T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı

Yüksek Lisans Tezi

ÇEVRİM İÇİ SINAVLARDA UYGULANABİLECEK KİMLİK DOĞRULAMA ŞEMALARINA İLİŞKİN ÖĞRETİM ELEMANI VE ÜNİVERSİTE ÖĞRENCİLERİNİN GÖRÜŞLERİNİN İNCELENMESİ

Canan BATTAL
ORCID: 0000-0002-7236-5864

Danışman
Doç. Dr. Şemseddin GÜNDÜZ
ORCID: 0000-0003-1075-0043

Konya – 2023

ÖN SÖZ (TEŞEKKÜR)

Bu çalışmanın konusunun belirlenmesinde ve hazırlanma sürecinin her aşamasında değerli bilgilerini ve zamanını esirgemeyen, her daim çalışmamla yakından ilgilenen, eleştirileriyle yol gösteren Doç. Dr. Şemseddin GÜNDÜZ hocama teşekkürü bir borç bilirim.

Kıymetli eşim Sefa BATTAL'a her şey için çok teşekkür ediyorum.

Tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen, her zaman yanımda olan kıymetli babam Levent YAZICI'ya, değerli annem Sündüs YAZICI'ya, tüm ailemiz için elinden geleni yapan sevgili ablam Hatice Betül ANIK'a ve ihtiyaç duyduğum her an yanımda olan değerli arkadaşım Esra ÇOLAK'a sonsuz teşekkürlerimi ve minnetimi özellikle belirtmek istiyorum. Son olarak beni teyze ve hala yapan güzel yeğenlerim Mirza Berk ANIK ve Alpay YAZICI'ya bana yaşattıkları güzel duygular için çok teşekkür ediyorum.

Canan BATTAL

Haziran 2023

İÇİNDEKİLER

TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Çevrim İçi Sınavlarda Uygulanabilecek Kimlik Doğrulama Şemalarına İlişkin Öğretim Elemanı ve Üniversite Öğrencilerinin Görüşlerinin İncelenmesi başlıklı tez çalışmamın toplam **81** sayfalık kısmına ilişkin, 16/06/2023 tarihinde tez danışmanım tarafından **Turnitin** adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı **%5** olarak belirlenmiştir.

Uygulanan filtrelemeler:

1. Tez çalışması orijinallik raporu sayfası hariç
2. Bilimsel etik beyannamesi sayfası hariç
3. Önsöz hariç
4. İçindekiler hariç
5. Simgeler ve kısaltmalar hariç
6. Kaynaklar hariç
7. Alıntılar dahil
8. 7 kelimeden daha az örtüşme içeren metin kısımları hariç

Necmettin Erbakan Üniversitesi Tez Çalışması Orijinallik Raporu Uygulama Esaslarını inceledim ve tez çalışmamın, bu uygulama esaslarında belirtilen azami benzerlik oranının (%30) altında olduğunu ve intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

16/06/2023

Canan BATTAL

Doç. Dr. Şemseddin GÜNDÜZ

BİLİMSEL ETİK BEYANNAMESİ

Bu tezin tamamının kendi çalışmam olduğunu, planlanmasından yazımına kadar tüm aşamalarında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez hazırlama kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını ve bu kaynakların kaynaklar listesine eklendiğini beyan ederim.

16/06/2023

Canan BATTAL

SİMGELER VE KISALTMALAR

Simgeler

%: Yüzde

***f*:** Frekans

$\bar{X}$: Ortalama

Kısaltmalar

BÖTE: Bilgisayar ve Öğretim Teknolojileri Eğitimi

E-Öğrenme: Elektronik Öğrenme

EYT: Eğitim Yönetim Sistemleri

EYS: Eğitim Yönetim Sistemleri

NIST: Ulusal Standartlar ve Teknoloji Enstitüsü

OTP: Tek Kullanımlık Şifre

PBAF: Profil Tabanlı Kimlik Doğrulama Sistemi

PIN: Kişisel Kimlik Numarası

ÖZET

Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
Yüksek Lisans Tezi

ÇEVRİM İÇİ SINAVLARDA UYGULANABİLECEK KİMLİK DOĞRULAMA ŞEMALARINA İLİŞKİN ÖĞRETİM ELEMANI VE ÜNİVERSİTE ÖĞRENCİLERİNİN GÖRÜŞLERİNİN İNCELENMESİ

