Medikal Bilgi Sistemlerinde Güvenlik, Mahremiyet ve Kimlik Doğrulama

Can Eren Aladağ[1], Ercan Kurtarangil[1], Şerif Bahtiyar[2]

[1] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

[2] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., Şişli, İstanbul

aladagc@itu.edu.tr, kurtarangil@itu.edu.tr, serif.bahtiyar@provus.com.tr

Özet: Medikal bilgi sistemleri, bilgisayar tabanlı bilgi sistemlerini kullanarak sağlık hizmetlerini geliştirmektedirler. Bu medikal sistemler, tanı, tedavi, sağlık verilerinin toplanması ve yönetilmesi gibi alanlarda yeni çözümler getirirler. Ancak, kişisel bilgileri ve sağlık ile ilgili bilgileri içermesi sebebi ile medikal bilgi sistemlerinin güvenliği kritik önemdedir. Bu çalışmamızda, öncelikle medikal alanda kullanılan bilgi sistemleri incelenmiştir. Daha sonra, bu sistemler ile ilgili mahremiyet tehditleri, gereklilikleri ve koruma yöntemleri çeşitli kategorilerde sınıflandırılarak incelenmiştir. Medikal bilgi sistemlerinin güvenliğinde diğer bir önemli konu kimlik doğrulamadır. Bu çalışmamızda, bu sistemlerde kullanılan kimlik doğrulama yöntemleri ve biyometrik kimlik doğrulama gibi olası kimlik doğrulama yöntemleri incelenmiştir. Son olarak bu medikal bilgi sistemlerindeki sorunlar ve gelecekte çalışılacak konular irdelenmiştir.

Anahtar Sözcükler: Medikal Bilgi Sistemleri, Mahremiyet, Mahremiyet Koruma Katmanları, Kimlik Doğrulama.

Security, Privacy, and Authentication of Medical Information Systems

Abstract: Medical information systems improve conventional health services via information systems. The medical systems are used to provide a lot of health services, such as diagnosis, management of patients' information. Because medical information systems contain patients' information that is considered as private information, security of such systems is a critical issue. In this paper, we have investigated the concept of medical information systems. Then, we have analyzed by classifying them according to existing privacy threats, requirements, and prevention methods. We have also investigated existing authentication methods for such systems and potential authentication methods like biometric authentication. Finally, we have pointed out challenging issues related to security of medical information systems.

Keywords: Medical Information Systems, Privacy, Privacy Protection Layers, Authentication.

1. Giriş

Medikal bilgi sistemleri, bilgisayar tabanlı bilgi sistemlerini kullanarak sağlık hizmetlerini geliştirmektedir. Bu medikal sistemler, tanı, tedavi, sağlık verilerinin toplanması ve yönetilmesi gibi alanlarda yeni çözümler getirirler. Medikal bilgi sistemleri, bilgiyi elektronik sağlık kayıtları (EHR) ya da kişisel sağlık kayıtları (PHR) gibi çeşitli formlarda kullanır. Elektronik sağlık kayıtları, bilgi iletişim teknolojilerini (ICT) kullanarak hasta bilgilerinin bir arada elektronik ortamda saklanmasından oluşur [2]. Elektronik sağlık kayıtları hastanelerde, kliniklerde, doktor ofislerinde kullanılır. Bu kayıtlar tıbbi alanda oluşan hataları azalıp, tedavilerin yönetilmesini kolaylaştırırken

hastalara ait birçok önemli bilgiyi içerdiği için mahremiyetin korunması açısından büyük riskler taşımaktadır [4].

Kişisel sağlık kayıtları (PHR), bireylerin Internet tabanlı uygulamalarla kullandıkları kişisel tıbbi verilerdir. Her iki bilgi sistemi tedavi geçmişi, genetik yatkınlık, laboratuar geçmişi gibi çeşitli kişisel bilgi içerir. Elektronik sağlık kayıtları sağlık çalışanları tarafından kullanılmasına karşın, kişisel sağlık kayıtları hastalar tarafından kullanılır [2].

