©2019 Published in 7th International Symposium on Innovative Technologies in Engineering and Science 22-24 November 2019 (ISITES2019 SanliUrfa - Turkey)
https://doi.org/10.33793/acperpro.02.03.104

E-Sağlık ve Güvenlik: Riskler, Fırsatlar ve Çözüm Önerileri

*[1]Çiğdem Çoban and [1]Mehmet Fatih Tüysüz
*[1]Harran Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Şanlıurfa, Türkiye

Özet

E-Sağlık; bilgi ve iletişim teknolojilerinin (BİT) sağladığı olanakların, hastalıkların teşhis ve tedavi edilmesi, sağlık hizmetlerine erişilebilirliğin arttırılması, sağlık sektöründe yer alan tüm paydaşlara kaliteli, verimli ve etkili sağlık hizmetlerin sunulması için kullanılmasıdır. E-Sağlık, sağlık hizmetlerini geliştiren ve kolaylaştıran avantajlara sahip olmasına rağmen, Elektronik Hasta Kayıtlarına (EHR) yetkisiz erişim, tıbbi verilerin gizliliği ve bütünlüğüne saldırı, sistem ve internet güvenliği sorunları gibi birçok güvenlik ve gizlilik sorunuyla karşı karşıyadır. Bu sorunlar, e-Sağlık sistemlerinin düzgün çalışmasını engelleyebilir ve sistem kullanıcılarına (hasta, doktor vs.) hatalı, eksik ve yanlış bilgiler verilmesine sebep olabilir. Bu durum tıbbi veri güvenliği için tehlike oluşturmaktadır. Bu nedenle e-Sağlık sistemlerinde güvenlik konusunun değerlendirilmesi büyük bir önem taşımaktadır. Bu çalışma kapsamında, e-Sağlıkta güvenlik konusu bilgi ve iletişim teknolojileri çerçevesinde ele alınmış, olası riskler ve fırsatlar göz önüne alınarak literatürde yapılan çalışmalar irdelenmiş ve gelecekte yapılması gereken öneriler okuyucuya sunulmuştur.

Anahtar Kelimeler: E-Sağlık, Güvenlik, Bilgi ve İletişim Teknolojileri

Abstract

E-Health is the use of information and communication technologies (ICT) facilities to diagnose and treat diseases, increase accessibility to health services, and provide quality, efficient and effective health services to all stakeholders in the health sector. Although E-Health has the advantages of improving and facilitating health services, it faces many security and privacy issues, including unauthorized access to Electronic Patient Records (EHR), intrusion and confidentiality of medical data, system and Internet security issues. These problems can prevent e-Health systems from functioning properly and cause system users (patients, doctors, etc.) to receive incorrect, incomplete or incorrect information. This is a danger to medical data security. For this reason, it is very important to evaluate the security issue in e-Health systems. Within the scope of this study, the subject of e-Health security has been handled within the framework of information and communication technologies, studies conducted in the literature have been examined by considering possible risks and opportunities, and the suggestions to be made in the future have been presented to the reader.

1. Giriş

1948 yılında Dünya Sağlık Örgütü (WHO) tarafından yapılan tanıma göre sağlık; sadece bireyin vücudunda hastalık ve sakatlığın olmayışını değil, kişinin bedenen, ruhen ve sosyal yönden tam bir iyilik halinde olmasını ifade etmektedir [1]. Bilgi ve iletişim teknolojisinin gelişmesi ve sağlık alanında kullanılması, dünyadaki geleneksel sağlık hizmeti yaklaşımını etkilemiştir. Tıbbi laboratuvarlar, hastane, sağlık sigortası şirketleri gibi çeşitli alanlarda bilgi ve iletişim teknolojileri kullanılması e-Sağlık olarak adlandırılan bir kavramı ortaya çıkarmıştır [2].

1.1. E-Sağlık

E-Sağlık, sağlık hizmetlerinin etkin ve verimli bir şekilde geliştirilmesi, sürdürülmesi ve sunulması için bilgi ve iletişim teknolojilerinin sağlık alanında kullanılmasıdır. Eysenbach'ın [3] literatürde yaygın bir şekilde kabul gören tanımına göre e-Sağlık "Tıp bilişimi, halk sağlığı ve

*Corresponding author: Address: Faculty of Engineering, Department of Computer Engineering Harran University, 63300, Şanlıurfa TURKEY. E-mail address: cigdemcoban@harran.edu.tr, Phone: +903183018

ticaret ile internet ve ilgili teknolojiler aracılığıyla sağlanan veya geliştirilen sağlık hizmetlerinin ve bilgilerin kesiştiği yeni bir alandır." Daha geniş anlamıyla bu ifade, bilgi ve iletişim teknolojilerini kullanarak sağlık hizmetini yerel, bölgesel ve dünya çapında geliştirebilmek için sadece teknik bir gelişmeyi değil, aynı zamanda akıl kavramını, bir düşünme biçimini, bir tutumu, bir ağa bağlılığı ve küresel düşünmeyi de karakterize etmektedir. Ayrıca e-Sağlık, Dünya Sağlık Örgütü (WHO) tarafından "Sağlık hizmetleri, sağlık gözetimi, sağlık literatürü ve sağlık eğitimi, bilgisi ve araştırması dâhil olmak üzere sağlık ve sağlıkla ilgili alanları desteklemek için bilgi ve iletişim teknolojilerinin (BİT) düşük maliyetli ve güvenli bir şekilde kullanımı" olarak tanımlanmıştır [4].