Canan BATTAL

Dijitalleşmeye giden dünyada eğitim süreçlerinde de büyük dönüşümler yaşanmaktadır. Sadece öğrenme süreçlerinde değil, ölçme değerlendirme süreçlerinde de özellikle çevrim içi ortamlarda büyük yenilikler oluşmaktadır. Bu çevrim içi sınavlara erişim için çeşitli kimlik doğrulama faktörlerine bağlı kimlik doğrulama şemaları kullanılmaktadır. Bu çalışmanın amacı çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin öğretim elemanı ve üniversite öğrencilerinin görüşlerinin incelenmesidir. Araştırma 2022-2023 eğitim yılında gerçekleştirilmiştir. Çalışma 9 farklı üniversitede, 9 farklı bölümde görev yapan öğretim elemanları ile gerçekleştirilmiştir. Bununla birlikte çalışma 7 farklı üniversitenin, 8 farklı bölümünde öğrenim gören öğrencilerin katılımından oluşmaktadır. Bu doğrultuda 10 öğretim elemanı ve 8 öğrenci ile yarı yapılandırılmış görüşme tekniği kullanılarak veriler toplanmıştır. Çalışma öncesinde katılımcılara konuya ilişkin bir video-animasyon izletilmiştir. Elde edilen veriler içerik analizi ile çözümlenmiştir. Bilgi güvenliği unsurlarına göre değerlendirilen kimlik doğrulama şemalarının tercih edilme durumları incelenmiştir. Yapılan araştırma sonucunda öğretim elemanlarının verdiği yanıtlara göre kullanılabilirlik için yaygın kullanılan kimlik doğrulama şeması parola olarak belirlenmiştir. Öğretim elemanları gizlilik için sırasıyla parola, tek kullanımlık şifre ve fiziksel aygıtı, güvenlik için yüz tarama ve parmak izi şemalarını tercih etmişlerdir. Yapılan araştırma sonucunda üniversite öğrencilerinin verdiği yanıtlara göre kullanılabilirlik için yaygın kullanılan kimlik doğrulama şeması parola olarak belirlenmiştir. Tercihler gizlilik için sırasıyla parola, tek kullanımlık şifre ve fiziksel aygıt olmuştur. Güvenlik için yüz tarama ve parmak izi olmuştur. Verilen yanıtlar bilgi güvenliği unsurları (kullanılabilirlik, gizlilik, güvenlik) bakımından değerlendirildiğinde elde edilen sonuçlar parola ve tek kullanımlık şifre gibi yaygın kullanılan kimlik doğrulama şemalarının, kimlik hırsızlığıyla mücadele etmek ya da güvenliği sağlamak için yeterli olmadığı yönündedir. Bu tür kimlik doğrulama şemalarının kolay bir şekilde unutulabilir, kaybolabilir, tahmin edilebilir, çalınabilir ve paylaşılabilir olduğu sonucuna ulaşılmıştır. Biyometrik faktöre bağlı kimlik doğrulama şemaları güvenlik bakımından yüksek güvenliğe sahip olsa da yaygın kullanımı nedeniyle kullanıcılar için birtakım endişeler taşımaktadır. Bu tür sistemlerin yaygınlaşması kullanıcıların biyometrik faktöre bağlı kimlik doğrulama şemalarını benimseyebilmeleri için güvenirlik kazanılabilir ve sistemlere entegre edilerek denemelerde bulunulabilir. Bunun sonucunda çevrim içi sınavların, sınava girecek öğrenci tarafından gerçekleşmesiyle ölçme değerlendirme sonuçlarının güvenirliği artırılabilir.

Anahtar Kelimeler: Bilgi güvenliği, çevrim içi sınav, gizlilik, güvenlik, kimlik doğrulama, kullanılabilirlik.

