Published on *CPS-VO* (https://cps-vo.org)

Home > Biblio > Printer-friendly PDF

Privacy-preserving pattern matching over encrypted genetic data in cloud computing

Submitted by grigby1 on Tue, 01/23/2018 - 2:54pm

Title	Privacy-preserving pattern matching over encrypted genetic data in cloud computing
Publication Type	Conference Paper
Year of Publication	2017
Authors	Wang, B., Song, W., Lou, W., Hou, Y. T.
Conference Name	IEEE INFOCOM 2017 - IEEE Conference on Computer Communications
Date Published	may
ISBN Number	978-1-5090-5336-0
Keywords	biology computing, cloud computing, Computational modeling, cryptography, data privacy, diseases, DNA, DNA cryptography, DNA data, DNA data privacy, DNA information, encrypted genetic data, Encryption, Genetics, genome matching problem, genomics, Health Care, health care model, Human Behavior, Metrics, Pattern matching, personal genomics services, personalized medicine, privacy, privacy guarantee, privacy-preserving pattern matching, pubcrawl, regular clinical laboratory tests, Resiliency, secure DNA sequence matching problem, Testing

Abstract

Personalized medicine performs diagnoses and treatments according to the DNA information of the patients. The new paradigm will change the health care model in the future. A doctor will perform the DNA sequence matching instead of the regular clinical laboratory tests to diagnose and medicate the diseases. Additionally, with the help of the affordable personal genomics services such as 23andMe, personalized medicine will be applied to a great population. Cloud computing will be the perfect computing model as the volume of the DNA data and the computation over it are often immense. However, due to the sensitivity, the DNA data should be encrypted before being outsourced into the cloud. In this paper, we start from a practical system model of the personalize medicine and present a solution for the secure DNA sequence matching problem in cloud computing. Comparing with the existing solutions, our scheme protects the DNA data privacy as well as the search pattern to provide a better privacy guarantee. We have proved that our scheme is secure under the well-defined cryptographic assumption, i.e., the sub-group decision assumption over a bilinear group. Unlike the existing interactive schemes, our scheme requires only one round of communication, which is critical in practical application scenarios. We also carry out a simulation study using the real-world DNA data to evaluate the performance of our scheme. The simulation results show that the computation overhead for real world problems is practical, and the communication cost is small. Furthermore, our scheme is not limited to the genome matching problem but it applies to general privacy preserving pattern matching problems which is widely used in real world.

URL https://ieeexplore.ieee.org/document/8057178
DOI 10.1109/INFOCOM.2017.8057178

Citation Key wang_privacy-preserving_2017

biology computing Cloud Computing Computational modeling Cryptography data privacy diseases DNA DNA cryptography DNA data DNA data privacy DNA information encrypted genetic data encryption Genetics genome matching problem genomics health care health care model Human behavior Metrics pattern matching personal genomics services personalized medicine privacy privacy guarantee privacy-preserving pattern matching pubcrawl regular clinical laboratory tests Resiliency secure DNA sequence matching problem testing