Exploiting Social Network to Enhance Human-to-Human Infection Analysis without Privacy Leakage

ABSTRACT

Human-to-human infection, as a type of fatal public health threats, can rapidly spread in a human population, resulting in a large amount of labor and health cost for treatment, control and prevention. To slow down the spread of infection, social network is envisioned to provide detailed contact statistics to isolate susceptive people who has frequent contacts with infected patients. In this paper, we propose a novel human-to-human infection analysis approach by exploiting social network data and health data that are collected by social network and e-healthcare technologies. We enable the social cloud server and health cloud server to exchange social contact information of infected patients and user’s health condition in a privacy-preserving way. Specifically, we propose a privacy-preserving data query method based on conditional oblivious transfer to guarantee that only the authorized entities can query

users’ social data and the social cloud server cannot infer anything during the query. In addition, we propose a privacy-preserving classification-based infection analysis method that can be performed by untrusted cloud servers without accessing the users’ health data. The performance evaluation shows that the proposed approach achieves higher infection analysis accuracy with the acceptable computational overhead.

**EXISTING SYSTEM**

* With the advanced and efficient homomorphic encryption techniques [25], Graepel et al. [26] propose a machine learning scheme with privacy preservation to outsource the heavy computation tasks to the powerful cloud servers. At the same time, data confidential and user privacy are achieved with the advantages of the adopted leveled homomorphic encryption scheme. This privacy-preserving machine learning scheme mainly solves the privacy issues during the data training phase.
* To perform both training and learning over encrypted data, Bost et al. [18] develop a set of secure machine learning classification schemes based on leveled fully homomorphic encryption
* Yuan et al. [30] propose a privacy-preserving back-propagation neural network learning algorithm based on “doubly homomorphic” encryption. This algorithm allows users to send encrypted data to the cloud server, which performs most of the computation tasks without compromising the privacy of user’s raw data. Another type of lightweight machine learning is decision tree based classification, which is studied in [31] and developed with privacy protection mechanisms.
* Recently, Zhou et al. [32] propose a secure text mining scheme, where a privacy-preserving data aggregation method is served as the building block to enable data training in cloud assisted e-healthcare system. Considering the data access problem, Zhou et al. [33] propose a user-controlled multi-level cooperative authentication scheme to protect user’s attribute information from disclosing during the data exchange.

**Disadvantages**

* + There is no naive Bayesian classification on Human to Human Infection Analysis.
  + There are no double encryption techniques to secure medical data.

**PROPOSED SYSTEM**

* In the proposed system, the system proposes a Privacy-preserving Infection Analysis approach (PIA) considering social network data associated with health data to infer human-to-human infection spread. This approach employs a privacy-preserving data query method based on conditional oblivious transfer to enable data sharing among different entities and a privacy-preserving classification-based infection analysis method to enable the cloud servers to infer infection spread and preserve health data privacy. The main contributions of this paper are four-fold.
* Firstly, the system analyzes the spread process of infectious disease with the consideration of user’s social contact and health condition. We exploit several key factors of infection, including immunity strength of the susceptible user, infectivity of the infected patient, their contact duration, and the type of contact. We also utilize naive Bayesian classification method to enhance infection analysis with the collaboration of social and health cloud servers.
* Secondly, the system also proposes a privacy-preserving data query method (PPDQ) based on conditional oblivious transfer to allow the authorized entity (i.e., hospital) to access the infected patient’s social network data from the social cloud server, but not allow the social cloud server to access and infer any data including patient’s identity. Furthermore, this method enables users to grant authorization to hospital, which cannot query any data without user’s authorization.
* Thirdly, the system proposes a privacy-preserving classification based infection analysis method (PCIA) to prevent user’s private social and health data from disclosing to the un trusted health cloud server. The PCIA enables users to encrypt raw data based on homomorphic encryption and send ciphertexts to the cloud server. Then, the health cloud server can infer infection spread during human-to-human contact without learning any user’s private information.

**Advantages**

* The system enables operations over cipher texts for healthcare systems
* A privacy-preserving clinical decision support system is proposed based on naive Bayesian classification.

**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

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL