Mersin Üniversitesi Eğitim Fakültesi Dergisi - Mersin University Journal of the Faculty of Education

"Mersin Üniversitesi Eğitim Fakültesi Dergisi, 2018; 14(2): 745-755"
Araştırma Makalesi / DOI: 10.17860/mersinefd.357339

E-Öğrenme ve E-Sınavlar: Çevrimiçi Ölçme Değerlendirme Süreçlerinde Kimlik Doğrulama Yöntemlerine İlişkin Öğrenen Görüşlerinin İncelenmesi

E-Learning and E-Exams: Examination of Learners' Perspectives Concerning the Authentication Methods in Online Assessment Processes

Aras BOZKURT*, Hasan UÇAR**

Öz: Uzaktan eğitimde çevrimiçi öğrenme ortamlarıyla beraber bu ortamlarda yapılan sınavlar da yaygınlaşmaktadır. Kimlik doğrulama yöntemleri çevrimiçi sınav güvenliğini arttırmasına rağmen, öğrenenlerin biyometrik/kişisel bilgilerinin ve kişisel nesnelerin kullanılmasından dolayı hassas süreçleri içermektedir. Bundan dolayı çevrimiçi sınavlarda kullanılan kimlik doğrulama yöntemlerinin daha fazla incelenmesine yönelik bir ihtiyaç vardır. Bu bağlamda bu çalışmada uzaktan öğrenenlerin bakış açısıyla çevrimiçi sınavlarda kullanılabilecek kimlik doğrulama yöntemlerine ilişkin öğrenen görüşleri incelenmiştir. Kesitsel tarama modelinde 186 uzaktan öğrenenle gerçekleştirilen bu çalışmada çevrimiçi sınavlarda hangi kimlik doğrulama yöntemlerinin daha güvenilir bulunduğuna ilişkin soruya yanıt aranmıştır. Araştırma bulgularına göre katılımcıların biyometrik ve bilgi tabanlı kimlik doğrulama yöntemlerini daha güvenilir bulduğu yönünde görüş bildirdikleri belirlenmiş; ancak çevrimiçi sınavlarda yapılan bu tür kimlik doğrulama yöntemlerine karşı güven konusunda kararsızların yüzdesinin de çok olduğu görülmüştür.
Anahtar Kelimeler: Uzaktan eğitim, e-öğrenme, e-sınav, ölçme değerlendirme, kimlik doğrulama

Abstract: Online exams together with the online learning environments in distance education become prevalent. Even though authentication methods increase online exam security, these methods contain sensitive processes because they require using biometric/ personal information and personal items of the learners. Therefore, authentication in online exams should be further explored. Within this context, the current study aimed to examine the authentication methods that can be utilized in online exams through online learners' viewpoints. A cross-sectional survey design was used for this study. The study was conducted with a sample of 186 total students to find the most reliable online exam authentication method according to online learners. The results showed that online learners thought biometric and information-based authentication methods were more reliable than other methods. However, it was found that most of the online learners are hesitant about the reliability of the authentication methods used in online exams.
Keywords: Distance education, e-learning, e-exam, assessment and evaluation, authentication

Giriş

Yükseköğretim kurumları daha fazla öğrenene ulaşmak ve eğitim fırsatı sunmak için ön lisans, lisans ve lisansüstü düzeyinde uzaktan öğretim yöntemine dayalı programlar açmaktadır. Uzaktan öğretim yoluyla açılan bu programların sayısı ise her geçen gün artmaktadır. Bunun yanı sıra çoğu yükseköğretim kurumu kampüs içindeki derslerin bir kısmını uzaktan öğretim yöntemiyle vermektedir. Uzaktan öğretim programları ile uzaktan öğretim yoluyla verilen derslere ilişkin ölçme değerlendirme süreçleri yüz yüze ve elektronik ortamda gözetimli ya da gözetimsiz olarak gerçekleştirilmektedir. Ancak gözetimsiz olarak yapılan elektronik sınavların (e-sınav) genel başarıya katkısı düşük oranda tutulmaktadır. Bu oran Türkiye'de Yükseköğretim

* Öğr. Gör. Dr., Anadolu Üniversitesi, Açıköğretim Fakültesi, Eskişehir, Türkiye. ORCID: 0000-0002-4520-642X, e-posta: arasbozkurt@gmail.com
** Öğr. Gör. Dr., Bilecik Şeyh Edebali Üniversitesi, Bozüyük Meslek Yüksekokulu, Bilecik, Türkiye. ORCID: 0000-0001-9174-4299, e-posta: hasanxucar@gmail.com

Gönderi Tarihi: 23.11.2017 - Kabul Tarihi: 29.06.2018

Kurulu (YÖK) (2013) tarafından yayımlanan Yükseköğretim Kurumlarında Uzaktan Öğretime İlişkin Usul ve Esaslara göre yüzde 20'den fazla olamamaktadır. Bu durum tamamen bu ortamlarda yapılan sınavların güvenliği ile ilgilidir. Bu sınavlarda yaşanan ve/veya yaşanması muhtemel akademik usulsüzlükler ile bilgi ve iletişim teknolojilerinde yaşanan gelişmeler uzaktan eğitim ortamlarında kullanılan ölçme değerlendirme süreçlerinde teknoloji destekli kimlik doğrulama yöntemlerinin kullanımının artmasını sağlamıştır. Uzaktan eğitimin e-öğrenme modeliyle çevrimiçi verildiği bu süreçlerde ölçme değerlendirmenin büyük bir yüzdesi çoğu zaman gerçek zamanlı ve gözetimli yüz yüze sınavlar veya öğrenci tarafından hazırlanan ödev ve projelerle sağlanmaktadır. Bununla beraber uzaktan eğitimin esnek öğrenme fırsatı sunmasının temel alındığı ölçme değerlendirme süreçlerinde güvenliği ve kimlik doğrulamayı sağlamak için geleneksel yöntemlerin kullanılması uzaktan eğitimin her zaman her yerde eğitim anlayışıyla çelişmektedir. Ortaya çıkan bu sınırlılığı azaltabilmek için günümüzde teknoloji destekli farklı kimlik doğrulama yöntemleri kullanılmaktadır. Bu bağlamda uzaktan öğrenenlerin akademik usulsüzlükleri azaltmak için çevrimiçi sınavlarda hangi kimlik doğrulama yöntemlerinin daha etkili olacağına ilişkin görüşlerinin belirlenmesi önemli bir konu olarak görülmektedir. Buradan hareketle bu çalışmanın amacı uzaktan öğrenenlerin çevrimiçi öğrenme ortamlarında yapılan ölçme değerlendirme süreçlerinde kimlik doğrulama yöntemlerine ilişkin görüşlerini belirlemektir.