E-Sağlık çatı kavramdır. Elektronik sağlık kayıtları (EHR), Kişisel Sağlık Kayıtları (PHR), Tele-Sağlık ve Tele-Tıp, Mobil-Sağlık (mHealth), sağlık alanındaki Büyük Veri Sistemleri, sensörler ve giyilebilir izleme sistemleri gibi birçok dijital sağlık alt alanlarını kapsamaktadır [5].
E-Sağlık sistemlerinde, iletişim ve ağ teknolojileri (5G, WI-FI), makineden makineye iletişim (M2M), akıllı ve giyilebilir kişisel cihazlar, Kablosuz Sensör Ağları (WSN), Kablosuz Vücut Alan Ağları (WBAN, BAN), Nesnelerin İnterneti (IoT), Bulut Bilişim, Büyük Veri (Big-Data) analitiği, Sosyal ağ analizi ve sosyal medya, 3D baskı, robotic, yapay zekâ gibi birçok bilgi ve iletişim teknolojileri kullanılmaktadır [6]. Bu çalışmada incelediğimiz literatür çalışmalarındaki bilgi ve iletişim teknolojilerine ait kısa tanımlar aşağıda okuyucu ile paylaşılmıştır.

- Kablosuz Sensör Ağları (WSN): Kablosuz bir ortamda birlikte çalışarak etraflarını algılayabilen, çevresiyle etkileşebilen yüzlerce sensör düğümünden oluşan ağdır.
- Kablosuz Medikal Sensör Ağı (WMSN): Sınırlı bellek, bilgi işlem gücü ve bant genişliği ile birçok sensör içeren sağlık alanında kullanılan bir WSN ağıdır [7].
- Kablosuz Vücut Alan Ağları (WBAN): İnsan vücudun üzerine veya içine yerleştirilen, kablosuz ortamda haberleşebilen, kesintisiz olarak kişinin sağlık durumunun gözlemlenmesini sağlayan küçük ve akıllı sensörlerin oluşturduğu ağdır [8].
- Mobil Sağlık: Dünya Sağlık Örgütünün (WHO) tanımına göre, akıllı telefon, hasta izleme cihazları, dijital ve mobil cihazlar ve diğer kablosuz araçlar kullanılarak, tıbbi ve halk sağlığı hizmetlerinin desteklenmesidir [4].
- Mobil Sağlık Ağları (MHN): Giyilebilir cihazlar, kullanıcılar, sunucular ve heterojen mobil ağlardan oluşan ağdır [9].
- Tele Tıp Tıbbi Bilgi Sistemi (TMIS): Hastaların evde sağlık izlemesi yapmasını ve tıbbi hizmetlere internet veya mobil ağ üzerinden erişebilmelerini sağlayan, kısacası tele tıp servislerini rahatça almalarına yardımcı olan sistemlerdir [10].
- Elektronik Sağlık Kayıtları (EHR): Kişilere ait geçmişteki, şimdiki ve gelecekteki fiziksel ve ruhsal sağlığı veya hastalıkları ile ilgili elektronik sistemler kullanılarak kayıt altına alınan, saklanan, iletilen, erişilen, ilişkilendirilen ve işlenen her türlü bilginin dijital ortamda tutulması ile oluşan kayıtlardır [11].
- Bulut Bilişim: Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tanımına göre, bulut bilişim, bilgi teknolojileri dünyasında depolama ve uygulamalar gibi hizmetler sağlamak için bilgisayar kaynaklarını ve modern teknolojik işlevleri kullanma modelidir [12].

1.2. Güvenlik

Bilgi ve iletişim teknolojilerinin kullanıldığı tüm alanlarda güvenlik kavramı en başta karşımıza çıkmaktadır. Özellikle, sağlık alanındaki sistemlerde önemli bir konudur, çünkü bu sistemlerdeki bilgilerin ele alınması sırasında güvenliğin çoğu yönü kritik öneme sahiptir. Güvenlik, bir bütün

olarak sistemin emniyetini kapsayan bir kavramdır [13]. Bu tanımı bilgi ve iletişim teknolojileri açısından genişletirsek; güvenlik, bilgi ve iletişim teknolojilerinin kullanıldığı sistemlerde hem sistemin emniyetinin sağlanması hem de bu sistemlerdeki verilerin gizliliğinin, bütünlüğünün ve doğruluğunun sağlanmasıdır. Ancak güvenlik denildiğinde ilk olarak veri ya da bilgi akla gelmektedir. Bir sistemin güvenliği sadece veri ya da bilginin güvenliği ile alakalı değildir. Sistemin güvenliği, veri, ağ ve cihaz güvenliği ile yani sistemin bütünüyle alakalıdır.

E-Sağlık sistemlerinde güvenliğin sağlanması son derece önemlidir. Bu sistemlerde kişilere ait hassas tıbbi ve kişisel verileri mevcuttur. Bu verilerin hiçbir şeklide bozulmaması, yetkisiz kişiler tarafından erişilmemesi, kayıp olmaması gerekmektedir. Bu verilerin güvenliği sağlanamazsa ve amacı dışında kullanımı hasta için tehlikeli sonuçlar oluşturabilir. Ayrıca bu sistemler çeşitli nedenlerden dolayı siber güvenlik olaylarına karşı savunmasız hale gelebilmektedir. Bu durumlarda oluşan güvenlik ihlalinin nüfusun büyük bölümünü etkileyebileceği gerçeği, e-Sağlık sistemlerinde güvenliği kritik bir konu haline getirmektedir [14]. E-Sağlık sistemlerinde yüksek düzeyde güvenlik sağlamak için ulusal ve uluslararası alanda birçok yasal düzenlemeler geliştirilmektedir. Yasal düzenlemeler, sistemlerde oluşan riskleri yönetmek, kişisel tıbbi verilerin gizliliğini ve güvenliğini sağlamak için yapılmaktadır. Örneğin, HIPAA olarak da bilinen Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası, 1996 yılında sağlık bilgilerinin güvenliğini ve gizliliğini korumak, nasıl kullanılmaları gerektiğini ve hasta verilerinin nasıl birbiriyle değiştirilmeleri gerektiğini belirlemek için Amerika Birleşik Devletleri (ABD) Kongresi tarafından ortaya konuluştur [2]. HIPAA'da bireylerin elektronik kişisel sağlık bilgileri korumak için ulusal standartlar ve kurallar belirlenmiştir.

