ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

An Expectation-Based Privacy-Conserving Friend Reference Scheme for Online Public Networks.

Aswini T[1], Anugraka I*, and L Lakshmanan.

Department of Computer Science Engineering, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

An Expectation-Based Privacy-Conserving Friend Reference Scheme for Online Public Networks which enable two strangers create trust associations based on the existing 1-hop friendships. The anonymous close friend authentication scheme to protect the communication among OSN users. Apply the secure KNN 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.

Keywords: IOT, KNN, PROPHET, OSN, BAYESIAN NETWORKS.

Corresponding author

INTRODUCTION

Computer security is also called as cyber security or IT security. It protects the system which contains information from theft or damage to the hardware or software, and to the information on them, as well as from disruption or misleading of the services which are provided.[1]It controls physical access to the hardware and also protecting against from harm that may come via network access, data and code injection, and due to some malpractice by operators, whether intentional or accidental, or may due to them being tricked into deviating from secure procedures.

Computer systems now includes a very wide variety of "smart" devices, including smart phones, televisions and tiny devices as part of Internet of Things - and networks include not only the Internet and private data networks, but also WiFi, Bluetooth and other wireless networks. Moreover Computer security covers all process and mechanism by which digital equipment, information and services are protected from the unintended or unauthorized access, changes or destruction and the process of applying security measures to assure integrity, availability and confidentiality of data in both transit and rests.

The only known construction of identity-based signature is that which can prove secure in the standard model is based on the approach of attaching the certificates to non-identity-based signatures. This folklore construction method leads to schemes which is somewhat inefficient and leaves the problem of finding more efficient construction. Our scheme is obtained from modification of Waters' recently proposed by identity-based encryption scheme. It is efficient and the signatures are short. [3]The scheme security is proven in the standard model and rest on the hardness of a computational Diffie-Hellman problem in a groups equipped with a pairing.

The problem of routing is intermittently connected networks. Because in those networks it is not guarantee that a fully linked path between a source and destination exists at any time, rendering that traditional routing protocols were unable to deliver messages between hosts. Therefore however a number of scenarios exists, where connectivity is intermittent , but where the possibility of communication is still desirable. Thus, there is a requirement for a way to route through such networks. We propose PROPHET, which is a probabilistic routing protocol for such networks and then compare it to the earlier presented [5]Epidemic Routing protocol through simulations. Then we show that the PROPHET is able to deliver more number of messages than Epidemic Routing with a lower communication overhead.

Content dissemination is very useful for mobile applications, like messaging, sharing files, and advertisement broadcast, etc. In real life also for various types of time-insensitive contents, such as family photos and videos, the process of content dissemination forms Delay Tolerant Networks (DTNs). [4]To improve the data forwarding performance in DTNs a lot of social-based approaches have been proposed, most of which leverage mobile user's social information which includes contact history, moving trajectory, personal profiles as metrics to design routing schemes.

On the other hand, users can accept the user-to-user interaction only if the users privacy issues of PHR are also well preserved. Here in this paper, we design a privacy preserving user-centric private matching scheme from the social perspective in a Health networks, where users use verified PHR to find or connect with other users who share the same situations and derive different user-centric results which is usually based on each and every user's own policy. In this scheme, the matching process guarantees both privacy and verifiability of users PHRs. Based on efficiency and security analysis, hereby we show that our work satisfies both privacy preservation and practicality requirements.

WORK RELATED

Trust and privacy in OSN

Lewis and Weigert [15], Trust is a critical determinant of sharing informations and developing new relationships. Hass[17], Mintz[16], Millions of people have joined social networking sites, adding profiles that reveals personal information. The reputations of social networking sites has been diminished by a number of incidents publicized by the news media. It is not possible to join a network of millions of people and trusting all of them. Since people are joining in networks and revealing information, where trust doesn't play a role in the use of social networking sites. Dwyer [7], Privacy within social networking sites is often not expected or is undefined.Chi Zhang et al.[6],OSNs such as Facebook, Twitter and Myspace, and have experienced exponential growth in recent years. These OSN offer attractive means of online social interaction and communications, but also raise privacy and security concerns. Meyerson and colleagues [3], Trust is also important for successful online interactions. Mayer, Davis, and Schoorman[5] said that Trust is the willingness of a party to be defenceless to the actions of another party based on the expectation where the other will perform a particular action which is important to the trustor, irrespective of the ability to monitor or control other party".Finally, Ziegler and Golbeck [13] argued strongly that there is evidence for the correlation between user's similarity and trust. Here, our learning approach for predicting user's inadequacy of accessing the specific data sets leverages, this scheme of similar users profile attributes indicates adequacy to access data.