Bu bildirinin ikinci bölümümde medikal sistemlerde mahremiyet konusunu inceledik. Üçüncü bölümü klinik doğrulamaya ayırdık ve son bölüm ile bildiriyi sonlandırdık.

2. Mahremiyet

Mahremiyet hasta ve doktor arasındaki en önemli hususlardan bir tanesidir. Hasta sağlık kayıtlarının temel amacı, tanı ve tedaviyi geliştirmek olsa da hastane, sigorta şirketleri gibi çeşitli alanlar tarafından farklı amaçlar için kullanılabilir. Oysa hasta sağlık kayıtları, kişiye ait kimlik bilgisi, geçmişine ait sağlık bilgisi, kullandığı tedavi yöntemleri, beslenme alışkanlığı, cinsel tercihi ve genetik bilgisi gibi çok yüksek seviyede kişisel bilgi içerir. Bu yüzden bu kayıtların mahremiyeti, farklı amaçlar için kullanılmaması, medikal bilgi sistemlerinin en önemli araştırma alanlarının başında gelmektedir [10].

Hastaların kişisel sağlık verilerinin paylaşımı konusundaki bakış açıları Sankar tarafından incelenmiştir [11]. Buna göre, öncelikle hastalar kendi kişisel bilgilerini sadece kendi tedavileriyle ilişkili kişiler arasında paylaşılmasını istemektedirler. Bunun yanı sıra, sağlık verilerinin doktorlar arasında paylaşılmasının farklı bakış açısı katarak tedavilerinin gelişmesine katkı sağlayacağına da inanılmaktadır. Ayrıca hastaların büyük bir kısmı, kişisel verilerinin işverenleri, aileleri gibi üçüncü kişilerle paylaşılmasını istememektedirler.

2.1 Mahremiyet Tehditleri

Medikal bilgi sistemlerindeki mahremiyet tehditlerini organizasyonel ve sistematik olmak üzere iki ana başlık altında incelenmektedir [12].

2.1.1 Organizasyonel Tehtitler

Organizasyonel tehditler, içeriden veya dışarıdan hasta kayıtlarına uygunsuz olarak erişmeye çalışmaktan kaynaklanmaktadır. Sisteme giriş yetkisi olan iç tehdit unsurları, yetkilerini kötü amaçlı kullanabilirler. Diğer yandan dış tehdit unsurları ise, sistem açıklarından faydalanarak sisteme yetkisiz erişimde bulunabilirler. Hasta sağlık verilerine yapılan saldırıların büyük bir kısmı ekonomik nedenlere dayanmaktadır. Bu veriler sigorta şirketleri, sağlık şirketleri, işverenler ve çeşitli suç odakları açısından ekonomik olarak yüksek değerlere sahiptir. Organizasyonel tehditler beş farklı bölümde sınıflandırılabilir [12].

İlk bölüme göre, sağlık personeli, kişisel sağlık verilerini dikkatsizlik ve kaza sonucu istenmeyen kişilerle paylaşabilir. Örneğin hasta kayıtlarının yanlış e-posta adresine gönderilmesi bunlardan biridir.

İkinci bölüm sağlık personelinin erişim yetkisi ve merakı ile ilgilidir. Sağlık personeli verilere erişim yetkisini kişisel amacı ya da merak nedeniyle kullanması, mahremiyet ihlaline neden olabilir. Örneğin, ünlü bir kişinin kişisel sağlık verilerinin ifşa edilmesi bunlardan biridir.

Üçüncü bölüm çıkar ile ilgilidir. Sağlık personeli kişisel çıkar ya da intikam için sağlık verilerine erişip, verileri sistem dışındaki kişilerle paylaşabilir.