Alanyazın taraması

Günümüzde uzaktan eğitimde e-öğrenme modeli, eğitimde ana akımın bir parçası olmuştur (Allen ve Seaman, 2008). Sürekli gelişen ve kendini güncelleyen teknolojilerle öğrenme içerikleri etkili bir biçimde sunulabilmektedir. Bununla beraber e-öğrenme süreçlerinde akademik güven bağlamında birçok kaygı ilgili alanyazında dile getirilmektedir (Alwi ve Fan, 2010; Keskin ve Güneş, 2015; Özen, 2016; Ramim ve Levy, 2006; Varol ve Karabatak, 2002). Bu kaygılardan bir tanesi e-öğrenme süreçlerinde yapılan çevrimiçi sınavlarda öğrencilerin kimliklerini doğrulamada çoğu zaman yetersiz kalmasıdır (Flior ve Kowalski, 2010). Bu sınırlılığı ortadan kaldırmak için çoğu kurum sınavları gözetimli olarak yüz yüze ortamda yapmaktadır (Gunasekaran, McNeil ve Shaul, 2002). Ancak bu tür yaklaşımlar birçok öğrencinin eğitim veren kurumlardan uzak olduğunu düşündüğümüzde pratik değildir ve e-öğrenmenin esneklik ilkesiyle çelişmektedir (Levy ve Ramim, 2007). Böyle bir yaklaşımın kabul görmesinin sebeplerinden birisinin de kurumların kopya çekme ve intihal gibi durumları ortadan kaldırma isteği olduğu söylenebilir.

Yapılan araştırmalar öğrenenlerin çevrimiçi sınavda kopya çekilebileceğine inandıkları (King, Guyette ve Piotrowski, 2009), çevrimiçi sınavlarda kopya çekme eğiliminde oldukları (Chapman, Davis, Toy ve Wright, 2004), çevrimiçi sınavlarda daha kolay kopya çekilebileceğini düşündükleri (Hillier, 2014) ve öğrenenlerin geleneksel sınavlara göre çevrimiçi sınavlarda daha çok kopya çektiklerini göstermektedir (Lanier, 2006). Çevrimiçi yapılan e-sınavların güvenilirliğiyle ilgili durumlar aşağıdaki gibi açıklanmıştır (Sindre ve Vegendla, 2015):

- Başka birisini taklit etme: Öğrencinin yerine sınava başkasının girmesi.
- Yardım/İşbirliği: Sınavda izin verilmemesine rağmen öğrencilerin başkalarından yardım alması veya sınava yönelik işbirlikçi bir eyleme girişmesi.
- İntihal: Doğru bir şekilde referans vermeden başkasının ifadelerini veya düşüncelerini kendi düşünceleri gibi kullanması.
- İzinsiz destek materyali kullanması: Sınavlarda izin verilmemesi veya bu yönde sınırlama olmasına rağmen öğrencinin materyal (örn: sözlük) veya araçları (örn: hesap makinası) kullanması.
- Zaman ihlali: Belirtilen zamandan önce sınava başlanması veya öğrencinin kendisine tanınan zamandan daha fazla süreyi kullanması.

- Sonuçları etkilemek için öğrencinin yalan söylemesi: Sınavı yapan kişiye öğrencinin yalan söyleyerek (örn: hasta olduğunu söylemek) veya gerçekte olmayan bir problemi yaşadığını ifade ederek (örn: bağlantı hatası) sınav sonucunu etkilemeye çalışması.
- Soru kaçakçılığı: Bazı kurumlar aynı veya benzer soruları farklı dönemlerde kullanabilmektedir. Soruların bu şekilde elde edilmesi veya sınavda sorulan soruların bu amaçla kullanılması.

Yukarıda bahsedilen akademik usulsüzlüklerden dolayı çevrimiçi ölçme değerlendirme süreçlerinde yüz yüze ölçme değerlendirme süreçlerine göre akademik güvensizlik daha fazla hissedilmektedir. Bu güvensizliğin temelinde ise öğreten ve öğrenenlerin fiziksel olarak birbirlerinden uzakta olmaları ve öğretenlerin e-sınav gibi ölçme ve değerlendirme süreçlerinde kendilerinden beklenen güvenlik unsurunu yeterince sağlayamayacakları düşüncesi yatmaktadır (Jung ve Yeom, 2009; Ramu ve Arivoli, 2013). Bununla beraber kopya çekmek ve intihal gibi akademik güvensizlik daha geniş bir bakış açısıyla ele alındığında yükseköğretimde daha önceden var olan ve halen devam eden bir durum olduğu söylenebilir (Lin ve Wen, 2007). Dolayısıyla bu durumu e-öğrenme gibi çevrimiçi süreçlerde azaltabilmek için farklı kimlik doğrulama sınıflandırmaları geliştirilmiş ve akademik güvensizlikten kaynaklanan sorunlar ortadan kaldırılmaya çalışılmıştır.