Türkiye'de kişisel verilerin korunması için 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu yayımlanmıştır [15]. Bu kanun ile kişisel verilerin güvenliği ile alakalı usul ve esaslar belirtilmiştir. Bu kanun sadece sağlık verileri değil, kişisel tüm veriler ile alakalıdır. Kişisel sağlık verileri ile alakalı birçok yönetmelik yayınlanmıştır. Bu yönetmeliklerin sonuncusu 21 Haziran 2019 tarihli ve 30308 sayılı "Kişisel Sağlık Verileri Hakkında Yönetmelik" olmuştur [16]. Bu yönetmelik ülkemizdeki kişisel sağlık verilerinin güvenliği ile alakalı gerekli düzenlemeleri içermektedir.

Bu çalışma kapsamında, e-Sağlık ve güvenlik konusu bilgi ve iletişim teknolojileri açısından ele alınmış, günümüzde ve gelecekte güvenliğin korunumu için yapılabilecek çalışmalar/ihtiyaçlar ortaya konulmuştur. Çalışmanın ikinci bölümünde e-Sağlıkta gizlilik ve güvenlik gereksinimlerinden bahsedilmektedir. Bölüm 3'te e-Sağlıkta güvenlik konusuna ait olası riskler ve fırsatlar bahsedilmektedir. Bölüm 4'te ise konu ile alakalı literatürde yapılmış çalışmalar okuyucuya sunulmuştur. Bölüm 5'te sürdürülebilir güvenli bir e-Sağlık için önerilerde bulunulmuş, gelecekteki olası etkilerinden bahsedilmiştir.

2. E-Sağlık Gizlilik ve Güvenlik Gereksinimleri

E-Sağlık sistemlerinin etkin kullanılması ve güvenliğin sağlanması için yönetim seviye güvenliği (veri erişim kontrolü, hesap verebilirlik, geri alına bilirlik), ağ seviyesi güvenliği (veri gizliliği, reddetmeme), fiziksel seviye güvenliği (sensör düğümü yakalama ve sıkışma saldırılarına karşı direnç) ve veri seviyesi güvenliği (veri şifreleme, bütünlüğü, veri doğrulama) gibi bir dizi güvenlik ve gizlilik gereksinimlerinin karşılanması gerekmektedir [17]. Bir e-Sağlık sisteminde güvenliğin sağlanması için önemli temel güvenlik gereksinimleri aşağıda okuyucu ile

paylaşılmıştır [2, 13, 14, 17, 18, 19].

- Gizlilik: Tıbbi verilerin yetkisiz erişim ve kullanıma karşı korunmasıdır. Kişisel mahremiyetin istila edilmeyeceği veya tıbbi bilgilerin ifşa edilmeyeceği garanti edilmektedir. E-Sağlık sistemlerinde hasta verileri gizli tutulmalıdır.
- Bütünlük: E-Sağlık sistemlerinde doğru tıbbi verilerin alınması, bu verilerin özgün ve eksiksiz olmasını ifade eder. Tıbbi veri güvenilir, doğru ve değiştirilemezdir.
- Güvenilirlik: Tıbbi verilerin yasal olmayan bir şekilde ya da yetkili olmayan kişiler tarafından değiştirilmesinin engellenmesini ifade eder.
- Kullanılabilirlik: Tıbbi verilerin herhangi bir durumda sağlık sistemindeki kullanıcılar tarafından kolayca ulaşılabilir olmasını ifade eder. Ayrıca e-Sağlık sistemlerinde ihtiyaç duyulduğunda gerekli mimarinin bileşenleri mevcut olmalıdır.
- Anonimlik: Tıbbi verilerin ve kullanıcıların gizliğinin sağlanması için, uygulama sağlayıcısı ve ağ yöneticisi dahil hiç kimsenin istemci kimliğini bilmemesini ifade eder. E-Sağlık sistemlerinde hasta ve kullanıcı anonimliği sağlanmalıdır.
- Esneklik: Acil bir durumda hastanın hayatını kurtarmak için belirli tıbbi verilere yetkisi olmayan izinsiz katılımcının veriye erişimni ifade eder. Erişim kuralı güvenlik açısından yeterli olmalıdır.

3. Olası Riskler ve Fırsatlar

E-sağlık sistemlerinin birçok yararı olmasına rağmen, taşınabilirliği ve tasarımları nedeniyle birçok güvenlik tehditlerine karşı savunmasızdır ve çeşitli güvenlik, gizlilik risklerine sahiptir. E-Sağlık sistemlerdeki bilgi teknolojileri güvenliği, hassas tıbbi verilerin yüksek güvenlik ve gizlilik gereklilikleri nedeniyle büyük bir endişe kaynağı olmaktadır. Bu sebepten dolayı sistemlerde güvenliğin risk ve fırsatlarının incelenmesi çok önemlidir. Tarafımızca yapılan literatür araştırması sonucunda gözlemlenen riskler aşağıda maddeler halinde açıklanmıştır.

- Sistem Kullanılabilirliği: E-Sağlık sistemlerine herhangi bir saldırı ya da bu sistemlerde oluşan herhangi bir teknik sorundan dolayı sisteme ve tıbbi bilgiye erişim olmaması hizmet sunumu önemli ölçüde etkilemektedir. Bu durum uygulama güvenliğinin azaltacağından e-Sağlık sistemi açısından büyük risk oluşturmaktadır.
- Birlikte Çalışabilirlik: E-Sağlık sistemlerinde yüksek düzeyde birlikte çalışabilirlik sağlanmaması ve bilgilerin birbirine bağlı birçok farklı sistem üzerinde güvenli bir şekilde iletilmesini sağlanmaması, etkin ve güvenli kullanım için risk oluşturmaktadır.
- Erişim Kontrolü ve Kimlik Doğrulama: E-Sağlık sistemlerine kullanıcı erişim rolleri düzgün tanımlanmadığı ya da dışarıdan saldırgan tarafından yapılan bir saldırı durumunda yetkisi olmayan kişilerin sisteme erişmesi, tıbbi veri ve sistem güvenliği için risk oluşturmaktadır. Bu durumda veri bütünlüğü ve gizliliği garanti edilemez.
- Veri Bütünlüğü: E-Sağlık sistemlerinde saldırgan ya da sağlık çalışanı tarafından hatta sistemdeki donanımsal ya da yazılımsal sorunlardan dolayı veri bütünlüğü bozulabilir. Verilerin eksik/değiştirilmiş olması bütünlüğün olmamasını ifade eder ve güvenlik riski oluşturmaktadır.
- Ağ Güvenliği: Ağ ortamı üzerinden birçok hizmete erişilebilir. Eğer çeşitli sebeplerden dolayı ağ ortamı güvenliği olmazsa, ortamda hizmet veren sistemlerde de güvenlikten bahsetmek zordur olur. E-Sağlık sistemlerinde tıbbi veriler ağ üzerinden iletilmekte olduğu için ağ ortamının güvenli olmaması durumunda sistemin ve verilerin güvenliği için risk oluşmaktadır.
- Veri Kaybı: E-Sağlık sistemlerinde yazılım/donanım hataları, ağ hataları, güvenlik saldırıları gibi durumlarda veri kaybı oluşabilir. Bu durumun oluşması hasta için büyük risk oluşturmaktadır.