Diğer bir mahremiyet tehdidi ise, saldırganların fiziksel güç kullanarak mahremiyet ihlaline neden olmasıdır.

Son olarak, sisteme ağ üzerinden yetkisiz erişim, verilerin açığa çıkmasına neden olabilir.

2.1.2 Sistematik Tehditler

Ethoni' ye göre mahremiyet ihlallerinin büyük bir kısmı, sisteme yasal olarak giriş yetkisi olan kişilerin verileri sistematik olarak başka amaçlar için kullanmasından ortaya çıkmaktadır [13]. Örneğin sigorta şirketlerinin sağlık verilerini hastaların tedavi masraflarını karşılamak için kullanmasının yanı sıra, bu verileri analiz ederek kişilere ait sağlık risklerini hesaplamak için kullanmaları ya da işverenlerin, adayları sağlık verilerine göre seçmesi sistematik mahremiyet ihlaline örnek verilebilir.

2. 2 Mahremiyet Gereklilikleri

Medikal bilgi sistemlerinde mahremiyetin tam anlamıyla korunabilmesi için bazı temel ilkeler bulunmaktadır. Öncelikle hastalar kendi mahremiyet endişeleri hakkında geri bildirimlerde bulunabilmeli ve bu geri bildirimler sistemin düzenlenmesinde etkili rol oynamalıdır. Ayrıca her bir hasta kendi bilgi akışını kontrol edebilmeli ve istenmeyen bilgi paylaşımları düzenlenip, iptal edilebilmelidir. Diğer bir önemli ilke ise, sistemin hastaları bilgi paylaşımı konusunda hiç kimseye güvenmesine gerek kalmayacak şekilde inşa edilmesidir. Örneğin hastaların sisteme girişi için kullandıkları şifrelerin sağlık personeli olsalar dahi kimseyle paylaşmaması gerekir. Son olarak medikal bilgi, hastaların genel profilini ve davranışlarını ortaya çıkarabilecek kadar geniş kapsamlı olmamalıdır [1].

2.3 Mahremiyet Koruma Katmanları

Medikal sistemlerde mahremiyeti korumak için geliştirilen yöntemler dört seviyeli katmanlarda incelenebilir [3].

İlk katman, mahremiyetin devlet tarafından kanun ve yasalarla güvence altına alınmasıdır. Bu konuda yapılan en önemli çalışma ABD tarafından yayınlanan HIPAA Mahremiyet Kurallarıdır.

İkinci katman, mahremiyetin organizasyonel seviyede korumayı amaçlamaktadır. Medikal bilginin sistem bazında mahremiyetin korunması için başta giriş kontrol sistemleri ve ilkeleri olmak üzere çeşitli araştırmalar yapılmaktadır.

Üçüncü seviye, hastaların kendi kişisel bilgilerinin mahremiyeti konusunda bilinçlendirmeyi amaçlamaktadır. Sıradan bir hasta, kişisel mahremiyetini korumak için bilmesi gereken prosedürlerin hepsine hâkim olamayabilir. Bu durumda çeşitli eğitimler ve kaynaklar aracılığıyla, insanların kendi mahremiyetlerinde oluşabilecek zafiyetlerin önüne geçilmesi amaçlanmaktadır.

Dördüncü ve son katmanda ise hasta kayıtlarının çeşitli bilimsel amaçlar doğrultusunda veri madenciliği yöntemleri ile toplanması sırasında verilerin kişisel kimliklerden arındırılarak anonimleştirilmesi üzerinde durmaktadır. Bu konuya Matlock'in HIPAA Mahremiyet Kurallarını göz önünde bulundurarak nöro resim (neuroimage) veri setindeki kişisel kimliklerin ortadan kaldırılması konusundaki çalışmaları örnek verilebilir [14].