ABSTRACT

Necmettin Erbakan University, Graduate School of Educational Sciences
Department of Computer Education and Instructional Technology
Computer Education and Instruction Technology Program
Master Thesis

ANALYZING OF THE OPINIONS OF INSTRUCTORS AND UNIVERSITY STUDENTS IN REGARDS TO AUTHENTICATION SCHEMES THAT CAN BE APPLIED IN ONLINE EXAMS

Canan BATTAL

In the world that is going digital, there are also great transformations in education processes. There are great innovations not only in learning processes but also in measurement and evaluation processes, especially in online environments. Authentication schemes based on various authentication factors are used to access these online exams. The aim of this study is to examine the opinions of lecturers and university students about authentication schemes that can be applied in online exams. The research was carried out in the 2022-2023 academic year. The study was carried out with lecturers working in 9 different departments at 9 different universities. However, the study consists of the participation of students studying in 8 different departments of 7 different universities. In this direction, data were collected by using a semi-structured interview technique with 10 instructors and 8 students. Before the study, a video animation on the subject was watched by the participants. The obtained data were analyzed by content analysis. The preference status of authentication schemes, which are evaluated according to information security elements, has been examined. As a result of the research, the commonly used authentication scheme for usability was determined as a password, according to the answers given by the instructors. Instructors preferred passwords, one-time passwords and physical devices for privacy, face scanning and fingerprint schemes for security, respectively. As a result of the research, the commonly used authentication scheme for usability was determined as a password, according to the answers given by university students. Preferences were a password, one-time password, and physical device for privacy, respectively. There has been face scanning and fingerprint for security. When the answers are evaluated in terms of information security elements (usability, privacy, security), the results are that commonly used authentication schemes such as passwords and one-time passwords are not sufficient to combat identity theft or provide security. It has been concluded that such authentication schemes can be easily forgotten, lost, guessed, stolen and shared. Although authentication schemes based on biometric factors have high security in terms of security, they have some concerns for users due to their widespread use. With the widespread use of such systems, reliability can be gained so that users can adopt biometric factor-based authentication schemes, and attempts can be made by integrating them into the systems. As a result, the reliability of the measurement and evaluation results can be increased by the fact that the online exams are carried out by the student who will take the exam.

Keywords: Information security, online exam, privacy, security, authentication, usability.

BÖLÜM 1

1. GİRİŞ

Bu bölümde problem durumu, araştırmanın amacı, araştırmanın önemi, sınırlılıklar ve tanımlar başlıkları yer almaktadır.

1.1. Problem Durumu

Uzaktan eğitim, öğrencilerin çevrim içi ortamda eş zamanlı (senkron) ve eş zamansız (asenkron) olmak üzere iki şekilde öğrenimini gerçekleştirmesine olanak sağlayan bir eğitim türüdür (Wang, 2008). Dersler, öğrenme materyalleri ve sınavlar ilgili branş öğretmenleri tarafından internet üzerinden sunulur. Sunulan dersler, öğrenme materyalleri ve sınavlar öğrenciler tarafından internet aracılığı ile erişilebilmektedir. Öğrencilere gerçek bir sınıf ortamında değil, bulunduğu herhangi bir ortamda da bu kaynaklara ulaşabilme ve çalışabilme imkânı sağlanmaktadır.

Uzaktan eğitim ve çevrim içi kurslar, eğitim alacak kişinin bulunduğu ortama bağlı olmadan eğitim almasına olanak sağlamaktadır. Buna bağlı olarak uzaktan eğitimin birçok üstünlüğü bulunmaktadır. Örneğin, örgün eğitime göre daha az bütçe gerektirir ve istenilen zamanda istenilen ortamdan erişim sağlanabilir (Kör, Çataloğlu, & Erbay, 2012). Uzaktan eğitimde eğitmen farklı yerlerde ikamet edebilir ve etkileşim çoğunlukla eş zamansızdır. Belirli bir bölgeyi kapsamamaktadır. Örneğin, öğrencinin bir üniversitede ders alması ya da sınava girmesi için, öğrencinin üniversitenin bulunduğu şehirde ya da ülkede olmasına gerek yoktur.

Uzaktan eğitim, bilgisayar ve iletişim teknolojisine dayalı cihazların kullanılmasıyla öğrenme sürecini kolaylaştırır ve geliştirir. Uzaktan eğitim, internet üzerinden eğitim (web tabanlı öğrenme), bilgisayar aracılığıyla sağlanan eğitim (bilgisayar tabanlı öğrenme), sanal sınıflar ve dijital platformlar gibi geniş bir uygulama ve süreci kapsamaktadır (Smeureanu & Isaila, 2008). İçerik, internet ortamında ses kaydı, video kaydı ve belgeler ile elektronik olarak sunulur. Aşağıda uzaktan eğitim sistemlerinin bazı özellikleri sunulmaktadır:

- Uzaktan eğitimde öğrenme süreci sanal bir sınıfta gerçekleşir.
- Eğitim materyali internet üzerinden öğrencilere sunulur.
- Metin, resim, diğer çevrim içi kaynaklar, bağlantılar, resimler, ses ve video sunumları içerir.