Previous research on OSN

Acquisti and Gross [14] studied that Facebook, a social networking site began focused on colleges and universities, and also now includes schools and other organizations. Their studies about this have collected information which are given in user's profile from Facebook by using web crawler, and also survey through members. They also said that Facebook users reveal lots of information about themselves, but not aware of privacy issues or who can view their information in profile[14]. Natalia Dudarenko and colleagues [11] developed CP-ranking algorithm which is used for ranking the profiles or contacts based on their communication in OSN.Recently, Akcora and colleagues have worked on risk management measures on OSN for social network users [19] , demonstrating of considering the importance of risk is one of their dimensions and to fully understand the different types of OSN contacts and the social graph topology also may highly influence the exposure of user's personal or private profile information. Studies the very first popular OSN site, Friendster, Boyd and colleagues [20]describe that how members can create their profile with the intention of interacting or communicating news or messages about themselves to others. Boyd, used an ethnographic approach which reveals the possibility of unintended issues or consequences. The results of the study encourages further research to understand the development of relationships in the online social network environment and to analyse the reasons of different behaviour on different sites.

DESIGN OF OSN

Design of OSN is a multi- step process that focus on software architecture, data structureprocedural details, algorithm etc… and interface between modules. The design process also translate the requirements into presentation of software that can be accessed for quality before coding. [7]Computer software design change continuously as new methods; better analysis and border understanding evolved. Software design is now at relatively early stage in its revolution.

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

Input Design

The input design is the connection between the information system and the user(fig.1). It comprises the developing procedures and specification for data preparation and these steps are necessary to put transaction data in to a usable form for processing that can be achieved by examining the computer to read data from a written or printed document or it can occur by having people interacting with data directly into the system.

The input design focuses on to control the amount of input required, the errors, avoiding delay, avoiding unwanted steps and keeping the process simple. So the input is designed in such a way so that it provides security and it is easy to use with retaining the privacy. Input Design considers the following things:

1. What data should be given as input?
2. How the data should be coded?
3. The dialog to guide the operating personnel in providing input.
4. Methods to prepare input validations and steps to follow when errors occurred.

Output Design

A quality output meets the requirements of the end user and presents the information clearly for their requirement. In any system, the result of processing is communicated to the users and to other system through outputs. In this output design (fig.2), it is determined that how the information is to be displaced for user's immediate need and also the hard copy output. It is the most important to direct source information to the user. Moreover efficient and intelligent output design enhances the system's relationship to help user decision-making.The output form of an information system should establish one or more of the following objectives.

1. Convey information about past activities, current status or projections for the Future.
2. Signal important events, opportunities, problems, or warnings.
3. To trigger an action.
4. To confirm an action.

