IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

Trust-based Collaborative Privacy Management in Online Social Networks

Sridharan M[1], Siva Ragavan S[2], Ranjith Kumar R[3], Arvind K A[4], Praveen Kumar S[5]

Assistant Professor, Department of Information Technology, Panimalar Engineering College, Chennai, India[1]

Student, Department of Information Technology, Panimalar Engineering College, Chennai, India[2,3,4,5]

Abstract: Online interpersonal organizations have now turned into the most famous stages for individuals to impart data to others. Alongside this, there is a genuine danger to people's security. One protection chance originates from the sharing of co-possessed information, i.e., when a client shares an information thing that includes numerous clients, a few clients' security might be imperiled, since various clients by and large have distinctive suppositions on who can get to the information. Step by step instructions to plan a shared administration component to manage such a security issue has as of late pulled in much consideration. In this paper, we propose a trust-based instrument to acknowledge community oriented security management. The trust esteems between clients are utilized to weight clients' feelings, and the qualities are refreshed by clients' protection misfortune. In addition, the client can make an exchange off between information sharing and security safeguarding by tuning the parameter of the proposed component. We define the choosing of the parameter as a multi-furnished desperado issue and apply the upper certainty bound arrangement to tackle the issue. Reenactment comes about exhibit that the trust-based instrument can urge the client to be thoughtful of others' protection, and the proposed crook approach can bring the client a high result.

Keywords: Protection, proposed, security, clients

I. INTRODUCTION

A. Purpose of system

The main aim of this project is to provide an trust based privacy management in OSN.

B. Project scope

In this paper we study the privacy issue caused by the sharing of co-owned data in OSNs. To help the owner of data collaborate with the stakeholders on the control of data sharing, we propose a trust-based mechanism. When a user is about to post a data item, the user first solicits the stakeholders' opinions on data sharing, and then makes the final decision by comparing the aggregated opinion with a pre-specified threshold. The more the user trusts a stakeholder, the more the user values the stakeholder's opinion.

C. Trust based approach

Using this requirement, our application provides high service with efficiently. Software requirements deal with defining software resource requirements and pre-requisites that need to be installed on a server that provide optimal functioning of an application.

II. LITERATURE SURVEY

A.Privacy and security for online social networks: challenges and opportunities security.

Online social networks such as Facebook , MySpace, and Twitter have experienced exponential growth in recent years. These OSNs offer attractive means of online social interactions and communications, but also raise privacy and security concerns. In this article we discuss the design issues for the security and privacy of OSNs. We find there are inherent design conflicts between these and the traditional design goals of OSNs such as usability and sociability. We present the unique security and privacy design challenges brought by the core functionalities of OSNs and highlight some opportunities of utilizing social network theory to mitigate these design conflicts.

B. Information security in big data: Privacy and data mining.

The growing popularity and development of data mining technologies bring serious threat to the security of individual,'s sensitive information. An emerging research topic in data mining, known as Privacy-Preserving Data Mining (PPDM), has been extensively studied in recent years. The basic idea of PPDM is to modify the data in such a way so as to perform data mining algorithms effectively without compromising the security of sensitive information contained in the data. Current studies of PPDM mainly focus on how to reduce the privacy risk brought by data mining

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 3, March 2019

operations, while in fact, unwanted disclosure of sensitive information may also happen in the process of data collecting, data publishing, and information (i.e., the data mining results) delivering. In this paper, we view the privacy issues related to data mining from a wider perspective and investigate various approaches that can help to protect sensitive information. In particular, we identify four different types of users involved in data mining applications, namely, data provider, data collector, data miner, and decision maker.

C. A framework for categorizing and applying privacy-preservation techniques in big data mining.
To protect sensitive information in mined data, researchers need a way to organize a variety of ongoing work. The Rampart framework categorizes protection approaches and encourages interdisciplinary solutions to the growing variety of privacy problems associated with knowledge discovery from data.

D. Privacy-preserving wireless communications using bipartite matching in social big data.
The enhanced wireless data transmissions have enabled the dramatical improvement of the service deployment, such as social networks and big data applications. The multi-channel wireless communication is one of the approaches for disseminating information when the user popularity is large in the dynamic and heterogeneous wireless networking environment. *Channel Scheduling Controllers* (CSCs) are vital components in data transmissions, which use *Nodes* to arrange real-time task scheduling. However, a fixed communication scheduling can hardly meet the requirement of the higher-level privacy protections because of the conflict caused by the performance and security demands. To address this issue, this paper proposes a novel algorithm using communication management techniques for enhancing the security of the systems and supporting applications with real-time constraints. The experimental results depict that the proposed approach can reduce the security cost by up to 32.62% and 23.37% on average, respectively, compare to the traditional methods.

III. System Analysis

A. Existing System
Online Social Networks (OSNs) are the trust relationship between users. The User would have been explored to protect sensitive data of users or to verify the user's identity. They are categorized studies on social trust based on three criteria, namely trust information collection, trust evaluation, and trust dissemination.

B. Proposed System
A trust-based mechanism is proposed for collaborative privacy management in OSNs. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more considerate of other users' privacy .The trust-based mechanism can encourage the user to be considerate of others' privacy, and the proposed bandit approach can bring the user a high payoff.

