Trust Based Secure Friend Recommendation System for OSN Using C4.5

Pooja Yadav [1], Shital Nalgirkar [2], Sachin Kolekar [3]

[1], [2], [3] **Assistant Professor, Department of Computer Engineering,RSCOE, Pune**

Abstract

Online social networking (OSN) has grown in recent years; by using NSO, people share information, any kind of data or knowledge through the internet. Using NSO makes it easy to make friends and communicate with them. In NSOs, secrecy is an important factor for their identity and secure social relationships. privacy protection techniques known as a secure trust-based referral system for NSOs using C4. Where OSN users use their properties to find matching friends; it communicates with strangers using a trusted multi-step sequence.

Keywords: Online, Social network, multi-person relationship, Privacy, C4.5 Classifier

Introduction

Online Social Networking (OSN) is enjoying an amazing rise these days. OSN is a fundamental part of online life. By using OSN, users can share multimedia content with each other while receiving specific content. People post on OSN as videos, photos and personal blogs on their profile and this information is seen by all users or selected users of OSNs.

The most common function of OSNs is to connect to another user of that network.   users use these sites for various reasons and the main motivation of OSNs is to maintain relationships and communicate with each other. The most popular activities in NSOs are uploading videos, photos, and messaging each other. In this paper, we propose privacy protection techniques known as trust-based secure friend recommendation system for NSOs using C4.5 and the impact of trust and privacy on the Internet. In this article, we review the literature review in Section II, the proposed approach of the system, the mathematical model of the system, the algorithm, and the experimental setup in Section III, and finally draw conclusions in Section IV.

Literature Review

In this article [1], the author suggested that online social networks such as Orkut, YouTube, and Flickr are among the most popular local networks on the Internet. A client provides a convenient technique for sharing, organizing, and finding content on the LAN (Local Area Network). The main areas allow you to memorize the characteristics of the chart of online social characteristics on the whole scale. It is important to take these charts into account and modify current systems. This paper proposes a large-scale measurement analysis of the structure of different ones. The author of online social networks Flickr, YouTube, Live Journal and Orkut collected information. In this article, the author tracked the freely available client links on a website and obtained a large portion of the chart from each social community. The author focused on various large-scale online social networks.

In this article [2], the author points out that it is not really known how protection and trust concerns affect social collaboration within an individual-to-individual communication goal. People who use Facebook to communicate a more distinctive trust with each other and people who use it and have been more active in sharing identifying information. The result of communicating on social networking sites, trust is not necessary to make new connections as is the case with face-to-face encounters. This study illustrates the online connections that can be made locally and found that trust and security guarantees are weak.

In this paper [3], writer attempts to deal with this difficulty through offering a decentralized technique that may tests that social community of a customer for find out buddies of buddies. Alternatively, simply practice records approximately the customers of the framework, those strategies are relying on actual buddies. Satisfactorily addresses the privateness issues. Similarly, writer display VENETA, writer proposed a brand-new pal to pal detection set of rules in a cell platform which includes unique features.

In this paper [4] writer first of all recognizes a extremely good substance of consider dimension and Quality –of- Service (QoS) primarily based totally directing dimension. They indicate the distinction among consider dimension and consider-primarily based totally distinguishing, the essential logarithmic residences are used for consider metric that should have preserve in thoughts the very last purpose to paintings efficiently and ideally with unique summed up department vector however connection nation directing conventions in WANETs.

In paper [5] writer used a Find U, Find U is a primary protection making sure character profile, FindU is co-coordinating plans for cell casual groups. In FindU, a preliminary consumer can locate from a social affair of customers, whose profile fine fits with his/her, the chance of touch truely essential and insignificant records approximately the personal features of the taking a hobby customer is traded. A few extending stages of customer's protection are described, with lowering measures of exchanged profile data.

In paper [6], writer proposed the capacity of social networks through filtering the data. Collaborative Filtering (CF) is a appropriate method for structures on social networking web sites, due to the fact Collaborative Filtering gathers tastes of same customers. On walking CF on social networking web sites is quantitative estimation of consider among buddies. In this paper a framework of collaborative filtering on social community is proposed, on measuring consider elements through records-mining over a survey dataset supplied through the Facebook Project. A consider elements may be used as enter parameters withinside the CF set of rules. Facebook is taken as a case study.

In paper [7] writer proposed, now a day, speaking and sharing data on social networking is well-known however to offer privateness and protection is greater difficult. Due to those new buddies is extended on-line. Existing KNN plan is used for to perform the secured social directed coordinating. By the usage of KNN, distance-primarily based totally gaining knowledge of isn't always clean which kind of distance to apply and offers the fine outcomes and calculation fee could be very high. The proposed framework use SVM classifier for stable social coordinate matching. Security evaluation and trial outcomes, we show that the protection, feasibility and precision of the proposed technique and its miles to something current one.

In paper [8] writer indicates that OSNs is on-line carrier that is used to keep social relationships, for this cause multichip consider chain courting observed through 1 hop consider relationships used. A new method KNN is used to keep privateness. OSN customers can locate their matched buddies through making use of their attributes the usage of multi hop consider chain.