Kimlik doğrulama faktörleri

Bilgisayar ve bilgi güvenliği alanlarında kullanılan kavramsal yaklaşımlardan biri de CIA üçlemesidir (confidentiality [gizlilik], integrity [bütünlük] and availability [uygunluk]) (Whitman ve Mattord, 2011). CIA kavramsal yaklaşımına göre bilgi güvenliği üç çeşit tehdit ortadan kaldırıldığında sağlanır. Bu tehditler: gizlilik, bütünlük ve uygunluktur (Parker, 2010; Whitman ve Mattord, 2011). Bunun yanı sıra, bilgi güvenliği süreçleri üç temel aşamadan oluşmaktadır: kimlik tanıtımı (identification), kimlik doğrulama (authentication) ve yetkilendirmedir (authorization) (Schneier, 2003). Bu süreçlerden kimlik doğrulama üç faktör ile açıklanmaktadır. Bunlar öğrencinin bildiği şeyleri ilgilendiren bilgi faktörlü yaklaşımlar (Örn: pin kodu veya şifre); öğrenciye ait bir şey ile ilgili olabilecek sahiplik faktörlü yaklaşımlar (Örn: erişim sağlayan akıllı kartlar) ve son olarak öğrencinin biyolojik olarak sahip olduğu veya biyolojik olarak yapabildiği bir şeyle ilgili biyometrik/kalıtımsal faktörlü yaklaşımlardır (Örn: parmak izi veya yazı yazma şekli) (Aggrawal, 2012; Furnell, 2007; Ramu ve Arivoli, 2013).

Şekil 1. Kimlik Doğrulama Faktörleri (Chandra ve Calderon, 2003).

***Bilgi tabanlı faktörler*:** Bu yaklaşımları incelediğimizde en çok kullanılan yöntemin kullanıcıların bilebileceği şeyler ile sağlanan bilgi tabanlı yöntem olduğu görülmektedir. Bu yöntemde kullanılan kimlik doğrulama şekilleri genellikle pin kodu veya şifre şeklindedir. Çoğu durumda güvenlik düzeyini arttırmak için annenin kızlık soyadı gibi ikincil sorularla kimlik doğrulaması sağlanmaya çalışılmaktadır. Bu yaklaşım, maliyet açısından çok ekonomik olması, kullanımının kolay olması ve kullanıcılar tarafından sıklıkla tercih edilmesinden dolayı üstünlüğe sahiptir. Ancak bu yaklaşım bazı sınırlılıklara da sahiptir. Bunlardan birincisi, oluşturulan kodlar veya şifreler çoğu zaman çok basit olmakta ve başkaları tarafından çok çabuk şekilde kırılabilmektedir. Bir diğer sınırlılık ise bu şifreler veya kodlar başkalarıyla paylaşıldığında çevrimiçi ortamlarda yapılan sınavlarda kopya çekme durumu kolaylıkla sağlanabilmektir. Bunun nedeni kod ve şifrelerle erişimin sağlanması, ama kişinin gerçek kişi olup olmadığının doğrulanamamasıdır.

***Nesne/sahiplik tabanlı faktörler*:** Bir diğer yaklaşım ise belirli nesnelerin kullanıldığı yaklaşımdır. Buna göre erişim, sahip olunan bir nesne ile sağlanmaktadır. Bu yaklaşımda kullanılan kimlik doğrulama nesnelerine manyetik kartlar, akıllı kartlar, dijital anahtarlar, belirli objeler veya günümüzde akıllı cihazların tanıtılmasıyla sağlanan erişim örnek olarak verilebilir. Eğer sınavlar herhangi bir yerde değil de belirli sınav merkezlerinde yapılırsa etkili bir şekilde kullanılabilmektedir. Bununla beraber bu yöntem de bazı sınırlılıklara sahiptir. Örneğin kod ve şifrelerle sağlanan erişime benzer bir şekilde belirli nesnelerin kullanılmasıyla erişim sağlanabilmekte ancak erişimi sağlayan kişinin doğrulamasını yapmakta yetersiz kalmaktadır. Bu tür nesnelerin üretilip kullanıcılara sağlanması da ayrıca maliyetlidir.

***Kalıtımsal/biometrik tabanlı faktörler*:** Son olarak kimlik doğrulama süreçlerinde biyometriklerin kullanımı erişimi sağlamak ve kişinin sistemde tanımlanan kişi olduğunu doğrulamak için etkili bir yöntemdir. Bu yaklaşım kendi içerisinde ikiye ayrılmaktadır. Bunlardan birincisi parmak izi, el/avuç izi, kan damarı deseni, göz/iris tanıma gibi tanımlamalara olanak sağlayan fizyolojik biyometrik teknikler; ikincisi ise konuşma tarzı, imza atma şekli, klavyede yazı yazma stili gibi daha sonradan kazanılan örüntüleri tanıyan davranışsal biyometrik tekniklerdir. Bu yöntem kişilerin erişim sağlaması ve kimliklerinin doğrulanması bakımından üstünlüklere sahiptir. Bununla beraber bu teknolojiler maliyet bağlamında çok ekonomik değildirler. Bu yöntem kimlik doğrulamadaki üstünlüklerinin yanı sıra kişisel verilerin güvenliği, etik durumlar ve sosyo-ekonomik açıdan bazı sınırlılıklara sahiptir. Örneğin öğrenciler biyometrik bilgilerinin üçüncü kişilerle paylaşılıp saklanmasını istemeyebilir. Bu durumdan farklı olarak kültürel veya sosyo-ekonomik sebeplerden dolayı biyometrik bilgilerin paylaşılması bazı kullanıcılar için sorunlu bir durum olabilmektedir.