- Uzaktan eğitimde ölçme değerlendirme süreci çevrim içi ortamda e-sınavlar aracılığı ile sağlanır.

Uzaktan eğitimle oluşan sanal sınıf; öğrencilerin etkinliklerini planlayan, tartışma formu ya da sohbet panosu kullanarak dersin özelliklerini tartışan, yardımcı kaynaklar sağlayan bir eğitmen tarafından koordine edilmektedir. Böylece öğrenme sosyal bir süreç haline gelerek, eğitmen ve öğrenciler arasındaki etkileşim ve iş birliği yoluyla bir öğrenme topluluğu oluşturmaktadır. Çoğu uzaktan eğitim sistemi, katılımcıların etkinlik izlemesine ve alt gruplar üzerinde çalışmalara, ses ve video etkileşimlerini içermektedir (Luminita, 2011). Eğitim sistemlerinin geliştirilmesindeki yeni eğilimler ve uzaktan erişilebilen uygulamaların geliştirilmesi, uzaktan eğitim sistemlerinin güvenlik yönetimi ve erişim kontrolü için bazı gereksinimler ortaya çıkarmıştır.

Uzaktan eğitimin birçok alanda yaygın kullanılması bu sistemlere güvenli bir şekilde erişim sağlanmasını da gerektirmektedir. Bilgisayar biliminde, gizli verilere ya da sistemlere erişim sağlamak için kullanıcının genellikle kimliğini doğrulaması gerekmektedir. Kullanıcıların kimlikleri doğrulayabilmeleri için çeşitli kimlik doğrulama şemaları geliştirilmiştir. Bu kimlik doğrulama şemaları, bilgisayar ortamında ve akıllı telefonlar üzerindeki etkileşimlerde yaygın olarak kullanılmaktadır. Kimlik doğrulama, bilgisayar sistemindeki bir kullanıcının ya da cihazın kişiye ait sistemlere erişim sağlayabilmesi için gerçekleştirilen ön koşul işlemi olarak tanımlanabilir. Kullanıcı, erişim sağlamak istediği sisteme önceden kaydedilen bilgilerinin girişini yapar ve sistem kayıtlı bilgiler ile kullanıcı girişini eşleştirerek kullanıcının ya da ilgili cihazın istenilen ara yüze ulaşmasını sağlar. Bu işlem, sistem ve kullanıcı arasındaki bilgi güvenliğini sağlamak amacıyla yapılır.

Uzaktan eğitimde güvenlik, günümüzde çevrim içi ortamda eğitimlerin arttığı ve giderek daha fazla insanın eğitim aldığı gerçek eğitim bağlamında önemli bir konudur. Dikkate alınması gereken birçok önemli öge vardır: kimlik doğrulama, erişim kontrolü, veri bütünlüğü, içerik koruma, vb. Bilgi güvenliği, şifreleme ve ağ protokolleri gibi yöntemler kullanılarak kullanıcı güvenliği sağlanabilir.

1.2. Araştırmanın Amacı

Bu araştırmanın amacı, çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin öğretim elemanı ve üniversite öğrencilerinin görüşlerini belirlemek ve analiz etmektir. Bu amaç doğrultusunda aşağıdaki sorulara yanıt aranmıştır.

1. Çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin öğretim elemanı görüşleri nelerdir?
2. Çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin üniversite öğrencilerinin görüşleri nelerdir?

1.3. Araştırmanın Önemi

Yapılan alan yazın taraması sonucunda birçok kimlik doğrulama şemasının olduğu ve günümüzde halen yeni kimlik doğrulama şemalarının geliştirildiği görülmektedir. Öğretim elemanları ve üniversite öğrencileri açısından uygun bulunan ve uygun olmayan kimlik doğrulama şemaları tespit edilebilir. Belirlenen sınırlılıkların giderilmesi için veriler oluşturulur. Öğretim elemanlarına ve üniversite öğrencilerine öneriler sunulur. Yetkili kişilere ve yöneticilere öneriler sunulur. Bunun sonucunda araştırmacılar, bir sistemde kimlik doğrulama şemalarından hangi koşullarda en uygun olduğunu öğrenebileceklerdir. Elde edilen sonuçların sistemin güvenirliğini ve kullanılabilirliğini artıracağı düşünülmüştür.