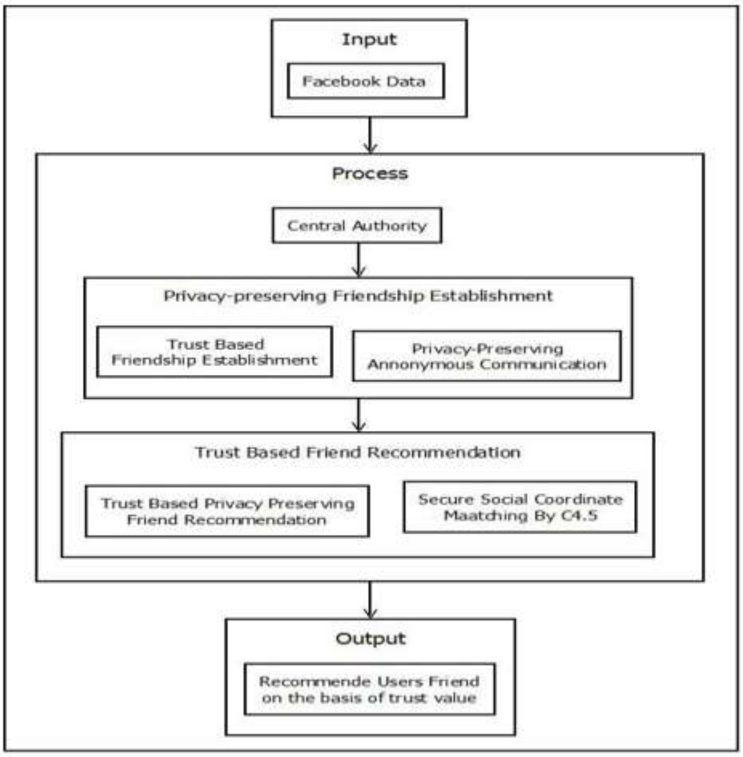
In paper [9], OSN's are used for to share information online. We propose two novel methods proximity measure in a privacy-preserving manner. First is holomorphic encryption scheme utilizing a universal hash function for efficiency purpose and second is protecting the source privacy through anonymous message routing and recommends friends accurately and efficiently. The proposed protocols provide a trade-off among security, accuracy, and efficiency; thus, users or the network provider can choose between these two protocols depending on the underlying requirements.

Proposed Approach

Problem Statement

For a given input of face book data, apply trust based secure friend recommendation system to provide users friend recommendation on the basis of trust values.

Proposed System Overview


Input
Facebook Data
Process
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 Maatching By C4.5
Output
Recommende Users Friend on the basis of trust value

To hide the identity and network address of OSN users, here we are assuming each OSN user has fully trusted friends. Example, user has several closest friends and they fully trust them. To hiding the identity network address and, users can route their packets to the destination via a specific trusted friend, and there by hide their identities with the help of their close friends.

To achieve the secure social coordination, here we apply secure KNN scheme and it modify. In this scheme, users' social coordinates can be formed into a set of binary vector B. Binary vector B is the social coordinate vector that contains query information, which can be any possible user's unique social coordinate in the OSN. The trust-based recommendation process should satisfy the above requirements, such that the trust chain could be set up according to the matching results and the trust requirement. The basic requirement of trust level derivation process is securely collecting the overall trust level based on each.

Modules of proposed system are as follows:

Privacy-Preserving friendship establishment:Privacy-preserving approach of the trust relationships between OSN users.

Trust Based Friend Recommendation:

The Trust Based Friend Recommendation consists oftwo sub protocols

Secure Social Coordinate Matching

Friend Recommendation Technique.

It is based on the matching outcomes of socialcoordinates and acceptance of true with relationships.

Trust Level Derivation:

It obtains objective trust level on particular trustchain.

Algorithm

Algorithm 1: C4.5 AlgorithmProcess:

C4.5 builds decision tree classification from a set of trainingdata.

Training data are set A = a1, a2, a3 … of already classified samples.

Each sample Si consist of a p-dimensional vector (X 1,i , X 2,i , X p,i ,) where Xj represent attribute values or features after sample, as well as class in which Si falls.

Base Cases: -

All the samples in the list belong to the same class. When this happens, it simply creates a leaf node for the decision tree saying to choose that class.

Node of the feature provides any information gain in this case C4.5 creates a decision node fighter up the tree using the expected value of the class.

Mathematical Model

System S is represented as S= {D, CA, T, R, O}

Input

Browse Dataset D= {d_1, d_2, d_3…d_n}

Where, D is a set of number of papers and d_1, d_2, d_3…d_n arethe number of papers.

Process

Central Authority

CA= {ca1, ca_2, ca_3…ca_n}

Where, CA is represented as a set of Central authority and ca_1,ca_2, ca_3…ca_n are the number of central authority process.

Privacy Preserving Friendship Establishment

T= {t0, t1, t2} Where, T is represented as a set of stepsperformed in this module.

t0= System set up

In this step, CA assigns the ID based public key and Private key pairs to each user in the system so that secret information of a user will not reveal.