Yapılan literatür araştırması sonucunda gözlemlenen fırsatlar ise aşağıda halinde açıklanmıştır.

- Erişim Kontrolü ve Kimlik Doğrulama: E-Sağlık sistemlerinde erişim kontrolü ve kimlik doğrulama mekanizmalarının olması sisteme yetkisiz erişim ve güvenli erişim sağlamaktadır. Bu durum sistem ve tıbbi verilerin güvenliğini sağlamakta yardımcı olmaktadır. Özellikle erişim kontrolü veri gizliliği ve bütünlüğünün sağlanması için temel güvencedir.
- Sağlık Hizmeti Ortamı: E-Sağlık sistemleri kamusal yada özel bulut altyapıları kullanrak hizmet verebilir. Özellikle özel bulut ortamı yüksek erişim kimlik bilgilerine ve şifrelemeye sahip olduğundan veri için güvenli ortam oluşturmaktadır. Ayrıca tıbbi verilere erişim istenilen zamanda ve her yerden sağlanabilmektedir. Bu durum kaliteli ve verimli bir sağlık hizmeti sunulması sağlamaktadır.
- E-Sağlık Hizmetleri: Günümüzde e-Sağlık hizmetleri, vatandaşlara ve hastalara zamana ve mekana bağlı olmaksızın sağlık hizmeti sağlamaktadır. Bu hizmetler çoğunlukla sistemler ve kullanıcılar birlikte çalışabilirliğine dayanır.
- Mobil-Sağlık Uygulamaları: E-Sağlık sisteminin bir parçası olan mobil-Sağlık uygulamaları, kolay hasta takibi, doktor ile hasta arasında zaman ve mekana bağlı kalmaksızın sürekli ve kolay iletişim sağlanmasını, ayrıca kişilerde çeşitli sağlık konularında sağlık bilincinin oluşmasını sağlar. Bu uygulamalarda cihaz, uygulama tabanlı güvenlik sağlanmalıdır.
- Elektronik Sağlık Kayıtları/ Kişisel Sağlık Kayıtları: E-Sağlık sistemlerindeki en önemli yapı olan tıbbi veriler, sistemde belirli bir standart çerçevesinde, gerektiği zaman paylaşılabilir olacak şekilde ve güvenli olarak tutulmaktadır. E-Sağlık sistemlerinde verilerin bu şeklide tutulması sağlık hizmetinin verimli ve kaliteli bir şekilde verilmesini sağlamaktadır.

4. E-Sağlıkta Güvenlik Çözümleri

Çalışmanın bu kısmında literatürde incelmiş olduğumuz çalışmalar anlatılacak ve bu çalışmaların güvenlik açısından eksiklikleri ve literature katkıları değerlendirilecektir.

Debiao He ve arkadaşlarının 2015 yılında yaptığı çalışmada, Kablosuz Medikal Sensör Ağları'nda (WMSN) güvenlik ve gizlilik arttırmak için bir anonim doğrulama protokolü önerilmiştir. Konu ile alakalı daha önce yapılan çalışmaların eksiklikleri göz önüne alınarak önerilen protokolün yapılan güvenlik analizinde, güvenlik açısından çeşitli saldırıları engellediği ve gizlilik açısından kullanıcı anonimliği sağladığı görülmektedir. Önerilen protokol yanlış oturum anahtarı planına sahiptir fakat yanlış şifre tespit mekanizması yoktur. Yanlış bir şifreyi ile şifre değişikliği durumunda DOS saldırılarına karsı savunmasızdır [7]. Debiao He ve arkadaşlarının 2017 yılında yaptığı çalışmada, Kablosuz Vücut Alan Ağları'nda (WBAN) iletişim sırasında gerekli olan güvenlik gereksinimlerini karşılamak, güvenliği arttırmak için kanıtlanabilir güvenlikli bir AA (anonymous authentication) programı önerilmektedir. Önerilen programda yapılan analizlerde, önceki çalışmaların güvenlik açısında zayıflığının giderildiği ayrıca hesaplama yükünün de azaltıldığı gösterilmektedir [8]. Zuowen Tan ve arkadaşlarının 2014 yılında yaptığı çalışma, Teletıp Tıbbi Bilgi Sistemi (TMIS) için üç faktörlü kimlik doğrulama şeması önerilmektedir. Önerilen şemada iki faktör kimlik doğrulama şemalarının güvenlik gereksinimlerini üç faktörlü kimlik doğrulama şemalarına uygulanmaktadır. Şemada güvenlik analizi yapıldığında; karşılıklı kimlik doğrulama, sunucu şifresi bilmeme, şifre özgürlüğü, biyometrik güncelleme, üç faktörlü güvenlik, kullanıcı anonimliği koruma sağlandığı gösterilmektedir. Şemanın farklı bilgi sistemlerinde nasıl çalıştığı ise bilinmemektedir [10]. Prosanta Gope ve arkadaşının 2016 yılında yaptığı çalışma, Vücut Sensör Ağları (BSN) tabanlı modern sağlık sistemindeki temel güvenlik gereksinimlerini vurgulamakta ve BSN-Care adlı BSN'de kullanan güvenli bir IoT tabanlı sağlık sistemi önerilmektedir. BSN-Care giyilebilir ve

