Cryptographic Solutions for Credibility and Liability Issues of Genomic Data

ABSTRACT

With the rapid decrease in the cost of whole genome sequencing and genotyping, today, genomic data is widely used in healthcare, research, and even in recreational genomics. However, benefits due to this wide use of genomic data come along with potential threats against individuals' privacy. Genomic data of an individual includes privacy sensitive data about him such as his physical characteristics, predisposition to diseases, and family members. Therefore, it is crucial to protect privacy of an individual's genomic data while allowing him to utilize his data to receive certain healthcare or recreational services. As a result, there has been significant amount of research efforts on privacy preserving processing and secure storage of genomic data.

EXISTING SYSTEM

Privacy leakage occurs when genomic data of the individual or his genetic test results are publicly shared by the service providers that collect such data at the first place. In such incidents, it is important to understand whom to keep liable due to such a leakage. Thus

- The individual wants to provide a digital consent along with his data specifying whether the service provider is allowed to further share his data.
- If his data is shared without his consent, the individual wants to determine the service provider that is responsible for this leakage.

Our main assumption is that the service provider (which receives genomic data or genetic test results from an individual) should prove the legitimacy of the data when sharing it with other entities. Otherwise, credibility of the shared data is not guaranteed, and hence data is not valuable. Under this assumption, if the service provider makes the data public (without the consent of the individual), it will be detected by the individual. Similarly, if the service provider tries to share the data offline with another (non-malicious) entity, that entity will understand that the corresponding data is being shared without the consent of the data owner. Note however that if the unauthorized offline sharing of genomic data is between a malicious service provider and other malicious service providers, there is no technical solution to detect this leakage.

Disadvantages

- Privacy preserving processing and secure storage of genomic data is less.
- Privacy leakage occurs when genomic data of the individual or his genetic test results are publicly shared by the service providers that collect such data at the first place.

PROPOSED SYSTEM

In this work, we proposed two cryptographic schemes to share genomic data and genetic test results. The proposed schemes are between a data owner and a service provider. Using the proposed schemes, on the one hand, a service provider can check the validity (or legitimacy) of genomic data it receives from a data owner (individual). On the other hand, the individual, via a digital consent, can make sure that the service provider will not further share his data without his permission. The proposed schemes are based on homomorphic signatures and aggregate signatures, and these cryptographic primitives enable us to link the information about the legitimacy of the data to the consent and the identity of the individual. We also discussed the security and practicality of the proposed schemes. The proposed schemes can be easily adopted by existing works on privacy preserving processing of genomic data.

Advantages

- The proposed techniques for the privacy-preserving storage, retrieval of raw-genomic data and guarantee long term security.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3

RAM : 512MB-2GB

HARD DISK : 40GB