Araştırmanın amacı

Bu çalışma Türkiye'de bir devlet üniversitesinde yükseköğretim düzeyinde uzaktan eğitim yoluyla ders alan öğrenenlerin çevrimiçi öğrenme ortamlarında kimlik doğrulama yöntemlerine ilişkin görüşlerini belirleyerek ilgili alanyazına katkı sağlamayı amaçlamaktadır. Çevrimiçi öğrenme ve ölçme değerlendirme süreçlerinin eğitimde ana akımın bir parçası olduğu günümüzde çalışma bulgularının ileri araştırmalara dayanak olacağı ve yol göstereceği düşünülmektedir. Bu doğrultuda bu çalışmanın genel amacı çevrimiçi öğrenme ortamlarında yapılan ölçme değerlendirme süreçlerinde kimlik doğrulama yöntemlerine ilişkin öğrenenlerin görüşlerini belirlemektir. Bu bağlamda aşağıdaki araştırma sorusuna yanıt aranmıştır.

- Yükseköğretimde uzaktan öğrenim gören öğrenenler çevrimiçi ortamlarda ölçme değerlendirme süreçlerinde kimlik doğrulama yöntemleri hakkında ne düşünmektedir?

Yöntem

Araştırma modeli

Bu çalışma bağlamında nicel veri toplama yöntemlerinden tarama modelinde gerçekleştirilmiş ve kesitsel desen kullanılmıştır. Bu tür tarama çalışmaları belirli bir zaman diliminde yürütülür

ve hedeflenen örneklemin tutumlarını, inançlarını, düşüncelerini ve davranışlarını belirlemek için kullanılabilir (Creswell, 2004). Bu çalışma türünde araştırmacının bir etkisi bulunmaz ve var olan durum olduğu gibi betimlenmeye çalışır. Bu araştırmada ilgili araştırma modelinin tercih edilmesi; ulaşılabilir örneklemde yer alan katılımcı sayısının sınırlı olması, bulguların betimsel istatistiklerle analiz edilmesi ve çevrimiçi kimlik doğrulama süreçlerinin yeni teknolojilere dayalı yaklaşımları içermesinden dolayı öğrenen görüşlerini inceleme gereksiniminden kaynaklanmaktadır.

Veri toplama aracı ve analiz süreci

Çalışmada veri toplama aracı olarak araştırmacılar tarafından geliştirilen ve 14 sorudan oluşan çevrimiçi bir anket uygulanmıştır. İlgili anket alanyazında yer alan kimlik doğrulama yöntemlerine göre oluşturulmuş, anket maddelerinin kapsam geçerliğini arttırmak için açık ve uzaktan öğrenme alanında doktora derecesine sahip başka araştırmacılardan görüş alınmış ve geliştirilen anketinin anlaşılırlığını ölçmek için başka bir devlet üniversitesinde uzaktan eğitim alan 15 katılımcıyla pilot uygulama yapılmıştır. Yanıtlanan anket 0,883 Cronbach Alpha değerine sahiptir. Bu bağlamda geliştirilen anketin yüksek düzeyde iç tutarlık değerlerine sahip olduğu söylenebilir. Geliştirilen anketin çağrı linki bir ay süreyle öğrenme yönetim sisteminde aktif tutulmuştur. Çağrı linki ilk sayfada çalışmaya katılım onay formunu sunmuş ve çalışmaya katılmayı kabul eden öğrenenlerin ankete ulaşması sağlanmıştır. Katılımcılar anketi isim belirtilmeden yanıtlamıştır. Katılımcılara kimlik doğrulama yöntemleri ile ilgili kısa bilgi verilmiş ve katılımcılar bu yöntemlerinin güvenirliğine ilişkin 5'li Likert üzerinden (1-Kesinlikle katılmıyorum, 5-Kesinlikle katılıyorum) değerlendirmelerde bulunmuştur. Çalışmanın güvenirliğini artırmak için geliştirilen anket formunda yer alan maddelerden biri kontrol maddesi olarak tasarımlanmış ve ankete ters madde olarak konulmuş; gerçek madde ve dönüştürülen her iki maddeye de aynı cevabı veren katılımcıların yanıtları analiz kapsamından çıkarılmıştır. Elde edilen verilerin analizinde betimsel istatistiklerden yararlanılmıştır.

Örneklem

Çalışmanın evreni bir devlet üniversitesinde eğitim gören ve uzaktan öğretim yöntemiyle ders alan ön lisans ve lisans öğrencileridir. Çalışmada ikinci araştırmacının uzaktan eğitim yoluyla verdiği derslere katılan öğrenenlerden veri toplanmış, bu bağlamda ulaşılabilir örneklem yöntemi tercih edilmiştir. Bu öğrenenler, bir öğretim yılı boyunca 4 çevrimiçi sınava katılmış ve kimlik doğulama yöntemlerinden kullanıcı adı/şifre yöntemini kullanmıştır. Çalışmaya katılım çağrısı öğrenme yönetim sistemi üzerinden yapılmış, 601 öğrenci çağrı metnine ve çalışma katılım onay formuna ulaşmıştır. Anket çağrısı ulaştırılan 601 katılımcıdan 363'ü çalışmaya katılmayı kabul etmiştir. Dolayısıyla ankete geri dönüş oranı %60,3'tür. Çalışmaya yanıt veren katılımcıların tutarlılığını sağlamak, içtenlikle ve dikkatli bir şekilde yanıt verdiklerini belirleyebilmek için anket maddelerinden biri ayrıca dönüştürülerek ters madde olarak verilmiş ve kontrol maddesi olarak kullanılmıştır. Dönüştürülen ters maddeye ve ilgili maddeye aynı yanıtı veren katılımcılar belirlenmiş ve toplam 152 katılımcı yanıtı araştırmadan çıkarılmıştır. Bu duruma ek olarak tüm sorulara aynı yanıtı veren 25 katılımcının cevabı da analizlerden çıkarılmış ve geriye kalan 186 katılımcı araştırmanın örneklemine dâhil edilmiş ve analizler bu örneklem üzerinden yapılmıştır.