1.4. Sayıltılar

- Öğretim elamanlarının yöneltilen soruları, objektif bir şekilde cevapladıkları varsayılmıştır.
- Çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarının incelendiği bu çalışmada, öğretim elemanlarının ve öğrencilerin bu sistemleri kullandığı ve yeterli bilgiye sahip olduğu varsayılmıştır.
- Öğretim elemanlarının ve öğrencilerin kimlik doğrulama şemalarının uygulanacağı sistemlere erişebilme ve kullanabilme durumlarının eşit olduğu varsayılmıştır.

1.5. Sınırlılıklar

- Örneklem açısından, Kocaeli Üniversitesi, Marmara Üniversitesi, Yıldız Teknik Üniversitesi, Ankara Hacı Bayram Veli Üniversitesi, Niğde Ömer Halisdemir Üniversitesi, Kocaeli Üniversitesi, Nişantaşı Üniversitesi, Karabük Üniversitesi, Ankara Sosyal Bilimler Üniversitesi, Kahramanmaraş Sütçü İmam Üniversitesi 2022-2023 Öğretim Yılı Güz Dönemi'nde uzaktan eğitim gerçekleştiren 10 öğretim elemanı ve İstanbul Üniversitesi, Selçuk Üniversitesi, Eskişehir Osmangazi Üniversitesi, Selçuk Üniversitesi, Isparta Süleyman Demirel Üniversitesi, Necmettin Erbakan Üniversitesi, Konya Gıda ve Tarım Üniversitesi, Karadeniz Teknik Üniversitesi 2022-2023 Öğretim Yılı Güz Dönemi'nde uzaktan eğitim gerçekleştiren 8 üniversite öğrencisi ile sınırlıdır.
- Araştırma verileri katılımcılar ile yapılan görüşmeler ile sınırlıdır.

- Günümüzde 20'den fazla kimlik doğrulama şemasının bulunması, bu kimlik doğrulama şemalarının bir laboratuvar çalışmasında değerlendirmelerinin zor olması nedeniyle sorun teşkil edecektir. Bu nedenle araştırmada kullanımı yaygın olan ve öğretim elemanı ve üniversite öğrencileri için uygun bulunan kimlik doğrulama şemaları seçilmiştir.
- Kullanılan kimlik doğrulama şemaları açısından, araştırma amaçlarına yönelik olarak seçilen beş kimlik doğrulama şeması (Parola, Tek Kullanımlık Şifre, Parmak İzi, Yüz Tarama, Fiziksel Aygıt) ile sınırlıdır.

1.6. Tanımlar

Öğretim elamanı; yükseköğretim kurumlarında görevli öğretim üyeleri, öğretim görevlileri ve araştırma görevlileridir (Yükseköğretim Kanunu, 2018).

Kimlik doğrulama şeması; kullanıcının kimlik bilgilerini içeren ve kimlik doğrulama sisteminden erişim izni almasını sağlayan yöntemlerdir.

BÖLÜM 2

2. ALAN YAZIN

2.1. Uzaktan Eğitim

Uzaktan eğitim, öğrenci ve öğretmenin fiziksel olarak farklı ortamlarda eş zamanlı ya da eş zamansız olarak gerçekleştirdiği bir öğretim yöntemidir. Uzaktan eğitim yazışma, ses, video, bilgisayar ve internet gibi teknolojilerin kombinasyonunu sağlayarak kullanılabilir (Roffe, 2004).

Uzaktan eğitim, farklı yerlerde bulunan öğrenci, öğretmen ve öğretim materyallerinin iletişim teknolojileri yardımıyla bir araya getirildiği kurumsal bir eğitim faaliyeti olarak tanımlanmaktadır (İskenderoğlu, İskenderoğlu, & Palancı, 2012). Uzaktan eğitim, eğitimsel sürecin desteklenmesi ve yapılandırılması için öğretmen ve öğrencilerin iki yönlü iletişiminin uzaktan sağlandığı ve iki yönlü iletimde teknolojinin kullanıldığı eğitimdir (Kaya, 2002). Uzaktan eğitimin bir diğer tanımı; kaynak ile alıcının öğrenme-öğretme süreçlerinin büyük bir bölümünde birbirlerinden ayrı (uzak) ortamlarda bulunmasıdır. Alıcılarına öğretim yaşı, amaçları, zamanı, yeri ve yöntemi gibi yönlerden "bireysellik, esneklik ve bağımsızlık" imkânı tanımaktadır. Öğrenme-öğretme süreçlerinde yazılı ve basılı materyaller, işitsel araçlar, teknolojiler, yüz yüze eğitim gibi materyal, araç ve teknoloji ve yöntemlerin kullanıldığı, kaynak ile alıcılar arasındaki iletişim ve etkileşimin ise tümleşik teknolojilerle sağlandığı planlı sistematik bir eğitim teknolojisi uygulamasıdır (Uşun, 2006).

