Güvenli Görevdeş Sağlık Paylaşımı

Sena Efsun CEBECİ, Alptekin KÜPÇÜ, Öznur ÖZKASAP

Bilgisayar Mühendisliği Bölümü, Koç Üniversitesi, İstanbul

Secure Peer-to-Peer Health-Sharing

Abstract: *Existing health information sharing systems deal with interoperability and standardization in a centralized manner, rather than attaching necessary importance to security and privacy issues. Several prior studies and research projects consider messaging and classifying standards, and semantic interoperability as their main objectives, whereas the security aspects are limited to encryption of the medical data and user authentication. Current centralized structures, such as Google Health providing a patient-oriented service and Sağlık-NET offering a healthcare-provider-oriented framework, have drawbacks in terms of robustness (single point-of-failure), scalability, and fairness (single privileged system provider). Existing decentralized solutions do not target security, privacy, and fairness issues.*

The aim of our work is to propose a secure P2P health information sharing system by improving state-of-the-art in terms of patient controlled sharing, fair medical data exchange, and decentralized P2P approach. It is well-known that P2P design principles help in reducing load on the peers and developing efficient network protocols. Furthermore, it is a constitutional right of a patient to control how medical information about himself / herself is shared, and under which circumstances. This will be enforced through cryptographic mechanisms. Another use of novel cryptographic primitives will mend itself into fair medical-data sharing protocols where the medical information about a patient gathered at different peers (e.g., healthcare providers) will be shared in a P2P system fairly. Thus, the patient will rest assured that any institution (s)he visits for medical purposes will be able to see all relevant aspects of the patient's medical history. That means, regardless of where the past visits of the patient have occurred, the appropriate cure can be carried on.

In our study, peers will be small-medium public or private hospitals, other healthcare organizations, or insurance companies. Our evaluation will be based on a prototype implementation and deployment first at Koç University network platform, and then at American Hospital for extended measurements. All cryptographic protocols will be proven secure, and their efficiency will be tested. We shall also conduct case studies that may include data of patients with serious diseases, such as breast cancer.

Key Words: Health Information Sharing, Peer-to-Peer Networks, Security, Privacy, Cryptographic Protocols

Özet:
Mevcut sağlık bilgi paylaşımı sistemleri, birlikte çalışabilirlik ve standardizasyon ile anlaşma konularını merkezi bir ortamda ele alarak güvenlik ve gizliliğe gerekli önemi vermemektedir. Birçok önceki çalışma ve araştırma projesi mesajlaşma ve sınıflandırma standartları ve anlamsal birlikte çalışabilirlik konularını ana hedefleri olarak göz önünde bulundurmuşlar, güvenlik konularını tıbbi veri şifreleme ve kullanıcı kimlik doğrulaması ile sınırlandırmışlardır. Google Health hasta odaklı hizmet veren bir merkezi yapı ve Sağlık-NET de sağlık-sağlayıcı odaklı bir çerçeve sunan merkezi yapıdır, dezavantajları sağlamlık (tek bir arıza noktası), ölçeklenebilirlik ve adalet (tek ayrıcalıklı bir sistem sağlayıcısı) açısındandır. Mevcut merkezi olmayan çözümler güvenlik, gizlilik ve adalet konularını hedeflememektedir.

Çalışmalarımızın amacı, hasta kontrollü paylaşımı, adil tıbbi veri alışverişi ve merkezi olmayan P2P yaklaşım açısından son teknoloji ürünü geliştirerek güvenli bir P2P sağlık bilgi paylaşım sistemi önermektir. P2P tasarım ilkelerinin, görevdeş yükü azaltmak ve verimli ağ protokolleri geliştirmekte yardımcı olduğu çok iyi bilinmektedir. Ayrıca, bir hastanın kendisi hakkında tıbbi bilgi paylaşımının nasıl ve hangi şartlar altında

paylaşıldığını kontrol etmesi anayasal bir haktır. Bu kriptolojik mekanizmalar aracılığıyla yürütülür. Yeni kriptolojik ilkellerin başka bir kullanımı da farklı düğümlerde (örn. sağlık hizmeti) toplanan hasta hakkındaki tıbbi bilginin P2P sistem ile adil olarak paylaşılıp tıbbi veri paylaşım protokollerinin kendini tamir etmesi olacaktır. Böylece, hasta tıbbi amaçlar için ziyaret ettiği herhangi bir kurum veya kurumlarda tıbbi geçmişinin ilgili tüm yönleriyle görülebileceğinin mümkün olacağından emin olacaktır. Bu da hastanın geçmiş ziyaretleri nerede meydana gelmiş olursa olsun uygun tedavinin yapılabilir olması anlamına gelmektedir.

Bizim çalışmamızda, ortaklarımız küçük-orta ölçekli bir kamu hastaneleri veya özel hastaneler, diğer sağlık kuruluşları ya da sigorta şirketleri olacaktır. Değerlendirmemiz, bir prototip uygulamaya ve dağıtıma bağlı olarak ilk Koç Üniversitesi ağ platformunda ardından da genişletilmiş ölçümler için Amerikan Hastanesi'nde yapılacaktır. Tüm şifreleme protokollerinin güvenliği kanıtlanmış olacak ve verimliliği test edilecektir. Ayrıca meme kanseri gibi ciddi hastalıkları olan hastaların verilerini içeren vaka çalışmaları da yürüteceğiz.

Anahtar Kelimeler: Sağlık Bilgisi Paylaşımı; Görevdeş (P2P) Ağlar; Güvenlik; Gizlilik; Kriptolojik Protokoller

Sorumlu Yazarın Adresi

Sena Efsun Cebeci
senacebeci@ku.edu.tr
Koç Üniversitesi, Mühendislik Fakültesi, Sarıyer, İstanbul
http://eng.ku.edu.tr/
http://crypto.ku.edu.tr/