Çalışmanın önemi ve sınırlılıkları

Bu çalışma, çevrimiçi ölçme değerlendirme süreçlerinde kullanılan kimlik doğrulama yöntemlerini Türkiye bağlamında uzaktan eğitim yoluyla ders alan yükseköğretim öğrencilerini konu alan öncü çalışmalardan biridir. Çalışmanın katılımcıları üniversitede YÖK tarafından zorunlu ders olarak belirtilen ortak dersleri (Türk Dili, Atatürk İlke ve İnkılap Tarihi ve Yabancı Dil dersleri) uzaktan eğitim yoluyla alan öğrenenlerdir. Dolayısıyla uzaktan eğitim derslerini seçmeli olarak alan öğrenenlerle benzer ileri çalışmalar yapılması bu çalışma bulgularıyla karşılaştırma yapmaya olanak sağlayacağı düşünülmektedir. Çalışmanın bu bağlamda önemli olduğu ve ileri araştırmalara dayanak olabileceği düşünülmektedir. Bunun yanında çalışma bazı

sınırlılıklara sahiptir. Öncelikle araştırma verileri sadece bir devlet üniversitesinde öğrenim gören yükseköğretim öğrencilerinden toplanmıştır. Öğrenenlerin çevrimiçi ölçme değerlendirme süreçlerinde kullanılan kimlik doğrulama süreçlerine yönelik tercihleri nicel betimsel istatistiklerle analiz edilmiştir. Araştırmanın örneklem büyüklüğü araştırma bulgularını genellemek bağlamında ayrıca sınırlılıklara sahiptir. Araştırma katılımcılarının geliştirilen ankette yer alan kimlik doğrulama yöntemlerine yönelik deneyimlerinin olmayabileceği ayrıca bir sınırlılık olarak değerlendirilmektedir.

Bulgular ve Tartışma

Demografik bulgular

Çalışmaya katılan öğrencilerin %52,1'i erkek, %47,8'i kadındır. Katılımcıların %51,7'si ön lisans, %47,3'ü ise lisans öğrencisidir. Katılımcıların %53,2'si daha önceden uzaktan eğitim deneyimine sahip olduklarını ifade etmişler, %46,8'i ise daha önce uzaktan eğitim deneyimine sahip olmadıklarını ifade etmişlerdir (Tablo 1).

Tablo 1.
Demografik Bilgiler (N=186).

Cinsiyet	*f*	%
• Erkek	97	52.2
• Kadın	89	47.8
Öğretim Türü		
• Ön lisans	98	52.7
• Lisans	88	47.3
Uzaktan Eğitim Deneyimi		
• Evet	99	53.2
• Hayır	87	46.8

Çalışmaya katılan öğrenenlerin demografik verileri incelendiğinde cinsiyet, devam ettikleri öğrenim türü ve uzaktan eğitim deneyimleri bağlamında dengeli bir dağılım olduğu görülmektedir. Katılımcıların yaşları incelendiğinde 18-22 yaş aralığında dağılımın yoğunlaştığı görülmektedir (Tablo 2). Katılımcıların yaş ortalaması 19.90'dır.

Tablo 2.
Katılımcıların Yaşları (N=186).

Yaş	*f*	%
• 18	32	17.2
• 19	58	31.2
• 20	52	28.0
• 21	24	12.9
• 22	11	5.9
• 23	3	1.6
• 24+	6	2.2

Çevrimiçi ölçme değerlendirme süreçlerinde kimlik doğrulama yöntemlerine ilişkin bulgular

Bu çalışma bağlamında katılımcılara çevrimiçi sınavlarda kullanılabilecek 14 kimlik doğrulama yöntemi sorulmuştur (Tablo 3). Verilen yanıtlardan katılıyorum ve kesinlikle katılıyorum

seçenekleri toplanarak katılımcı yanıtlarına göre ortaya çıkan en güvenilir kimlik doğrulama sürecinden daha az güvenilir bulunan güvenlik doğrulama sürecine doğru bir sıralama yapılıştır.

Katılımcıların çevrimiçi sınavlarda kullanılabilecek kimlik doğrulama yöntemlerine ilişkin yanıtları incelendiğinde öğrencilerin fizyolojik biyometrik yaklaşımlardan parmak izi/avuç izi eşleşmesini (%56,4) en güvenilir kimlik doğrulama yöntemi olarak kabul ettikleri görülmektedir. Bilgi tabanlı yaklaşımlardan kullanıcı adı ve parola kullanımı ikinci (%54,9), kişisel bilgilerin güvenlik sorusu şeklinde sorulması üçüncü (%51,6) en güvenilir kimlik doğrulama yaklaşımı olarak belirtilmiştir. Bununla beraber ilk sıralarda yer alan kimlik doğrulama yöntemleri arasında yüzdelik durumlarına göre belirgin bir farkın olmadığı görülmektedir.

Tablo 3.
Yükseköğretim Öğrencilerinin Çevrimiçi Ölçme Değerlendirme Süreçlerinde Kimlik Doğrulama Yöntemlerine İlişkin Görüşleri (N=186).