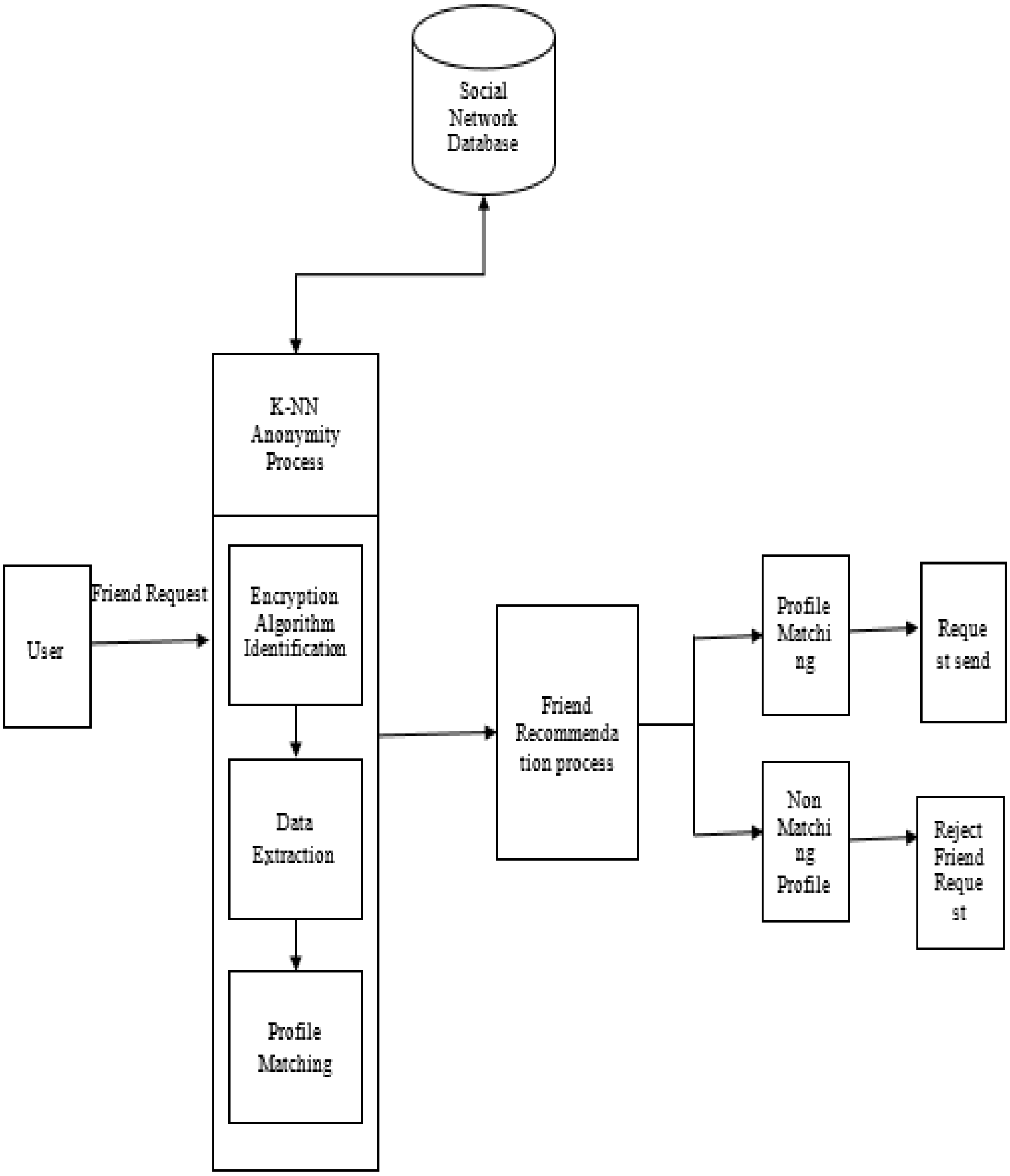

Figure 1: Design of OSN

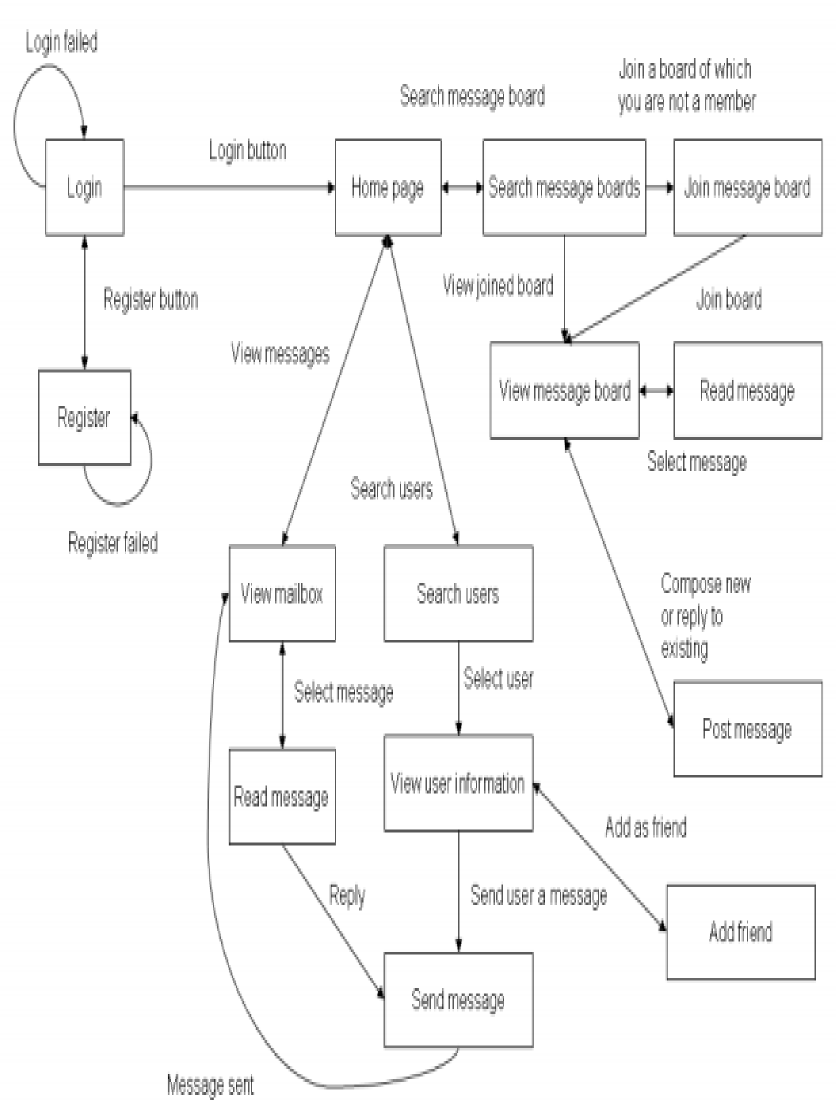

Figure 2: Proposed system architecture

The data's which are collected is put into the server for further process. 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. It identifies the fake users and also views the first post of user time line. After extracting the lifestyles from the Social Networks. We represent the similarity of other users one by one in a graph construction method. Based on the graph method ranking will be displayed according to the users Knowledge. By implementing all those above activities, we are adding a feedback mechanism to gather the users query and further to improve the friend recommendation process. As a result the number of friend request gets moderated when compared to other social networking sites (fig.3).

ALGORITHM SPECIFICATION

K-NEARESTNEIGHBOR CLASSIFICATION METHOD

K-NN is a type of instance-based learning or lazy learning, where the function is approximated locally and all the computational process are deferred until classification. This algorithm is simplest when compared among all machine learning algorithms. The neighbours are taken from a group of objects for which the class or object property value is known.