yerleştirilebilir sensörlerden oluşan bir BSN mimarisidir. Bu sistemde güvenlik gereksinimleri karşılamak için gereksinimler ağ ve veri güvenliği olarak ikiye ayrılmıştır. Ağ güvenliğini sağlamak için Lightweight Anonymous Authentication Protocol (Hafif Anonim Kimlik Doğrulama Protokolü), veri güvenliği için de OCB onaylı şifreleme modu önerilmektedir. Bu sistemde yapılan analizlerin sonucunda; sistem güvenlik gereksinimlerini etkili bir şekilde yerine getirmeyi garanti edebilmektedir ve makul bir hesaplama ek yükü sağlamaktadır [13]. Ajmal Sawand ve arkadaşlarının 2015 yılında yaptığı çalışma, verimli ve güvenli e-Sağlık izlemenin tasarlanması için gelişmiş e-Sağlık izleme sistemi için kapsamlı bir CPS tabanlı e-Sağlık izleme çerçevesi sunmaktadır. Burada verilen mimari, en gelişmiş ağ ve kablosuz iletişim teknolojileri tarafından iyi bir şekilde bağlanan fiziksel katmanlardan ve siber katmanlarından oluşan CPS'nin (Cyber Physical Systems) tipik bir uygulaması olarak düşünülebilir. Çerçevenin güvenliği incelemek için gerekli kullanım ölçütleri tanımlanmıştır. Temel güvenlik ve gizlilik gereksinimlerini, yönetim, ağ, bilgi ve fiziksel olmak üzere dört ana kategoriye ayrılarak incelenmiştir. Daha sonra, e-Sağlık izleme sistemlerini hedef alan güvenlik tehditleri ve çözümleri incelenmiştir [17].

Benjamin Fabian ve arkadaşlarının 2014 yılında yaptığı çalışma, çok sayıda bağımsız bulut sağlayıcısından (Multi-Cloud) oluşan veri bulutu ortamında farklı kuruluşlar arasında sağlık verilerin paylaşılması için güvenli ve gizliliğin korunmasına yönelik bir mimari ve uygulamasını sunmuştur. Mimaride CP-ABE şifrelemeye dayanan rol tabanlı erişim kontrol mekanizmasını kriptografik olarak uygulanmaktadır ve verilerin yetkisiz değiştirilmesini önlemek, veride bütünlük ve orijinallik için kriptografik Hash tabanlı Mesaj Doğrulama Kodu (HMAC) kullanılmaktadır. Çalışma kapsamında geçici ve acil durumlar için bir mimari geliştirilmelidir [19]. Aqeel Sahi ve arkadaşlarının 2016 yılında yaptığı çalışma, elektronik sağlık bilgilerinin güvenliğini ve bulut ortamında sağlık kayıtlarının mahremiyetini sağlamak için iki yaklaşımda bulunmuştur. Birincisi, bulutta elektronik sağlık kayıtlarının (EHR) sadece güvenliğini sağlamak için PEM-AES'e dayalı güvenlik koruma yaklaşımıdır. İkincisi, kişisel sağlık kayıtlarının (PHR) mahremiyetini arttırmak için anahtar değişim protokolüne (3PAKE) dayalı kimlik doğrulama ile gizlilik koruma yaklaşımıdır. Yaklaşımlar gerekli güvenlik ve gizlilik gereksinimlerini karşılamaktadır. Yaklaşımlardan herhangi birinin başarısız olması durumunda ise mekanizma verimli bir şekilde çalışmamaktadır [20]. Jun Zhou ve arkadaşlarının 2015 yılında yaptığı çalışma ile, dağıtılmış m-Sağlık bulut sisteminde belirtilen gizlilik ve güvenlik gereksinimini gerçekleştiren, yetkili erişilebilir gizlilik modeli ve hasta tarafından yönetilebilen çok seviyeli gizliliği koruyan kooperatif doğrulama şeması (PSMPA) önerilmiştir. Çalışmada yetkili erişilebilir gizlilik modeli (AAPM) kurulmuştur. PSMPA bu modeli uygulamak için üç farklı güvenlik seviyesi ve gizlilik gereksinimini gerçekleştirmek üzere önerilen tasarımdır. PSMPA'nın kötü niyetli saldırılara karşı koyabildiği yapılan analizlerde ortaya konulmuştur. Buradaki gizlilik modeli ve doğrulama şeması güvenlik ve verimlilik sağlaması açısından önemlidir [21]. Xu A. Wang ve arkadaşları 2017 yılında yaptığı çalışmada, e-Sağlık sisteminin güvenliğini ve mahremiyetini sağlamak için farklı şifreleme teknikleri tanımlanmaktadır. Kimlik Tabanlı Şifreleme (IBE) ve yeni Kimlik Tabanlı Proxy Yeniden Şifreleme (IBPRE) şemalarını içeren bu tekniklerin güvenlik ve performans analizleri yapılmaktadır. Analiz sonuçlarında, yeni geliştirilen IBPRE'nin daha sonra buluttaki sağlık bilgisini korumak için kullanılabilecek yeniden şifreleme için daha güvenli ve verimli olduğu görülmüştür [22].