Uzaktan eğitim kavram olarak 1927 yılında somutlaşmaya başlamıştır. Türkiye'de üniversitelerde aktif olarak ön lisans, lisans ve lisansüstü programlarda uzaktan eğitim sistemi kullanılmaktadır (Alkan, 1997).

Tüm sistemlerde olduğu gibi öğrenciler için olduğu kadar uzaktan eğitim veren kurumlar için de önemli olan, öğrencilerin eğitim sürecinde gerçekte ne ölçüde öğrendiklerini belirlemektir (Altan & Seferoğlu, 2009). Bunu belirlerken öğrencilerin ölçme değerlendirme sürecinde özellikle sınavlara erişim sağlarken kimlik doğrulama işlemini doğru bir şekilde gerçekleştirmelerine ihtiyaç duyulmaktadır. Ayrıca uzaktan eğitimle birlikte çevrim içi sınavların yaygınlaşması bu eğitim modeline erişim sağlarken farklı kimlik doğrulama seçenekleri ile bilgi güvenliğini artırma ihtiyacı ortaya çıkarmıştır. Uzaktan eğitim ölçme değerlendirme sürecinde farklı kimlik doğrulama şemaları hakkında öğretim elemanlarının bu kimlik doğrulama şemalarını gizlilik, güvenlik ve kullanılabilirlik bakımından

değerlendirmelerinin kimlik doğrulama şemalarına karşı algılarının ve görüşlerinin ortaya çıkmasını sağlayacaktır.

Günümüzde uzaktan eğitim ortamları giderek artmaktadır ve öğrenciler için alternatif öğrenme ortamları sağlanmaktadır. Çevrim içi ortamların yaygınlaşması ile çevrim içi sınavlar da artmaya başlamıştır.

2.2. Çevrim içi Sınavlar

Çevrim içi sınavlar, öğrencilerin performansının ölçülebilmesi ve değerlendirilmesi için uzaktan eğitimin en önemli parçasıdır. Yaygın olarak elektronik sınavlar (e-exams) olarak bilinen ve daha önce bilgisayar tabanlı değerlendirme yöntemi olarak bilinen çevrim içi sınavlar, "web ya da intranet aracılığıyla sınavların yapılmasını içeren bir sistem" olarak tanımlanabilir (Charles, Adebiyi, & Ekong, 2007). Çevrim içi sınavlar öğretmenin çoktan seçmeli, doğru-yanlış ve kısa cevaplı sorular dahil olmak üzere çeşitli soru türlerinden oluşan sınavlar tasarlamasına ve düzenlemesine olanak tanımaktadır. Bu nedenle çevrim içi sınav sistemleri, özellikle sınıfların kalabalık olduğu durumlarda, sınavın tasarlanması ve sunulmasından, notlandırılmasına, raporlanmasına, sonuçların saklanmasına ve istatistiksel analizlerin yapılmasına kadar geleneksel kâğıt üzerinde yapılan sınavlara nispeten daha fazla kolaylık sağlamaktadır. Çevrim içi sınavları yönetim süreci, uzaktan eğitimin en zorlayıcı yönlerinden biridir. Çevrim içi sınavlar, öğrencilerin ve eğitmenlerin fiziksel olarak aynı yerde bulunmadan gerçekleştiği sınavlar olduğundan bu sınavlara erişimin, sınav bütünlüğü ve güvenliği konusunda çeşitli sorunlar ortaya çıkmaktadır. Örneğin, çevrim içi ortamda, özellikle sürekli izlemenin olmadığı durumlarda, sınava giren bir kişinin kimliğinin doğrulanması son derece problem oluşturmaktadır.