IV. System Design

A. System Architecture
Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

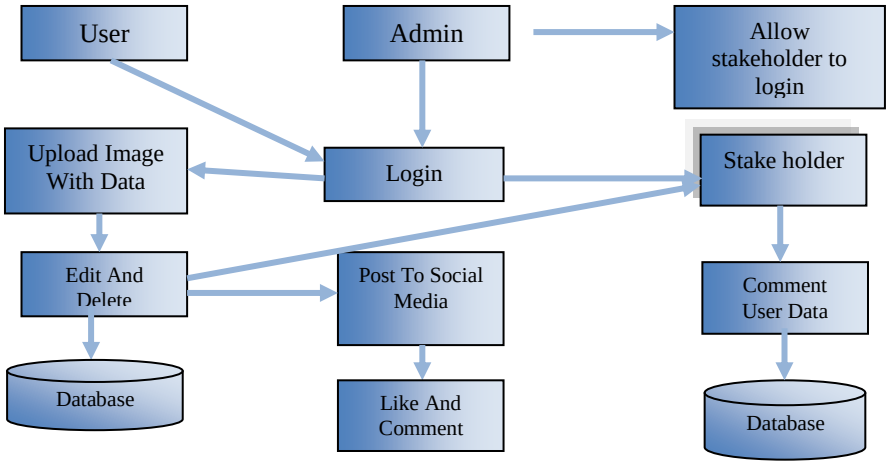

Fig. 1 Architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

V. MODULES

The proposed system consists of four main modules. They are:

- Authentication
- Register user details
- Upload image with content
- Send to stakeholder or post directly

A.Authentication

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password.

B.Register user details.

The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself.The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself.

C. Upload image with content

User uploads the image with data which he/she is going to post and stored in the database.

D. Send to stakeholder or post directly

The user post the image directly or send to stakeholder for her opinion

CONCLUSION

In this paper we study the privacy issue caused by the sharing of co-owned data in OSNs. To help the owner of data collaborate with the stakeholders on the control of data sharing, we propose a trust-based mechanism. When a user is about to post a data item, the user first solicits the stakeholders' opinions on data sharing, and then makes the final decision by comparing the aggregated opinion with a pre-specified threshold. The more the user trusts a stakeholder, the more the user values the stakeholder's opinion. If a user suffers a privacy loss because of the data sharing behavior of another user, then the user's trust in another user decreases. On the other hand, considering that the user needs to balance between data sharing and privacy preserving, we apply a bandit approach to tune the threshold in the proposed trust-based mechanism, so that the user can get a high long-turn payoff which is defined as the difference between the benefit from posting data and the privacy loss caused by other users. We have conducted simulations on synthetic data and real-world data to verify the feasibility of the proposed methods. Simulation results show that compared to directly posting data without asking others for permission, a user will suffer less privacy loss if he/she always considers other users' privacy. And by applying the proposed UCB policy to determine the threshold, the user can get higher payoffs than setting the threshold to a fixed or random value.

REFERENCES

[1]. N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," IEEE Transactions on Information Forensics and Security, vol. 9, no. 8, pp. 1251–1263, Aug 2014.

[2]. W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," ACM Computing Surveys, vol. 45, no. 4, pp. 47:1–47:33, August 2013. [20]. Y. Tang, H. Wang, and W. Dou, "Trust based incentive in p2p network," in IEEE International Conference on E-Commerce Technology for Dynamic E-Business, September 2004, pp. 302–305.

[3]. N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," Social Network Analysis and Mining, vol. 7, no. 1, p. 7, February 2017.

[4]. Y. Sun, C. Zhang, J. Pang, B. Alcalde, and S. Mauw, "A trust-augmented voting scheme for collaborative privacy management," J. Comput. Secur., vol. 20, no. 4, pp. 437–459, July 2012.

[5]. V. Buskens, "The social structure of trust," Social Networks, vol. 20, no. 3, pp. 265–289, 1998. [24]. S. Nepal, W. Sherchan, and C. Paris, "Strust: A trust model for social networks," in 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 2011, pp. 841–846.

[6]. O. Richters and T. P. Peixoto, "Trust transitivity in social networks," PLOS ONE, vol. 6, no. 4, pp. 1–14, 04 2011.[Online].. Available: https://doi.org/10.1371/journal.pone.0018384.

[7]. G. Liu, Y. Wang, M. A. Organ et al., "Trust transitivity in complex social networks." in AAAI, vol. 11, no. 2011, 2011, pp. 1222–1229.

[8]. J. Du, C. Jiang, K. C. Chen, Y. Ren, and H. V. Poor, "Community structured evolutionary game for privacy protection in social networks," IEEE Transactions on Information Forensics and Security, vol. PP, no. 99, pp. 1–1, 2017.

[9]. L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? a contract theoretic approach," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1256–1269, 2015.

[10]. Bubeck and N. Cesa-Bianchi, "Regret analysis of stochastic and no stochastic multi-armed bandit problems," Foundations and Trends R in Machine Learning, vol. 5, no. 1, pp. 1–122, 2012