Nafiseh Kahani ve arkadaşlarının 2016 yılında yaptığı çalışma, bulut tabanlı e-Sağlık sistemlerinde hem kimlik doğrulama hem de erişim kontrolünü koruyan, iki aşamalı anahtar

erişim kontrolü ve sıfır bilgi protokolüne dayanan yeni bir bilgi erişim yöntemi önermektedir. Sistemdeki iki adımlı ortak anahtar şifreleme ve DUKPT kombinasyonu, farklı varlıklar arasında güvenli bağlantılar kurmak için kullanılmıştır. Şemada çeşitli saldırılar ve veri gizliliğine karşı direnç analizi yapıldığında sonuçlar, şemanın makul sayıda yanıt süresi ile çok sayıda eşzamanlı kimlik doğrulama talebini tolere ettiğini göstermektedir. Fakat, sistem sınırlı sayıda varlığa sahiptir ve ölçeklenebilir değildir [23]. Danan Thilakanathan ve arkadaşlarının 2014 yılında yaptığı çalışma, mobil sağlık uygulamalarında bulut'taki verilerin güvenli bir şekilde paylaşılmasına izin verecek güvenlik protokolü ortaya koymak amacındadır. Makalede ilk olarak mobil telecare uygulaması gösterilmektedir ve bu uygulama güvenli bir veri paylaşım modeli ve protokolünü göstermek için kullanılmaktadır. Protokolde ElGamal-bazlı proxy yeniden şifreleme kullanılmaktadır. Protokol güvenlik açısından verimli olsa da, yükleme zamanının uzun sürmesi ve veri paylaşımı hizmetinin güvenli olmadığı durumlarda nasıl çalışacağının bilinmemesidir sorun teşkil etmektedir [24]. Jiang Qi ve arkadaşlarının 2017 yılında yaptığı çalışmada, giyilebilir sağlık izleme sistemlerinde (WHMS) güvenlik sağlanması amacıyla belirlen güvenlik gereksinimlerini sağlamak için, uçtan uca karşılıklı kimlik doğrulama protokolü tasarlanmıştır. Protokol kuadratik tortulara dayanmaktadır. Protokolde yapılan güvenlik analizi, protokolün tüm olası saldırılara karşı güvenli olduğunu ve daha fazla güvenlik özelliği sağladığını kanıtlanmaktadır. Başlıca sakıncası protokolün giyilebilir sağlık izleme sistemlerinde pratik bir kullanıma uygun olmamasıdır [25]. Weiran Liu ve arkadaşlarının 2015 yılında yaptığı çalışma, elektronik sağlık verilerini depolama verilerine vermeden önce güvenceye almak için rol tabanlı bir erişim kontrolü (RBAC) şeması önermektedir. Çalışmada Rol Tabanlı Erişim Kontrolü (RBAC) ile Hiyerarşik Kimlik Tabanlı Şifreleme (HIBE) şemasını birleştirilmektedir. Yapılan güvenlik analizinde veri gizliliği sağlanmaktadır. Sakıncası ise, güvenilir ve doğru erişim kontrolü gerekliliklerini sağlamamasıdır [26]. Mohammed R. Abdmeziem ve arkadaşlarının 2015 yılında yaptığı çalışma, yüksek kaynak kısıtlı düğüm ve uzak sunucu arasında güvenli bir uçtan uca iletişim kanalı kurmak için iş birliği prensibine ve ağır kriptografik ilkellerin kullanılmasına dayanan, uçtan uca anahtar yönetim protokolü önermektedir. Protokolü hem güvenlik özellikleri hem de enerji tasarrufu açısından değerlendirmek için, AVISPA aracı kullanılmaktadır. Sonuçlar, protokolün güvenlik özellikleri korunurken, enerji alanında önemli bir kazanç sağladığını göstermektedir [27]. Bruno M. C. Silva ve arkadaşlarının 2018 yılında yaptığı çalışma, mobil sağlık sistemlerinde kullanıcıları verilerinin gizliliğini, bütünlüğünü ve orijinalliğini garanti etmeye çalışan yeni bir veri şifreleme çözümü önermektedir. Ayrıca DE4MHA olan ve olmayan m-sağlık uygulamasının performansını karşılaştıran bir performans değerlendirme çalışması sunmaktadır. DE4MHA, simetrik ve asimetrik şifreleme algoritmaları kullanarak karma bir yaklaşım kullanır. Bu çalışmada m-sağlık ağ mimarisi için en uygun simetrik algoritmanın AES olduğu, ağ senaryoları için en uygun asimetrik algoritmanın RSA olduğu ve web servisleriyle iletişim için HTTPS protokolünün en uygun güvenlik mekanizması olduğu ortaya çıkmıştır [28].

5. Sürdürülebilir Güvenli Bir E-Sağlık İçin Öneriler

Literatürdeki mevcut çalışmalar e-Sağlık sistemindeki genel güvenlik ve gizlilik gereksinimlerini karşılayabilecek öneriler sunmaktadır. Ayrıca bu mevcut çalışmalarda, en çok araştırılan alanların kimlik doğrulama, şifreleme, veri iletimi gibi güvenlik ve gizlilik için kullanılan teknikler öneren alanlar olduğu açıkça görülmektedir. E-Sağlık sisteminde güvenlik önlemlerini almak ve uygulamak için farklı yaklaşımlar önermek çok önemlidir. Burada iki soru ortaya çıkmaktadır: birincisi, “E-Sağlık sistemlerinde güvenlik ve gizlilikten kimler sorumludur?”; ikincisi: “E-Sağlık

sistemlerinde güvenlik ve gizlilik için neler yapılmalıdır?". Birinci soruya, kişinin kendisi (hasta), sağlık çalışanları, sağlık kurumları, hükümet ve sistem geliştiricileri cevap olarak verilebilir. Çünkü e-Sağlık sisteminin güvenliğini sağlamak için sistem ile ilgili olan herkesin gerekli güvenlik ve gizlilik gereksinimlerini karşılaması gerekmektedir. İkinci soru ise aşağıda maddeler halinde irdelenmiştir,