Çevrimiçi ölçme değerlendirme süreçlerinde:	**Kesinlikle katılmıyorum**		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle katılıyorum**		**Ortalama**	**Standart Sapma**
	f	**%**	*f*	**%**	*f*	**%**	*f*	**%**	*f*	**%**		
1-parmak izi/avuç izi tanımlaması yapılarak kimlik doğrulaması yapılan sınavlar güvenlidir.	24	12,9	28	15,1	29	15,6	67	36,0	38	20,4	3,36	1,313
2-kullanıcı adı ve parola kullanılarak yapılan sınavlar güvenlidir.	17	9,1	31	16,7	36	19,4	60	32,3	42	22,6	3,42	1,259
3-kişisel bilgileriniz ile ilgili sorular sorularak (anne kızlık soyadı, doğum yeri vb.) yapılan kimlik doğrulaması güvenlidir.	19	10,2	36	19,4	35	18,8	56	30,1	40	21,5	3,33	1,289
4-dijital imza kullanılarak kimlik doğrulaması yapılan sınavlar güvenlidir.	19	10,2	33	17,7	38	20,4	71	38,2	25	13,4	3,27	1,200
5-profil fotoğrafım çekilerek yüz tanıma teknolojisine dayalı olarak kimlik doğrulaması yapılan sınavlar güvenlidir.	24	12,9	34	18,3	34	18,3	69	37,1	25	13,4	3,20	1,256
6-daha önce verilen veya sınav esnasında üzerime kayıtlı mobil cihazlara gelen bir pin kodu aracılığıyla kimlik doğrulaması yapılan sınavlar güvenlidir.	16	8,6	39	21,0	38	20,4	57	30,6	36	19,4	3,31	1,243
7-bizlere verilen kimlik kartını veya başka bir nesneyi tanıyan araçlarla yapılan kimlik doğrulaması güvenlidir.	16	8,6	36	19,4	44	23,7	62	33,3	28	15,1	3,27	1,187
8-göz tanıma teknolojisi ile kimlik doğrulaması yapılan sınavlar güvenlidir.	27	14,5	32	17,2	38	20,4	58	31,2	31	16,7	3,18	1,307
9-örnek ses kaydım alınarak ses tanıma teknolojisine dayalı olarak kimlik doğrulaması yapılan sınavlar güvenlidir.	28	15,1	45	24,2	45	24,2	55	29,6	13	7,0	2,89	1,190
10-yüzümün değişik açılardan video görüntüsü alınarak yüz tanıma teknolojine dayalı olarak kimlik doğrulaması yapılan sınavlar güvenlidir.	38	20,4	42	22,6	42	22,6	48	25,8	16	8,6	2,80	1,170
11-İnternet üzerinden yapılan sınavlarda IP adresi kontrolü ile kimlik doğrulaması yapılan sınavlar güvenlidir.	26	14,0	44	23,7	54	29,0	47	25,3	15	8,1	2,90	1,170
12-dokunmatik bir ekran üzerine	31	16,7	43	23,1	53	28,5	42	22,6	17	9,1	2,84	1,214

imza atılarak ve el yazısı yazılarak kimlik doğrulaması yapılan sınavlar güvenlidir.												
13-sürekli açık kamera ve mikrofon sistemi ile kimlik doğrulaması yapılan sınavlar güvenlidir.	35	18,8	48	25,8	46	24,7	45	24,2	12	6,5	2,74	1,204
14-klavye üzerine yazdığım örnek yazı ile yazı yazma şeklim örneklenip sınavlarda klavye kullanma tarzım ile eşleştirme yapılarak kimlik doğrulaması yapılan sınavlar güvenlidir.	39	21,0	59	31,7	45	24,2	32	17,2	11	5,9	2,55	1,172

Katılımcı yanıtları incelendiğinde hemen hemen tüm kimlik doğrulama yöntemleri için katılımcılar arasında yaklaşık %20 oranında kararsızım ifadesini işaretleyenlerin olması dikkat çekicidir. Bunun nedeni olarak katılımcıların ilgili yöntemler konusunda yeterli düzeyde bilgiye sahip olmadıkları ve/veya hangi yöntemin daha güvenli olduğu konusunda tam emin olmadıkları düşünülmektedir.

İlgili alanyazın incelendiğinde her bir yöntemin güçlü ve zayıf yanları olduğu anlaşılmakta ve tek bir yöntemin bir diğerine göre üstün olmadığı görülmektedir (Bhagat, 2014). Bu çalışmanın bulguları da bu düşünceyi destekler niteliktedir. Araştırma bulguları incelendiğinde öğrencilerin belirli bir yöntemi diğerlerinden daha fazla güvenilir bulmadıkları, maddeler arasında yüzdesel geçişlerin aşamalı bir şekilde gerçekleştiği görülmektedir. Ayrıca bu yöntemlerin ne kadar güvenilir olduğuna yönelik kararsız olanların oranı da dikkat çekicidir.

Engelbrecht ve Harding (2003) yaptıkları çalışmada öğrencilerin çoğunluğunun (%56,6) çevrimiçi sınavları tercih ettiklerini ifade etmişler, ancak öğrencilerin yaklaşık olarak yarısı da geleneksel sınavlarını tercih ettiklerini belirtmişlerdir. Her ne kadar bu çalışma bulgularıyla doğrudan örtüşmese de bu çalışma kapsamında e-sınavlarda uygulanabilecek kimlik doğrulama yöntemlerinin ilgili çalışmada çevrimiçi sınavlara olan yüzdesel oranla benzeştiği görülmektedir. Yine bu çalışmada belirgin bir şekilde ifade edilen kararsızım seçeneğinin Engelbrecht ve Harding (2003) tarafından yapılan çalışmada da olduğu gibi geleneksel sınavı tercih eden öğrencilerden kaynaklanabileceği düşünülmektedir.

Levy, Ramim, Furnell ve Clarke (2011) 163 katılımcı ile yaptıkları çalışmada bu çalışmanın bulgularını doğrular nitelikte öğrencilerin %56'sının parmak izi kullanılarak kimlik doğrulaması yapılmasına istekli olduklarını ortaya çıkarmıştır. Her ne kadar bu yüzde kabul edilebilir bir orana karşılık gelse de parmak izi gibi taklit edilmesi neredeyse imkânsız bir kimlik doğrulama yönteminin belirgin bir çoğunlukla güvenilir bulunmaması ilginç bir bulgudur. Dolayısıyla kimlik doğrulama yöntemlerinin güvenilir bulunup bulunmamasında başka değişkenlerin de etkili olabileceği düşüncesi güçlenmektedir.