Algorithm Steps

```
STEP 1: BEGIN
 STEP 2: Input: D = {($x_1$, $c_1$), . . . , ($x_N$ , $c_N$ )}
 STEP 3: x = ($x_1$. . . $x_n$) new instance to be classified
 STEP 4: FOR each labelled instance ($x_i$, $c_i$)  calculate d (xi, x)
 STEP 5: Order d ($x_i$ , x) from lowest to highest,
  (i  = 1. . . N)
 STEP 6: Select the K nearest instances to x: $D^k_x$
 STEP 7: Assign to x the most frequent class in $D^k_x$
STEP 8: END
```

BAYESIAN NETWORKS PROBABILITY CALCULATION ALGORITHM

A Bayesian network is an acyclic directed graph, where the nodes represents variables and the edges represents dependencies. Bayesian networks, also known as belief net- works, belong to the family of probabilistic graphical models. These probabilistic models are used to represent knowledge about an uncertain domain.

Algorithm Steps

STEP 1: Input: The database of the friendship relations between users in the social network; the database of the users' m attributes.

STEP 2: Construct the social network graph for the user by the database of the relation. Consider that all user's existing friend are Vt ; the set of the persons in Vt who have already been friends of user is Vf ; the set of the other n persons in Vt will be the candidates for the friend recommendation system and we mark it as Vc .