- E-Sağlık sistemlerine denetimin olması sistem güvenliğini etkileyebilecek her türlü suiistimal davranışının belirlenmesinde yardımcı olacaktır. Hükümet, yasal çerçevede sistemleri denetlemelidir. Ayrıca tıbbi veri, hasta gizliliğinin ve sistem güvenliğinin iç ihlallerini takip etmek için, sistem geliştirici tarafından sistemdeki bileşenler izlenmeli ve kaydedilmelidir.
- E-Sağlık sistemlerinde güvenlik ve gizliliği sağlamak için genellikle RBAC (Rol Tabanlı Erişim Kontrolü) modeli kullanılmaktadır. Bazı çalışmalarda farklı modeller (ABAC, DAC, MAC) de kullanılmıştır. Bu modelleri birleştirerek tek bir model oluşturmak, güvenlik ve gizliliği sağlamak için daha iyi performans gösterebilir.
- Literatürdeki çoğu çalışmada, e-Sağlık sisteminin güvenlik ve gizliliği sağlamak için şifreleme mekanizması kullanılmaktadır. Özellikle Öznitelik Tabanlı Şifrelemenin (ABE) e-Sağlık sistemlerinde gizliliğin sağlanmasında iyi olduğu bilinir, ancak verilerin şifresini çözerken aşırı hesaplamalar vardır ve performansını etkiler. Sistem verilerini şifrelemek için Gelişmiş Şifreleme Standardı (AES) kullanılabilir. Ayrıca kullanılan şifreleme anahtarı en az 128 bite sahip olmalıdır. Vücut Sensör Ağları (BSN) olan e-Sağlık sistemlerinde kimlik doğrulama ve anahtar dağıtımı güvenliği için şifreleme yöntemleri kullanılmalıdır. Çözümleri araştırmak ve şifreleme anahtarını 192 veya 256 bitlik olarak geliştirmek, sistem geliştiricisi için iyi bir araştırma alanı olarak kabul edilebilir.
- E-Sağlık sistemlerinde herhangi bir durumdan dolayı oluşan güvenlik ihlalinde, sağlık kurumları ilgili hastalara yetkili yerlere mümkün olan en kısa sürede bilgi vermelidir. Eğer güvenlik ihlalini hasta fark etmiş ise sistemdeki ihlalin giderilmesi için geri bildirimde bulunmalıdır. Sistem geliştiricisi herhangi bir güvenli ihlalini tespit edecek şeklide sistemi geliştirmelidir. Bu şeklide kendini kontrol eden sistem iyi bir araştırma alanı olarak kabul edilebilir.
- Literatüre göre, e-Sağlık sistemlerinde en yaygın kimlik doğrulama mekanizmaları, PKI (Açık Anahtar Altyapısı) ve giriş/şifre temelli dijital imza şemalarıdır [2]. Sistemlerde kullanıcı tarafından bilinen şifre ya da parmak izi gibi biyometrik özelliğini kullanarak çok faktörlü kimlik doğrulama kullanılması daha iyidir. Kimlik doğrulama için çok faktörlü kimlik doğrulamayı geliştirmek, sistem geliştiricisi için iyi bir araştırma alanı olarak kabul edilebilir.
- E-sağlık sistemlerinde veri transferi sırasında iletişimin dinlemesi ve değiştirilmesini engellemek yani güvenliği sağlamak için Aktarım Katmanı Güvenliği'ni (TLS) 128 bit şifreleme yöntemleri ve Sanal Özel Ağlar (VPN) kullanılmaktadır. Burada 256 bit şifreleme yöntemleri ile TLS kullanmak, sistem geliştiricileri için iyi bir araştırma alanı olarak kabul edilebilir.
- Literatürde yapılan araştırmaya göre, tıbbi verilere erişim kontrolü, hasta merkezli olmalıdır. Hastalar, istedikleri zaman bilgilere erişebilmeli veya bu bilgilere erişimlerini yasaklayabilmelidir. Burada önemli olan bu işlemlerin güvenli olmasıdır. Hasta sistem güvenliğini tehlikeye atmamalıdır ve kritik verileri değiştirmemelidir. Bu şekilde hastanın kontrol ettiği sistemin güvenliği kontrol etmek, sistem geliştiricileri tarafından yapılmalıdır.
- E-Sağlık sistemlerinde sistem sağlayıcısı ya da sağlık kurumları tarafından belirlen mutlaka bir gizlilik politikası olmalıdır. Verilerin toplanması, saklanması, uygulama hakkında ayrıntılı bilgi içeren bu politika hasta tarafında kabul edilirse işlem yapılmalıdır. Sistemin herhangi bir anındaki kullanıcı için politikanın erişilebilir olması gerekmektedir. Ayrıca politikaya bağlı olarak sistemde yapılanların kontrol edilebildiği mekanizma sistem geliştiricileri tarafından yapılmalıdır.

Gelecekte e-Sağlık sistemlerinde daha verimli ve başarılı güvenlik için, Elektronik Sağlık

Kayıtları, Mobil-Sağlık, Nesnelerin İnterneti (IoT), Kablosuz Teknoloji, Bulut Bilişim ve Vücut Alan Ağları gibi alt alanlarda daha fazla çalışma yapmak gerekmektedir. Özellikle bu alt alanların birlikte çalışabilirliği göz önüne alınarak heterojenik bir yapıya sahip e-Sağlık sistemlerinde güvenlik ile alakalı çalışmalar yapılmalıdır. E-Sağlık için geliştirilen uygulamalarda güvenliğin sağlanıp sağlanmadığını kontrol eden mekanizmalar mutlaka olmalıdır. Bu kontrol mekanizmaları uygulamalar geliştirildiğinde gözden kaçan açıkları ortaya çıkaracaktır ve güvenlik açısından başarı elde edilmesini sağlayacaktır. Kısacası gelişen bilgi ve iletişim teknolojileri göz önüne alınarak olası saldırılar incelenip mevcut ve gelecekteki sistemlerde bu saldırılara karşı önlem alabilen, güvenlik ve gizlilik gereksinimlerini karşılayan sistemler geliştirilmelidir.