Sonuç ve Öneriler

Bu çalışma kapsamında çevrimiçi sınavlarda kullanılabilecek kimlik doğrulama yöntemlerine ilişkin öğrenen görüşleri incelenmiştir. Bilgi tabanlı, nesne/sahiplik tabanlı ve kalıtımsal/biometrik tabanlı yaklaşımlar incelendiğinde hiçbir yaklaşımın öğrenenler tarafından yüksek oranda kabul görmediği ve genellenebilir çözümler sunmadığı görülmektedir. Hiç şüphesiz biometrik yaklaşımlar gibi bazı kimlik doğrulama yaklaşımları çok güçlü çözüm önerileri üretebilse de çoğu zaman bu yaklaşımlar kullanıcılar tarafından kabul görmemekte veya maliyetli bulunduğu için kurumlar tarafından tercih edilememektedir. Dolayısıyla ilgili alanyazında yer alan tartışmalara ve bu çalışma bulgularına dayanarak en güvenilir kimlik doğrulama yönteminden daha çok en güvenilir kimlik doğrulama kombinasyonlarından bahsetmek daha doğru bir yaklaşım olabilir. Ayrıca kimlik doğrulama yönteminin güvenilir olmasının yanı sıra hangi bağlamlarda kullanılacağının da belirleyici olduğu düşünülmektedir. Örneğin çevrimiçi sınavın 100 kişilik bir grup mu yoksa 10000 kişilik bir kitle mi olduğu, sınavın resmi bir kurumda mı yapıldığı yoksa herhangi bir yerde mi yapıldığı, bu sınavlara

katılacakların kültürel ve sosyo-ekonomik geçmişleri ve sınavı yapan kurumun teknolojik altyapı olanaklarının da belirleyici değişkenler olduğu düşünülmektedir.

Bu çalışma bulguları ve ilgili alanyazında ele alınan konular bağlamında aşağıda yer alan öneriler ileride yapılacak araştırmalar için önerilebilir. Çevrimiçi sınavlarda her ne kadar ileri düzey kimlik doğrulama yöntemleri kullanılsa da öğrencilerin bu sınavlara yeterince güvenmedikleri veya bu sınavlarda kullanılan kimlik doğrulama yöntemleriyle sağlanan güvenlik yöntemleri hakkında kararsız oldukları görülmektedir. Bu durumun sebebinin kişisel verilerin korunması bağlamında gerekli yasal düzenlemelerin yeterince yapılmaması veya öğrencilerin kişisel bilgilerinin korunacağı konusunda bilgi sahibi olmamalarından kaynaklanabileceği düşünülmektedir. Dolayısıyla ne tür düzenlemelere gereksinim olduğu yönünde çalışmalar yapılarak yetkili mercilere rehber niteliğinde çalışmalar yapılmasının ilgili alanyazına olduğu kadar ilgili alanda çalışmalar yapan kanun koyuculara da yardımcı olabileceği düşünülmektedir. Bu duruma ek olarak bu çalışmaya katılan öğrencilerin çevrimiçi sınavlarda akademik usulsüzlük yapmalarından dolayı öz deneyimsel bir yaklaşımla güvensizliklerini ve/veya kararsızlıklarını ifade etmiş olabilecekleri de dikkate alınmalıdır. Dolayısıyla öğrencilerin akademik usulsüzlük (kopya çekme, intihal vb.) yönündeki algılarını derinlemesine inceleyen çalışmaların alanyazına katkı sağlayacağı düşünülmektedir. Ayrıca çevrimiçi ölçme değerlendirme süreçlerinde kullanılan kimlik doğrulama yöntemlerinde kişisel verilerin paylaşılması gerekliliğinin cinsiyet bağlamında öğrenen tercihlerini etkileyip etkilemediğinin belirlenmesine yönelik yapılacak çalışmaların ilgili alanyazına katkı sağlayacağı düşünülmektedir. Bunun yanı sıra öğrenenlerin hangi sebeple kimlik doğrulama yöntemlerini tercih ettiklerinin veya etmediklerinin belirlenmesi için derinlemesine analiz imkânı sağlayacak nitel araştırmalar da önemli çalışmalar olabilir. Son olarak, çevrimiçi ölçme değerlendirme süreçlerinde kullanılan kimlik doğrulama yöntemlerinde öğrenen tercihlerinin belirlenmesine yönelik yapılacak bir ölçek geliştirme çalışmasının bu yönde planlamalar yapan eğitimcilere, öğretim tasarımcılarına ve kurumlara faydalı olacağı düşünülmektedir.

Kaynaklar

Aggrawal, N. (2012). Authentication methods: A review. *Productivity, 52*(4), 243-248.

Allen, I. E. ve Seaman, J. (2008). *Staying the course: Online education in the United States, 2008.* Sloan Consortium.

Alwi, N. H. M. ve Fan, I. S. (2010). Threats analysis for e-learning. *International Journal of Technology Enhanced Learning, 2*(4), 358-371.

Bhagat, V. B. (2014). Student authentication framework for online examination using visual cryptography. *International Journal for Research in Applied Science and Engineering Technology, 2*(7), 316-319.

Chandra, A. ve Calderon, T. G. (2003). Toward a biometric security layer in accounting systems. *Journal of Information Systems, 17*(2), 51-70.

Chapman, K., Davis, R., Toy, D. ve Wright, L. (2004). Academic Integrity in the Business School Environment: I'll Get by with a Little Help from My Friends. *Journal of Marketing Education, 26*, 236-249.

Creswell, J. W. (2004). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research.* Pearson.

