ Q_D^{-\{2\}}$
for j=1→|F$_{R1(F)}$ |do
M={$B_{Ri1}^{T} A_{Ri.j,}^{-[1]}, B_{Ri2}^{T}\ A_{Ri.j}^{-\{2\}}.\ B_{Ri1}^{-1}\ Q_D^{-[1]}, B_{Ri2}^{-1} Q_D^{-\{2\}}$}
 if$T_{Ri.Ri+1}$<$T_{Ri.Ri-1}$and$M_i$<$M_{i+1}$then
  Choose$max\{M\}$and derive$P_i$;
  Return $R_{i+1}$as next recommender;
  else
  Choose $R_i$ with lower M;
  end if
  end for
  $R_i$ →$S$:$R_{i+1}$,pk/sk keypair commitment $\tau_{Ri+1.Ri}$
  end if
  end for
```

Algorithm 2 SVM Algorithm

```
candidate SV = f closest pair from opposite classes g
while there are violating points do
Find a violator candidate SV = candidate SVS violator
if any p < 0 due to addition of c to S then candidate
   SV = candidateSV p
repeat till all such points are pruned
end if
end while
```

3.5 Experimental Setup

We use Java framework (version jdk 8) on Windows platform building the system, the development tool used is Net beans (version8.1). The system can run on any slandered machine, no specific hardware to run the application.

4 RESULTS

Figure 2 shows the Precision Graph comparison between system implemented by using secure KNN and system by using SVM. The propose system have high precision value than the existing system because.

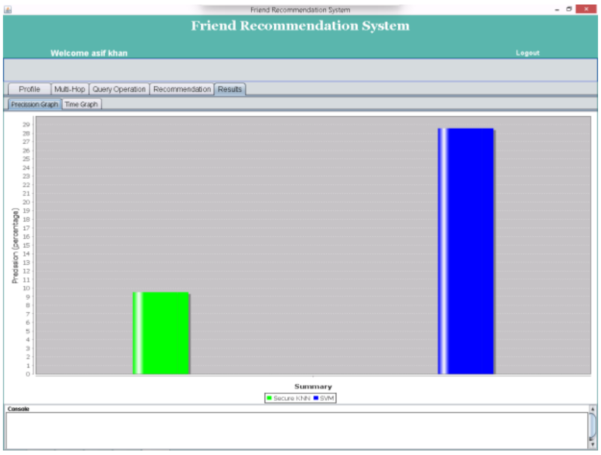

Fig 2: Precision Graph

Figure 3 shows the Time Graph comparison between existing system and proposed system, from the graph it is shown that Time required for the proposed system is less than the time required for the existing system.

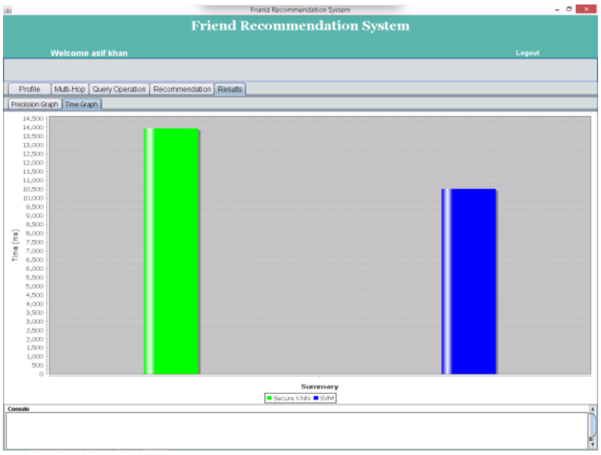

Fig 3: Time Graph

5 CONCLUSION

In this paper, system generates a privacy preserving trust-based friend recommendation method for online social networks, which authorize two unknown persons to set up trust connections in small of the multi hop trust friendship. For security point of view, first design the unknown best friend authentication plan to secure the correspondence among OSN users. At this point, we use the SVM classifier as the running protocol to evaluate the encrypted social direction coordinating results. To find out the objective trust score, framework use an answer for execute the average trust score as the transitive general value without trading off every people trust level. Go through the security investigation and exploratory evaluation, we design that the security, feasibility and accuracy of the proposed system is giving the better performance as compared to existing one.

6 REFERENCES

[1] Chi Zhang, ”A Trust-Based Privacy-Preserving FriendRecommendation Scheme for Online Social Networks”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURECOMPUTING, VOL. 12, NO. 4, JULY/AUGUST 2015.

[2] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B.Bhattacharjee, “Measurement and analysis of online socialnetworks,” in Proc. 7th ACM SIGCOMM Conf. InternetMeas., 2007, pp. 2942.

[3] R. Dey, C. Tang, K. Ross, and N. Saxena, “Estimating ageprivacy leakage in online social networks,” in Proc. IEEEConf. Comput.Commun., 2012, pp. 2836-2840.

[4] C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacyconcern within social networking sites: A comparison offacebook and myspace,” in Proc. 13th Amer. Conf. Inf.Syst., 2007, p. 339

[5] C. Zhang, X. Zhu, Y. Song, and Y. Fang, “A formal study oftrust based routing in wireless ad hoc networks,” in Proc.IEEE 29th Int. Conf. Comput. Commun ., Mar. 2010, pp.1-9.

[6] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking,” in Proc. IEEE Int. Conf. Wireless MobileComput. Netw.Commun., Oct. 2008, pp. 184-189.

[7] P. W. L. Fong, M. Anwar, and Z. Zhao, “A privacy preservation model for facebook-style social network systems,”in Proc. 14t Eur. Conf. Res. Computer. Security, 2009, pp.303-320.

[8] B. Carminati, E. Ferrari, and A. Perego, “Enforcing accesscontrol in web-based social networks,” ACM Trans. Inf.Syst. Security, vol. 13, no. 1, pp. 6:1-6:38, Nov. 2009.

[9] 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.