3. Kimlik Doğrulama

İletişim halinde olan sistemler birbirlerini doğrulamak zorundadır. Bu yüzden kimlik doğrulama yöntemleri güvenlik işleyişi için ön koşul hale gelmiştir. Medikal bilgi sistemlerinde bilgi güvenliğini sağlamak için bu ön koşul çok önemli hale gelmektedir. Örneğin, doktorlar hastaların verilerine ulaşırken önce kimlik doğrulamadan geçmelidirler [5].

3.1 Kimlik Doğrulama Yöntemleri

Medikal bilgi sistemlerinde kimlik doğrulama yöntemleri birçok yolla gerçekleşebilir. Bu kimlik doğrulama yöntemleri tek başına kullanılabileceği gibi diğer kimlik doğrulama yöntemleri ile birlikte de kullanılabilir. Bu çalışmada, parola ile kimlik doğrulama ve biyometrik kimlik doğrulama olmak üzere iki kimlik doğrulama yöntemi araştırılmıştır.

3.1.1 Parola ile Kimlik Doğrulama

Medikal bilgi sistemlerinde en çok kullanılan kimlik doğrulama yöntemi diğer sistemlerde olduğu gibi kullanıcı numarası ve parolası kullanmaktır. Kullanıcı numaraları ve parolaları özel bir veri tabanında tutulabileceği gibi birçok sistemin ortak kullandığı bir veritabanında da tutulabilir. Kullanıcı numaraları veritabanında şifrelenmemesine rağmen, PIN ya da parolalar veri tabanında şifrelenirler. Kullanıcı numarasını yazdıktan sonra numara veri tabanındaki mevcut numaralar ile karşılaştırılır. Eğer numaralar eşleşirse yazılan parola şifrelenerek mevcut şifrelenmiş veri tabanındaki parola ile karşılaştırılır. Tekrar eşleşme durumunda kimlik doğrulama tamamlanmış olur [9].

Sadece kullanıcının bildiği verilerliden oluşan kimlik doğrulama tipi olan parola ile kimlik doğrulama tipini kullanarak oluşturulan tek fazlı kimlik doğrulama yöntemi yeterince güvenli değildir. Daha güvenli olan iki fazlı kimlik doğrulama sistemleri tercih edilmelidir. İki fazlı kimlik doğrulama sistemlerinde kullanıcının ezberlemek zorunda olmadığı bir diğer faz eklenir. Örneğin, iki fazlı kimlik doğrulama sisteminde ilk faz olarak parola ile kimlik doğrulama yöntemi, ikinci faz olarak biyometrik kimlik doğruma yöntemlerinden biri kullanılabilir. Ya da ikinci faz olarak kullanıcının sahip olduğu kimlik doğrulama yöntemi olarak bilinen tek kullanımlık şifre üreten akıllı cihazlar gibi yöntemler de kullanılabilir [6].

3.1.2 Biyometrik Kimlik Doğrulama

Biyometrik sistemlerde yüz şekli, parmak izi, avuç izi, ses ve iris gibi anatomik özellikler insanı tanımlamakta kullanıldığı gibi yürüyüş biçimi, hal ve hareketler, imza gibi davranış biçimleri de insanı tanımlamakta kullanılır. Bu özellikler, bireye özgü olduğu için biyometrik sistemler biyometrik kimlik doğrulama yönteminin geliştirilmesinde kullanılmaktadır. Biyometrik kimlik doğrulama, medikal bilgi sistemlerine giriş yapmak isteyen kullanıcıları belirlemede çok güvenlidir ve yapay değildir. Biyometrik kimlik doğrulama yöntemi aynı zamanda inkâr edilemez bir kimlik doğrulama yöntemidir [7].