Engelbrecht, J. ve Harding, A. (2004). Combing online and paper assessment in a web-based course in undergraduate mathematics. *Journal of Computers in Mathematics and Science Teaching, 23*(3), 217-231.

Flior, E. ve Kowalski, K. (2010, April). Continuous biometric user authentication in online examinations. *Seventh International Conference on Information Technology (ITNG2010)* içinde (s. 488-492). Las Vegas, Nevada, USA.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security, 26*(7-8), 445-51.

Gao, Q. (2012). Biometric authentication to prevent e-cheating. *International Journal of Instructional Technology and Distance Learning, 9*(2), 3-14.

Gunasekaran, A., McNeil, R. D. ve Shaul, D. (2002). E-learning: Research and applications. *Industrial and Commercial Training, 34*(2), 44-54.

Hillier, M. (2014). The very idea of e-Exams: student (pre) conceptions. In *Australasian Society for Computers in Learning in Tertiary Education Conference*. Sydney, Australia.

Jung, I. Y. ve Yeom, H. Y. (2009). Enhanced security for online exams using group cryptography. *IEEE transactions on Education, 52*(3), 340-349.

Keskin, Ö. G. K. ve Güneş, A. (2015). Online sınav sistemlerinde güvenlik sorunları ve güvenli online sınav giriş uygulaması. *Eğitim ve Öğretim Araştırmaları Dergisi, 4*(4), 48-54.

King, C., Guyette, R. ve Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *The Journal of Educators Online, 6*(1).

Lanier, M. (2006). Academic integrity and distance learning. *Journal of Criminal Justice Education, 17*(2), 244-261.

Levy, Y. ve Ramim, M. (2007). A theoretical approach for biometrics authentication of e-exams. *Chais Conference on Instructional Technologies Research* içinde (ss. 93-101), The Open University of Israel, Raanana, Israel.

Levy, Y., Ramim, M. M., Furnell, S. M. ve Clarke, N. L. (2011). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems, 28*(2), 102-113.

Lin, C. H. S. ve Wen, L. Y. M. (2007). Academic dishonesty in higher education—a nationwide study in Taiwan. *Higher Education, 54*(1), 85-97.

Özen, Z. (2016). *Kimlik doğrulaması için tuş vuruş dinamiklerine dayalı bir güvenlik sisteminin yapay sinir ağları ile geliştirilmesi* (Yayımlanmamış doktora tezi). İstanbul: İstanbul Üniversitesi.

Parker, D. (2010). Our excessively simplistic information security model and how to fix it. *ISSA Journal*, 12-21.

Ramim, M. ve Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

Ramu, T. ve Arivoli, T. (2013). A framework of secure biometric based online exam authentication: an alternative to traditional exam. *Int J Sci Eng Res, 4*(11), 52-60.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world.* New York: Springer.

Sindre, G. ve Vegendla, A. (2015). E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures. *Norsk informasjons sikkerhets konferanse (NISK), 8*(1), 34-45.

Varol, A. ve Karabatak, M. (2002). Çevrimiçi uzaktan eğitimde sınav otomasyonu. *II. Uluslararası Eğitim Teknolojileri Sempozyumu ve Fuarı* (16-18 Ekim 2002).

Yükseköğretim Kurulu. (2013). Yükseköğretim kurumlarında uzaktan öğretime ilişkin usul ve esaslar.

Whitman, M. E. ve Mattord, H. J. (2011). *Principles of information security.* Cengage Learning.

Extended Abstract

Introduction

Higher education institutions (HEIs) provide learning opportunities in different levels by benefiting from distance education, mostly through e-learning programs delivered through distance education enable lifelong learning and make education accessible. However, because of the security issues in exams, many HEIs do proctored exams in face-to-face settings, which conflicts with the principle of the flexibility provided through distance education. In digital knowledge age, the e-learning model has become part of the mainstream education. Learning contents can be delivered effectively with ever-evolving and self-updating technologies. However, in the context of academic confidence in the e-learning, many concerns are expressed in related literature. One of these concerns is the inability in confirming the identities of students during online exams in e-learning processes.

The information security processes are related to three important concepts: identification, authentication, authorization. The authentication process is explained with three approaches. These are knowledge-based authentication, object-based authentication, and biometrics-based authentication.

Purpose of the Research and Methodology

Based on above discussions, this research intends to examine the authentication methods in online assessment processes through online learners' viewpoints. For the purposes of the study, the research employed quantitative cross-sectional survey model. An online questionnaire, which included 14 items, was used for data collection. The sample of the study composed of associate and bachelor's degree students in Bilecik Şeyh Edebali University. The call for participation was active in learning management system of the Bilecik Şeyh Edebali University. A total of 601 students accessed to the consent form and 363 students agreed to participate in research. After the initial examination, a total of 186 students were included to research sampling and analysis was carried out according to their answers.

Findings and Conclusion

Of all the research participants, 52.1% were male, and 47.8% were females. 51.7% of the participants were associate and 47.3% are bachelor's degree students. 53.2% of respondents stated that they previously had distance education experience and 46.8% stated that they did not have previous distance education experience.

When participants' responses were examined, it was seen that the students were considered for fingerprint/palm print matching (56.4%) from physiological biometric approaches to be the most reliable authentication method. The second most reliable approach was the use of username and password (54.9%) and the third most reliable approach (51.6%) was the use of personal information as a security question from the knowledge-based approach. However, there appears to be no significant difference between the authentication methods in the first place according to percentiles of participants' preferences.

It is also noteworthy that there is some indication of ambiguity about 20% in participants' responses (those who selected neither agree nor disagree) for almost all authentication methods. It is conceivable, as a basis, that participants do not have sufficient knowledge of the methods involved and/or are not entirely sure which method is safer than the others. In line with the findings of this research, when the related literature is examined, it is understood that each method has strengths and weaknesses, and it seems that one method does not dominate one another.