Sonuç

E-Sağlık sistemlerinde hizmetten en üst düzeyde ve güvenli bir şekilde yararlanmak için, gerekli güvenlik ve gizlilik mekanizmalarını uygulamak çok önemlidir. Bu çalışma kapsamında, e-Sağlıkta güvenlik konusu bilgi ve iletişim teknolojileri çerçevesinde ele alınmış, gerekli güvenlik ve gizlilik gereksinimleri incelenmiştir. Olası riskler ve fırsatlar göz önüne alınarak literatürde yapılan çalışmalar irdelenmiş ve gelecekte yapılması gereken öneriler okuyucuya sunulmuştur. Çalışmadaki öneriler dikkate alınırsa daha güvenli e-Sağlık sistemleri geliştirmek mümkün olacaktır. Özellikle gelişen bilgi ve iletişim teknolojileri göz önüne alınarak ve ayrıca sistem ile ilişkisi olan herkesin gerekli sorumluluklarını yerine getirmesi sistemin daha verimli, kaliteli, güvenli olmasını sağlayacaktır. Kaliteli ve verimli bir sistem her zaman kullanım açısından ilk tercih sebebi olacaktır. Çalışmadaki önerilerimize göre, mevcut e-Sağlık sistemlerinde geliştirilen uygulamaların ne kadar güvenli ve gizli olduğunu ölçen, yani güvenliğin ve gizliliğin sağlanıp sağlanmadığını kontrol eden bir uygulama geliştirmeği hedeflemekteyiz. Gerçekleştireceğimiz uygulamanın güvenilir veri ölçümü, veri iletişimi ve veri analizi sağlanmasını kontrol etmek için bir kontrol mekanizması görevini üstleneceğini umuyoruz.

Kaynaklar

[1] WHO. Constitution Of The World Health Organization. [Online]. Available: https://www.who.int/governance/eb/who_constitution_en.pdf (Erişim Tarihi:05.10.2019)

[2] Azeez, N.A. and Vyver CV. Security and privacy issues in e-health cloud based system: A comprehensive content analysis. Egyptian Informatics Journal, 2019; 20(2): 97-108.

[3] Eysenbach G. What is e-health?. J Med Internet Res. 2001;3(2). doi: 10.2196/jmir.3.2.e20

[4] WHO. Global diffusion of eHealth: Making universal health coverage achievable. December 2016. [Online]. Available: https://www.who.int/goe/publications/global_diffusion/en/ (Erişim Tarihi: 05.10.2019)

[5] Erişim Tarihi: 5 Ekim 2019. https://innovatemedtec.com/digital-health/ehealth

[6] Aceto G., Persico V., Pescapéa A. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications. 2018; 107:125-154.

[7] He D., Kumar N.,Chen J., Lee C., Chilamkurti N. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems. 2015; 21(1): 49-60.

[8] He D., Zeadally S., Kumar N., Lee J.H. Anonymous Authentication for Wireless Body Area Networks With Provable Security.IEEE SYSTEMS JOURNAL. 2017;11(4): 2590-2601.

[9] Zhang K., Liang X., Yang K. , Su Z., Shen X.S., Luo H. H. Security and privacy for mobile healthcare networks: From a quality of protection perspective. IEEE Wireless Communications. 2015; 22(4):104-112.

[10] Tan Z. A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine

Information Systems. Journal of Medical Systems.2014; 38(16).
[11] Erişim tarihi: 5 Ekim 2019, https://dijitalhastane.saglik.gov.tr/TR,4874/ehr-electronic-health-record---esk-elektronik-saglik-kaydi.html
[12] Mell P., Grance T. The NIST Definition of Cloud Computing.2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[13] Gope P., Hwang T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal. March 2016; 16(5):1368-1376.
[14] ENISA. Security and Resilience in eHealth. December 2015. [Online]. Available: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services.(Erişim Tarihi: 05.10.2019).
[15] Kişisel Verilerin Korunması Kanunu No 6698. 2016. Türkiye. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf. (Erişim Tarihi: 05.10.2019).
[16] Kişisel Sağlik Verileri Hakkinda Yönetmelik. 2019. Türkiye. http://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm. (Erişim Tarihi 05.10.2019).
[17] Sawand A., Djahel S., Zhang Z., Naït-Abdesselam F. Toward Energy-Efficient and Trustworthy eHealth Monitoring System. China Commun. 2015; 2 (1):46-65.
[18] Zhang M., Raghunathan A., Jha N.K. Trustworthiness of Medical Devices and Body Area Networks. Proceedings of the IEEE. August 2014; 102(8): 1142-1188.
[19] Fabian B., Ermakova T., Junghanns P. Collaborative and secure sharing of healthcare data in multi-clouds.Information Systems. March 2015;48:132-150.
[20] Sahi A., Lai D. Li Y. Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. Computers in Biology and Medicine.2016; 78: 1-8.
[21] Zhou J., Lin X., Dong X., Cao Z. PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System. IEEE Transactıons On Parallel And Dıstrıbuted Systems. JUNE 2015; 26(6).
[22] Wang X.A., Ma J., Xhafa F., Zhang M., Luo X. Cost-effective secure E-health cloud system using identity based cryptographic techniques. Future Gener Comput Syst. 2017;67:242-254.
[23] Kahani N., Elgazzar K., Cordy K. Authentication and Access Control in e-Health Systems in the Cloud.In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (BigDataSecurity), New York, USA, 2016, pp.13-23.
[24] Thilakanathan D., Chen S., Nepal S., Calvo, R.A., Alem L.A platform for secure monitoring and sharing of generic health data in the Cloud. Future Generation Computer Systems.2014; 35:102–113. Doi:10.1016/j.future.2013.09.011.
[25] Qi J., Ma J., Chao Y., Ma X., Shin J., Chaudhry S.A. Efficient end-to-end authentication protocol for wearable health monitoring systems. Computers & Electrical Engineering. October. 2017; 63: 182-195.
[26] Liu W., Liu X., Liu J., Wu Q., Zhang J., Li Y. Auditing and Revocation Enabled Role-Based Access Control over Outsourced Private EHRs. In: 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), New York, NY, USA, 2015, pp. 336–341.
[27] Abdmeziem M.R., Tandjaoui, D. An end-to-end secure key management protocol for e-health applications. Computers & Electrical Engineering. April 2015; 44. Doi:10.1016/j.compeleceng.2015.03.030.
[28] Silva B.M., Rodrigues J., Canelo F., Lopes I.M.C., Lloret J. Towards a cooperative security system for mobile-health applications. Electron Commer Res.2019;19:629-654.