Bu çevrim içi sistemlere erişim sağlamak, öğrenenin gizliliğini ve güvenliğini korumak, aynı zamanda ölçme değerlendirme aşamasında çeşitli hilelere başvurulmaması için kimlik doğrulama yöntemlerine ihtiyaç duyulmaktadır. Bu yöntemlerin kullanıcı bilgilerini içermesi nedeniyle hassasiyetle oluşturulması ve korunması gerekmektedir.

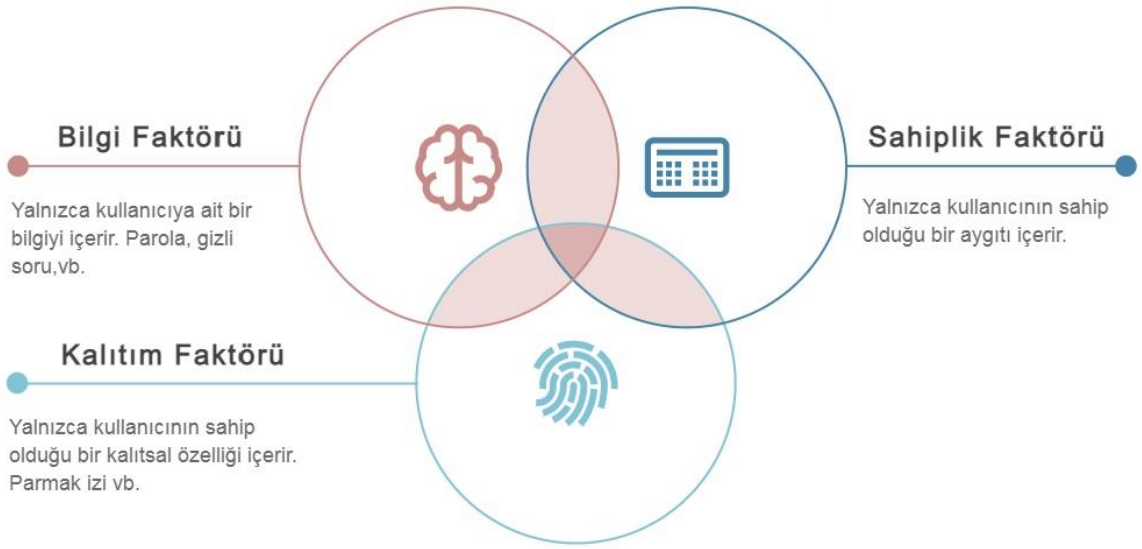
2.3. Kimlik Doğrulama (Authentication)

Kimlik doğrulama, bir kullanıcının ya da aygıtın var olan kimlik bilgileri ile sistemde kayıtlı olan bilgilerinin eşleşmesini ve sisteme erişimini sağlayan işlemdir. Kimlik doğrulama, kişisel ve değerli verileri üçüncü tarafların yetkisiz erişimine karşı korumanın önemli bir yoludur (Zimmermann & Gerber, 2020). Kimlik doğrulama kullanıcıların bilgilerine,

nesnelerine ve biyometrik özelliklerine dayanmaktadır. Araştırma esasına dayalı çevrim içi sınavların daha kullanılabilir ve güvenilir olması, mevcut elektronik sınav sisteminin de güvenli bir kimlik doğrulama hizmeti sunmasını gerektirmektedir.

2.4. Kimlik Doğrulama Faktörleri

Kullanıcıların gerçekliğini doğrulamak için çeşitli kimlik doğrulama faktörleri geliştirilmiştir (Bhagat, 2014). Beş farklı kimlik doğrulama faktörü bulunmaktadır (Kayrancıoğlu, 2019). Bilgi faktörü, sahiplik faktörü, kalıtım/biyometrik faktörü, konum faktörü ve zaman faktörü beş farklı kimlik doğrulama seçenekleri sunmaktadır. Bu yöntemlerin temel amacı, kullanıcının kimlik doğrulamasını daha güvenilir ve güvenli hale getirmektir. Eğitim kurumlarının birçoğu, çevrim içi sınav yapmak için bu yöntemleri kullanmaktadır. Bu çalışmada üç kimlik doğrulama faktörü ile araştırma gerçekleştirilecektir. Bunlar; bilgi faktörü, kalıtım faktörü ve sahiplik faktörüdür.



Şekil 2.1 Kimlik Doğrulama Faktörleri (Rolfe, 2019).