Davranışsal biyometrik kimlik doğrulama yöntemleri kimlik doğrulama süresini kısalttığı için medikal bilgi sistemlerinde iki fazlı kimlik doğrulamada tercih edilmektedir. Yeni geliştirilen kimlik doğrulama yöntemlerinden olan ekran parmak izi yöntemi iki fazlı kimlik doğrulama sistemlerinde ikinci faz olarak kullanılabilir. Bu yöntem kullanıcıların sistemde yaptığı hareketleri kayıt edip, oluşturduğu kayıtlardan veri seti elde eder. Eğer sonraki oturumlarında bu veri setlerinden farklı bir şekilde sistemde dolanım yapıyorsa sistem hata verir ve sistemdeki oturum sonlandırılır [8].

4. Sonuç

Medikal bilgi sistemleri gelişen teknolojiye paralel olarak sağlık alanına birçok yenilikler ve kolaylıklar sunmaktadır. Bu yeniliklerle birlikte güvenlik ve mahremiyetin korunması açısından yeni endişeleri de beraberinde getirmektedir.

Bu çalışmada, öncelikle mahremiyet konusu ele alınarak mahremiyet tehditleri, gereklilikleri ve koruma yöntemleri çeşitli kategorilerde sınıflandırılarak incelenmiştir. Daha sonrasında, tıbbi bilgi sistemlerinde kullanılan kimlik doğrulama yöntemleri ve biyometrik kimlik doğrulama gibi olası kimlik doğrulama yöntemleri incelenmiştir.

Teşekkürler
Bu çalışma EUREKA ITEA2 projesi ADAX (proje no. 10030) ve TEYDEB projesi AKFİS (proje no. 1130018) tarafından desteklenmiştir.

5. Kaynaklar

[1] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., Muller, G., "Aspects of privacy for electronic health records", **International journal of medical informatics,** 80:26-31, (2011).

[2] Senor, I. C., Aleman, J. L. F., Toval, A., "Personal Health Records:New Means to Safely Handle Health Data?", **IEEE Computer,** 45: 27-33, (2012).

[3] Datta, A., Dave, N., Mitchell, J., Nissenbaum, H., Sharma, D., "Privacy Challenges in Patient-Centric Health Information Systems", **1st Usenix Workshop on Health Security and Privacy**, ABD, 1-2, (2010).

[4] Chun, S. A., Vaidya, J., "Privacy in Health Informatics", **International Journal of Computational Models and Algorithms in Medicine**, 3: i-vi, (2012).

[5] Sun, J., Fang, Y., Zhu, X., "Privacy And Emergency Response In E-Healthcare Leveraging Wireless Body Sensor Networks", **IEEE Wireless Communications**, 66–73, (2010).

[6] Chess, B., Arkin, B., "The Case for Mobile Two-Factor Authentication", **IEEE Security & Privacy**, 81-85, 2011.

[7] Jain, A. K., "Biometric Authentication: System Security and User Privacy", **IEEE Computer Society,** 87–92, (2012).

[8] Patel, V.M., Yeh, T., Fathy, M. E., Zhang, Y., Chen, Y., Chellappa, B. R., Davis, L., "Screen Fingerprints: A Novel Modality for Active Authentication", **IT Pro**, 38-42, (2013).

[9] Wager, K. S., Lee, F. W., Glaser, J. P., "Health Care Information Systems", **Second Edition Jossey Bass**, 2009.

[10] Mercuri, R.T., "The HIPAA-potamus in health care data security", **Communications of the ACM**, 47:25–28, (2004).

[11] Sankar, P., Moran, S., Merz, J.F., Jones, N.L., "Patient perspectives on medical confidentiality: a review of the literature", **Journal of General Internal Medicine**, 18:659–669, (2012).

[12] Rindfleisch, T.C., "Privacy, information technology, and health care", **Communications of the ACM**, 40:93–100, (1997).

[13] Etzioni, A., "The Limits of Privacy", **Basic Books**, New York, (1999).

[14] Matlock, M., Schimke, N., Kong, L., Macke, S., Hale, J., "Systematic Redaction for Neuroimage Data", **International Journal of Computing Models and Algorithms Medicine,** 3:1-18, (2012).