

Follow But No Track: Privacy Preserved Profile Publishing in Cyber-Physical Social Systems

ABSTRACT

Cyber-Physical Social Systems (CPSSs), as a new extension of social networks, is changing our life according to the recent studies. 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 reveals that the performance is comparable to the global optimal one.

EXISTING SYSTEM

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. A 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 a 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.

DRAWBACKS

- It provides limited privacy preservation for sensitive physical information.
- It provides our location which is not secure.

PROPOSED SYSTEM

In this paper, 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 reveals that the performance is comparable to the global optimal one.

ADVANTAGES

- It preserves the physical profiles by carefully selecting the public records.
- It retain utility for individuals within the social networks.
- It supports a user-friendly control so that users can adjust their preference and sensitivity on privacy.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X
- Programming Language : Java
- Java Version : JDK 1.6 and above