The Privacy Concerns and User Expectations with a Corresponding Data Publishing Mechanism

[1]Peetha V S V D M Nagendra Pavan Kumar, Mtech Student,
[2]V Rajesh Babu, Assistant Professor,
[1,2]Dept of CSE, Eluru College of Engineering and Technology,
Duggirala(V), Pedavegi(M), Eluru, Andhra Pradesh.

ABSTRACT

Due to the close correlation with individual's physical features and status, the adoption of Cyber-Physical Social Systems (CPSSs) has been inevitably hindered by users' privacy concerns. Such concerns keep growing as our bile devices have more embedded sensors, while the existing countermeasures only provide incapable and limited privacy preservation for sensitive physical information. Therefore, we propose a novel privacy preservation framework for CPSSs.We formulate both the privacy concerns and user expectations in CPSSs based on real-world knowledge. We also design a corresponding data publishing mechanism for users. It regulates the publishing behaviors to hide sensitive physical profiles. Meanwhile, the published data retain comprehensive social profiles for users. Our analysis demonstrates that the mechanism achieves a local maximized performance on the aspect published data size. The experiment results towards real datasets reveal that the performance is comparable to the global optimal one.

INTRODUCTION

Cyber-Physical Social Systems (CPSSs), as a new extension of social networks, is changing our life according to the recent studies. Users update their physical data collected through pervasive sensors in their mobile devices. They even act as ”sensors” themselves by taking photos or making comments. In such systems, the users are the creators and builders. They participate in both the computation and formation of the system. On the other hand, users establish their profiles as they do in a regular social network by publishing their sensed data. They form their own reputations and achieve a self actualization. An typical CPSS is the Local Business Service System (LBSS), where users initially visit some Point of Interests (PoIs) in their cities and upload photos and comments like ”intellectual sensors”. Others who are in favor of these comments would praise or follow them. Unfortunately, while enhancing the functionality of existing Cyber Physical Systems, the CPSS also brings privacy threats to users, since the generated data usually reveal some private information such as locations, motions, and personal habits. The

users could suffer physical threats, which are far more harmful than advertisements or spam mails. Therefore, the users face severe challenges when sharing their data in CPSSs. As a solution, this paper studies the privacy preserved data publishing problem in CPSSs.

The privacy issues in CPSSs are actually different from the ones in regular social networks or the ones towards physical data. Most previous works focusing on data privacy issues only preserve privacy for single or several records. Take the privacy preservation for geographical locations as an example. The corresponding problems are well-studied ranging from hiding sensitive locations to avoiding inferring locations from public records. The typical techniques include true location obfuscation, anonymity, etc.

However, these countermeasures are incapable for CPSSs since users often contribute long-term behaviors and expect their whole physical profiles or patterns to be privacy preserved. More specifically, as in a social network, users establish their profiles via long-term participation. They publish and share numerous records revealing their general physical profiles such as mobility pattern in daily life. The physical profiles are closely related to their behaviors in the physical world. For example, the mobility pattern refers to a user's moving regularity, like appearance possibility in an urban area, visit of abnormal POIs and many more. Adversaries can crawl the published records from the systems and infer the profile to obtain the private information such as working and residential areas, abnormal visiting behaviors, or even potential changes in one's life. Such information may be further used for advertisement delivery or even physical stalking. According to the study on a real-case dataset, users with only a moderate number of published records already reveal some features of their mobility patterns. Therefore, there must be a well-designed tool to help users regulate their publishing behaviors in CPSSs.

EXISTING SYSTEM

- Privacy preservation in cyber-physical systems has been attracting the attention from both academic and industrial communities. This issue draws even more attention in the recent years due to the pervasively embedded sensors in mobile devices.
- Xu et al. Propose an approach based on the virtual reality techniques to bypass face authentication tests and protect user privacy by avoiding the exposure of their real faces.

DISADVANTAGES OF EXISTING SYSTEM:

- Typical studies include exposure of sensitive information, privacy preservation of physical data, and usage or access to sensor data.
- There work mainly studies the domain-specific data privacy, while ignoring the utility in social networks.

PROPOSED SYSTEM:

- We propose novel definitions on the utility on social profiles and privacy on physical profiles for CPSSs, which are more reasonable for real world scenarios.
- We formulate the record publishing problem in CPSSs and propose a heuristic algorithm to select the published records.
- We analyze and prove that the heuristic algorithm can satisfy all the constraints while publishing a maximal number of records for each user.
- We also propose an adaptive algorithm to support the publishing of novel records.

ADVANTAGES OF PROPOSED SYSTEM:

- For the utility in social networks, our mechanism maintains the consistency with the original social profile and publishes a maximum number of records.
- It guarantees that users can attract the same type of followers and show their activeness.

IMPLEMENTATION

SCREENS

Fig: Home Page

Fig: Admin Login

Fig: Admin Home

Fig: User Registration

Fig: User Home

CONCLUSION

In this paper, we investigate the problem of privacy preservation in CPSSs which inherit features from both cyber-physical systems and social networks and face novel privacy issues. A thoroughly designed countermeasure is expected to handle the privacy issues for physical data, while maintaining a good utility as in social networks. We prove that the proposed algorithm can achieve a maximal number of published records. The evaluation on real dataset validates the effectiveness of the algorithm on both physical privacy and social utility. Our study could work as a general tool in preserving users' privacy when they share their physical data with others in CPSSs.

REFERENCES

[1] A. Sheth, P. Anantharam, and C. Henson, "Physical-cyber-social computing: An early 21st century approach," IEEE Intelligent Systems, vol. 28, no. 1, pp. 78–82, 2013.

[2] F. Li, C. Tian, T. Li, and Y. Wang, "Energy efficient social routing framework for mobile social sensing networks," Tsinghua Science and Technology, vol. 21, no. 4, pp. 363–373, 2016.

[3] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolba, "A greedy model with small world for improving the robustness of heterogeneous internet of things," Computer Networks, vol. 101, pp. 127–143, 2016.

[4] L. Hu, A. Sun, and Y. Liu, "Your neighbors affect your ratings: on geographical neighborhood influence to rating prediction," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval, pp. 345–354, ACM, 2014.

[5] T. Qiu, A. Zhao, R. Ma, V. Chang, F. Liu, and Z. Fu, "A task-efficient sink node based on embedded multi-core soc for internet of things," Future Generation Computer Systems, 2016.

[6] Y. Wang, D. Xu, and F. Li, "Providing location-aware location privacy protection for mobile location-based services," Tsinghua Science and Technology, vol. 21, no. 3, pp. 243–259, 2016.

[7] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "Cap: A contextaware privacy protection system for location-based services," in Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on, pp. 49–57, IEEE, 2009.

[8] K. Fawaz, H. Feng, and K. G. Shin, "Anatomization and protection of mobile apps: Location privacy threats," in 24th USENIX Security Symposium (USENIX Security 15), pp. 753–768, 2015.

[9] T. Qiu, X. Liu, L. Feng, Y. Zhou, and K. Zheng, "An efficient treebased self-organizing protocol for internet of things," IEEE Access, vol. 4, pp. 3535–3546, 2016.

[10] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," IEEE Transactions on Vehicular Technology, 2016.