ID= {ID1, ID2 ...IDn}

t1= Trust based friendship establishment

OSN users assigning different types trust levels T ϵ [0; 1]; to each one of their 1-hop friends.

F= {f1, f2, f3... fn}

Where, F is representing as a set of trust value assigns to multiple users.

t2= Privacy preserving anonymous communication

After t0 and t1, OSNs members in 1-hop initiate the anonymous communication.

The process is as follows:

$$Q \longrightarrow Q.j : E_{pk_{Q.j}}(PS^{\alpha}_{F.q}||sk_{PS^{\alpha}_{F.Q}}), exp, \sigma Q$$

$$Q.j \longrightarrow PS^{\beta}_{F.i} : PS^{\alpha}_{F.q}, n1, \sigma Q.j$$

$$PS^{\beta}_{F.i} \longrightarrow Q.j : PS^{\beta}_{F.i}, n2, \Phi_{\beta,\alpha}$$

$$Q.j \longrightarrow PS^{\beta}_{F.i} : \Phi_{\alpha,\beta}$$

Trust based friend recommendationR = {rp1, rp2}

The trust-based friend recommendation includes two majorsub protocols:

Secure Social Coordinate Matching

Friend Recommendation Process.

rP1= Secure Social Coordinate Matching

In this step, we apply the modified c4.5 classifier scheme, inwhich User’s Social Coordinates are formed into a set of binaryvector A.

rP2= Friend Recommendation Process

The trust-based recommendation process should satisfy andthe trust chain set up according to the matching results

Output:

Final Output

O= {o1, o2, o3... on}

Where, O is representing as a set of Final Output and o1, o2,o3…. o_n are number of final outputs.

Results & Discussion

Experimental Setup

The system is built using Java framework on Windows platform. The Net beans IDE are used as a development tool. The system doesn’t require any specific hardware to run; any standard machine is capable of running the application.

DataSet Used

For this system, we have taken online user's data which is retrieved from Facebook. Data is consisting of user details which have privacy policies. There is no need of any dataset.

Expected Result

In this section discussed the experimental result of the proposed system.

In table 1 shows the time required for the proposed system andexisting system.

System	Time Required
Existing system using KNN	428765ms
Proposed system using C4.5	357286ms

Following figure 2 shows the time comparison graph of theproposed system with the existing system.

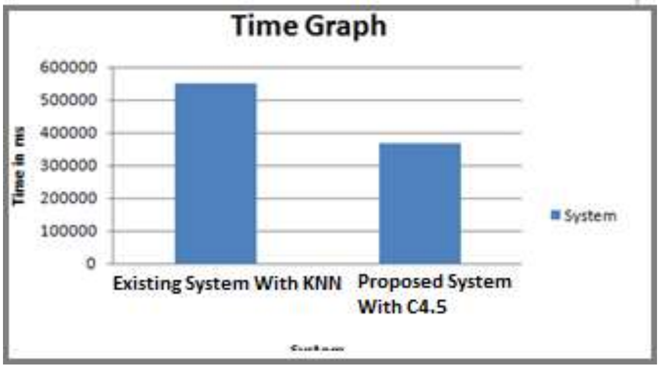


Fig. 2: Time Graph

Conclusion

In this study, for online social networks this system uses a privacy-preserving trust-based friend recommendation scheme. 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 sortof 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 C4.5 classifier for secure social coordinate matching. Through security analysis and trial outcomes, we demonstrate that the security, feasibility and precision of the proposed method are to have superior to anything existingone. Experimental results prove that the proposed system is more secure than the existing system, it performs better thanthe existing system.

References

1. Chi Zhang, “A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks”, IEEE transactions on dependable andsecure computing, 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 social networks,” inProc. 7th ACM SIGCOMM Conf. Internet Meas., 2007, pp. 2942.

3. C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacy concern within social networking sites: A comparison office book and myspace,” in Proc. 13th Amer. Conf. Inf. Syst., 2007, p. 339

4. M. von Arb, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking” Oct. 2008.

5. Y. Fang Y. Song, “A formal study of trust-based routing in wireless ad hoc networks,” in IEEE 29th Mar.2010.

6. N. Cao, S. Yu, “FindU: Privacy preserving personal profile matching in mobile social networks,” pp. 2435-2443 In IEEE Apr.2011.

7. W. Chen, “Social network collaborative filtering framework and online trust factors: A case study on Facebook,” pp. 266-273 in Proc. 5th Int. Conf. Digital Inf. Manage.,Jul. 2010.

8. Sandeep Konjere and V.N. Dhawas “Online Social Network for Recommendation System using SVM” International Journal of Computer Applications (0975 –8887) Volume 147 –No.14, August 2016

9. Nisha S Sarma, Anna Prathibha Shobak “Friend Recommendation in KNN Classification "international Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2016

10. Bharat K Samanthula, Lei Ken “Privacy Preserving and Efficient Friend Recommendation in Online Social Networks”, Transactions on Data Privacy Volume 8 Issue 2, August 2015 ISSN: 1888-5063 EISSN: 2013-1631