Available online at www.sciencedirect.com

ScienceDirect

Cognitive Systems Research 52 (2018) 629–639

Cognitive Systems RESEARCH

www.elsevier.com/locate/cogsys

Research and application of virtual user context information security strategy based on group intelligent computing

Xian Tan [a,b], Fasheng Yu [a,*]

[a] Communication & Journalism College, Central China Normal University, Wuhan, China
[b] College of Literature and Communication, Hubei University for Nationalities, Enshi, China

Received 20 June 2018; received in revised form 31 July 2018; accepted 13 August 2018
Available online 23 August 2018

Abstract

This article first introduced the current technology of the privacy protection model, and analyzed their characteristics and deficiencies. Afterwards, from the point of view of revenue, the shortcomings of the traditional privacy protection model have analyzed through the group intelligent computing method. Based on this, this paper proposes a research and application of virtual user information of security strategy based on group intelligent computing, through the collection of visitor's private information historical access data, intelligent calculation of the strategy group between the visitor and the interviewee. The setting of the threshold of the visited person can protect the privacy information of the user more effectively. In this paper, the implementation flow, algorithm implementation process, and specific architecture design of the proposed virtual user of privacy protection model based on group intelligent computing are introduced respectively. The specific algorithms include PCA, BP neural network, and genetic algorithm. Finally, the proposed privacy has verified through experiments. Protection model can protect user privacy more effectively than traditional privacy protection model. In the future, we will further expand and improve the privacy protection model of virtual users based on group intelligent computing, including considering the dynamic and inconsistency of access to the privacy information, that is, accessing different private information will produce different overlay effects and parallelism. We will also study how to apply this model to actual systems such as shopping websites and social platforms, and use commercial data to evaluate the performance of the model and further improve it.

Keywords: Virtual user context; PCA; BP neural network; Genetic algorithm; Group-intelligent-computing; Public-opinion-dissemination

1. Introduction

In recent years, the rise of Web 2.0 technology has further expanded the interaction between users and computers and improved the user experience, but it has also accelerated the growth of Internet information resources. Massive information brings more choices to the Internet users. At the same time, it also has to spend a lot of time and energy to find information that they are interested in or useful for themselves from the huge information database, which leads to information. "Overload" and "information explosion" issues. With the rapid development of mobile Internet technology and the widespread application of mobile social networking platforms, social mobility on the Internet has become a general trend. The mobile social network realizes the degree of intimacy between people and maximizes the user's information for business. However, due to the existence of a large number of loopholes in network

* Corresponding author at: Communication & Journalism College, Central China Normal University, Wuhan, China.
E-mail address: hbht@qq.com (F. Yu).

https://doi.org/10.1016/j.cogsys.2018.08.016
1389-0417/

technology and other related factors, the user information security is facing a huge threat (Ball, Qela, & Wesolkowski, 2016; Mijumbi et al., 2016). The establishment of user information of security protection strategy under the mobile social network is an urgent task. Mobile social networks are based on traditional social networks, incorporate modern new mobile network technologies to provide users with convenience, and personalized services, thereby embodying the innovative and authentic characteristics of mobile social networks. User information security refers to the meaning of the user's security status level and information protection level. It refers to the user's awareness of information disclosure and the user's protection actions and measures taken by the user. The user information under the mobile social network merges the natural information of the traditional user with the behavior information of the social network. All information closely related to the user can be called user information. As the mathematical model of neural network has made great progress, the mathematical model is improved and established by using special data mining method (Yu and Li, 2018).

Anonymity is one of the commonly used privacy protection methods. Its main principle is to use the anonymous method instead of using the user's real identity information to obtain or use the user's private information, so that others cannot use the collected information. The user's real identity has linked to achieve the purpose of protecting user privacy. According to different objects, anonymity mainly includes node anonymity and edge anonymity, and the combination of the two can achieve better privacy protection effect. The main idea of node anonymity is that after the attacker selects an attack target, the probability of leaking the privacy is less than 1/K when the match has identified in the anonymized social network (Mijumbi et al., 2016). The main method is to cluster all the nodes in the social network into several clusters. Super-nodes, where each super-node contains at least K nodes and the nodes in the super-node are indistinguishable from each other. The disadvantage of node K-anonymity is its low efficiency, which is not suitable for large networks. Edge K-anonymity is similar to the main idea of node K-anonymity. The main method is to form a sub-graph by some edges. When a visiting attacker uses the specific sub-graph where the target is located as background knowledge for privacy attack, there are at least K in the social network (Ali, Khan, & Vasilakos, 2015). The sub-graphs can be used as candidates, so that the probability that the target subgraph causes privacy leak is lower than 1/K. Since Sweeney (Zhang et al., 2014) proposed K-anonymity technology to protect user privacy information in 2002, experts and scholars have conducted in-depth research on anonymous methods. Mallya, Kothari and Mehta (2018) proposed a method to solve the problem of data privacy protection of Web query services under personalized conditions, based on the impact of quasi-identifiers on sensitive attributes in previous K-anonymity algorithms. The data privacy protection of the query service directly uses the anonymized data to calculate the utility of the quasi-identifiers on the sensitive attributes and improve the utility matrix to achieve better protection of data privacy and security. Li and Mao (2015) proposed a privacy protection method for user collaboration without anonymous area because of the location-based K-anonymous method based on the central server based on the privacy leakage problem caused by wide application of location-based services. CoPrivacy achieves the effect of K-anonymity without using anonymous areas, and improves the overall performance of anonymous systems, simplifying the query processing process of service providers. Manvi and Shyam (2014) have proposed a track privacy protection of PrivateCheckIn for wireless network check-in service nickname user's trajectory privacy leakage problem, designed a check-in sequence caching mechanism, and built a prefix tree for the cached check-in sequence. Prune and reconstruct the prefix tree to form a K-anonymous prefix tree and traverse the K-anonymous prefix tree to obtain a K-anonymity check-in sequence to achieve the privacy protection effect of the track K-anonymity. However, there are many imperfections in anonymous privacy protection methods. In essence, the protection object in the anonymous protection method is not the privacy information itself, but the identity of the private information owner. The protection of privacy information has achieved by hiding the identity information of the private information owner. Therefore, once the privacy information owner's identity information has leaked through other channels or methods, all of its private information will be revealed. In addition, since the background information obtained can have analyzed, and attacked. Anonymous protection cannot effectively resist the consistency attacks, and background knowledge attacks, resulting in the vulnerability of anonymous comparison. The second main technical means of privacy protection is based on access control privacy protection. This method is mainly to properly extend the traditional information security-oriented access control methods to meet the requirements of protecting user privacy information. Terzi, Terzi, and Sagiroglu (2015) have proposed a method to protect digital privacy information by studying the application of access control in the medical field to improve the security of digital information in the medical field. In the ubiquitous computing environment, the user's willingness to protect privacy can be achieved through the 616-computer journal that allows users to formulate privacy-oriented access control policies (privacy policies) in 2016. The unified expression of the privacy policy and its execution mechanism can be effective. A lightweight and conditional privacy protection authentication and access control scheme suitable for ubiquitous computing environments to solve the problem of providing services only for legitimate users in ubiquitous computing environments and users wishing to obtain privacy. Lu et al. have proposed a computational framework SPOC for security and privacy protection in mobile medical emergencies.