STEP 3: Estimate the probability P(x1) that Vt will be friend of the user for attribute i by the statistical result of Vt and Vf . For all m attributes, we get
{P (x1), P (x2), … , P (xm)}.

STEP 4: Calculate the probability P for each of the n candidates in Vc using Equation (5) and {P (x1), P (x2),… , P (xm)}.

STEP 5: Sort the n candidate by the value of probability P.

STEP 6: Return: Top k of the sorted n candidates as the list of friend recommendation result.

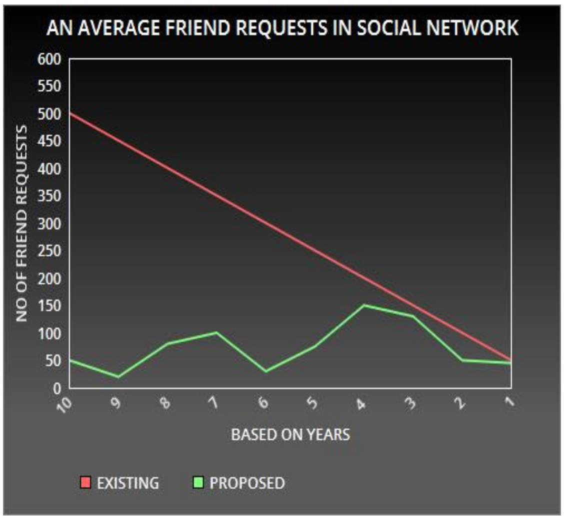

Figure 3: Maximum Number of Friend Requests in Existing System Compared with Proposed System

CONCLUSION

A privacy preserving trust in friend recommendation scheme for OSN, which enables two strangers trust relationships based on existing 1-hop friendships. For privacy concerns, we first design the anonymous close friend authentication scheme to secure the communication among Online Social Network(OSN) users. Then here we apply the secure KNN computation is running protocol to derive encrypted social coordinate matching results. For deriving the objective trust level, we proposed a solution in this scheme to calculate the average trust level as the transitive overall value without compromising each individual's trust level. The results of this paper encourage further research in the effort to understand the development of relationships in the online social environment.

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," in Proc. 3rd ACM Int. Conf. Web Search Data Mining, 2010, pp. 251–260.

[3] Meyerson, D., Weick, K. E., & Kramer, R. M. (1996) "Swift trust and temporary groups," in R. M. Kramer, Tyler, T. R. (Ed.) Trust in organizations: Frontiers of theory and research, Thousand Oaks, CA: Sage Publications.

[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] Mayer, R. C., J. H. Davis, and F. D. Schoorman (1995) "An Integrative Model of Organizational Trust," The Academy of Management Review (20) 3, pp. 709-734.

[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," in Proc. 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. 14th Eur. Conf. Res. Comput. Security, 2009, pp. 303–320.

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

[11] Natalia Dudarenko, Juwel Rana, Kåre Synnes, "Ranking Algorithm by Contacts Priority for Social Communication Systems" Third Conference on Smart Spaces, ruSMART 2010, and 10th International Conference, NEW2AN 2010, pp 38-49.

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

[13] Ziegler C-N, Golbeck J (2007) "Investigating interactions of trust and interest similarity". Decis Support Syst 43(2):460– 475

[14] Acquisti, A. and R. Gross. (2006) "Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook." Proceedings of the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006.

[15] Lewis, J. D. and A. Weigert (1985) "Trust as a Social Reality," Social Forces (63) 4, pp. 967-985.

[16] Mintz, J. (2005) "Friendster's 'Eww' Moment," in The Wall Street Journal, pp. B1.

[17] Hass, N. (2006) "In Your Facebook.com," in The New York Times, pp. 30-31. New York.

[18] 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.

[19] Akcora C, Carminati B, Ferrari E (2012) Privacy in social net- works: how risky is your social graph? In: 2012 IEEE 28th international conference on data engineering, IEEE, pp 9–19.

[20] Boyd, d. (2004) "Friendster and Publicly Articulated Social Networks". Proceedings of the SIGCHI Conference on Human Factors and Computing Systems, Vienna, Austria, 2004.