2.4.1 Bilgi Faktörü

Bilgi faktörleri, kullanıcının sisteme güvenli bir şekilde erişim sağlayarak, kullanıcının verilerini ya da kişisel bilgilerini koruması için geliştirilen kimlik doğrulama şemalarını içerir. Sistem kullanıcıdan kayıt sırasında sağladıkları kişisel ya da biyografik bilgileri (örneğin, ilk evcil hayvanın adı, doğum yeri, vb.) istemektedir (Schechter, Brush, & Egelman, 2009). Kullanıcı adı ya da e-posta adresi kendi başına bir kimlik doğrulama faktörü olarak kabul edilmemektedir. Kullanıcı adı ya da e-posta adresinin doğru kişi tarafından sağlandığını

doğrulamak için kimlik doğrulama şemaları kullanılır. Parola, kişisel kimlik numarası (PIN), gizli soru ve tek kullanımlık şifre bu kimlik doğrulama şemalarına örnek olarak verilebilir.

Parola (Password)

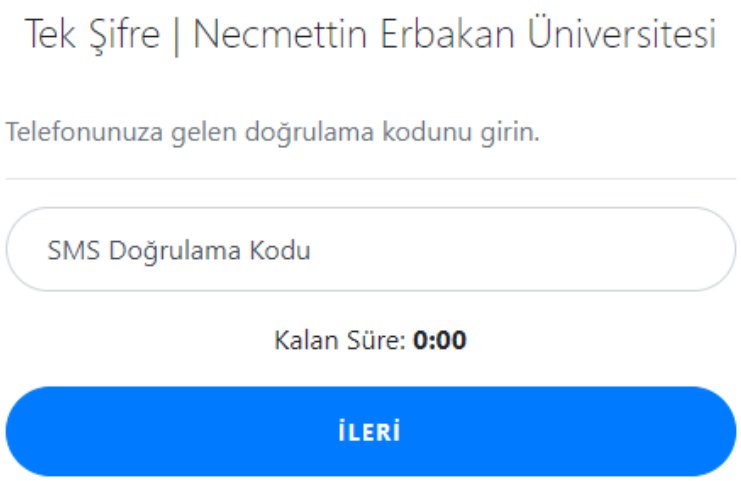
Parola, birçok sisteme erişim sağlamak için kullanılan en yaygın bilgi tabanlı kimlik doğrulama şemasıdır. Parola tabanlı kimlik doğrulamanın güvenliği, yetkili kullanıcının belirlediği şifreyi yalnızca kendisinin bilmesi ve hatırlamasına dayalıdır. Çeşitli sistemlerde parola tabanlı sistemlerin güvenliğini sağlama çabalarının birçoğu, daha iyi bir parola oluşturulması ile yetkisiz erişimi engellemeye odaklanır (Menkus, 1988). Ancak parola, teknik güvenlik sorunları ve her hesap için farklı parolaların ezberlenmesi konusunda yüksek bilişsel yük gibi çeşitli eksikliklere sahiptir (Stobert & Biddle, 2013). Ulusal Standartlar ve Teknoloji Enstitüsü'ne (NIST) göre oluşturulacak parolanın en az sekiz karakter olması gerekmektedir.

Şekil 2.2 Parola Kimlik Doğrulama Şeması (Necmettin Erbakan Üniversitesi, 2023).

Tek Kullanımlık Şifre (OTP – One Time Password)

Tek seferlik PIN, tek seferlik yetkilendirme kodu (OTAC) ve dinamik şifre olarak da bilinen tek seferlik şifre (OTP), bir bilgisayar sisteminde ya da dijital bir aygıtta oturum açmak için bir kez kullanılan iki faktörlü (bilgi faktörü, sahiplik faktörü) kimlik doğrulama şemasıdır. Tek kullanımlık şifreler, güvenli bir ortamdaki iki tarafın birbirinden ayrılabilmesi ve iki ayrı güvenli ortamdan mükemmel bir gizlilikle iletişim kurabilmesi gereken durumlarda pratiktir. Bunun yanı sıra Google'ın kimlik doğrulama sistemleri sorumlusu Mark Risher "Bulduğumuz gerçeklerden biri, insanların ihtiyaç duyduklarından daha fazla güvenliği kabul etmeyecekleri"

bu nedenle “Büyük ölçekli bir internet sağlayıcısı olarak, tüketici için bu doğru dengeyi bulmak istiyoruz” demiştir (Brandom, 2017).

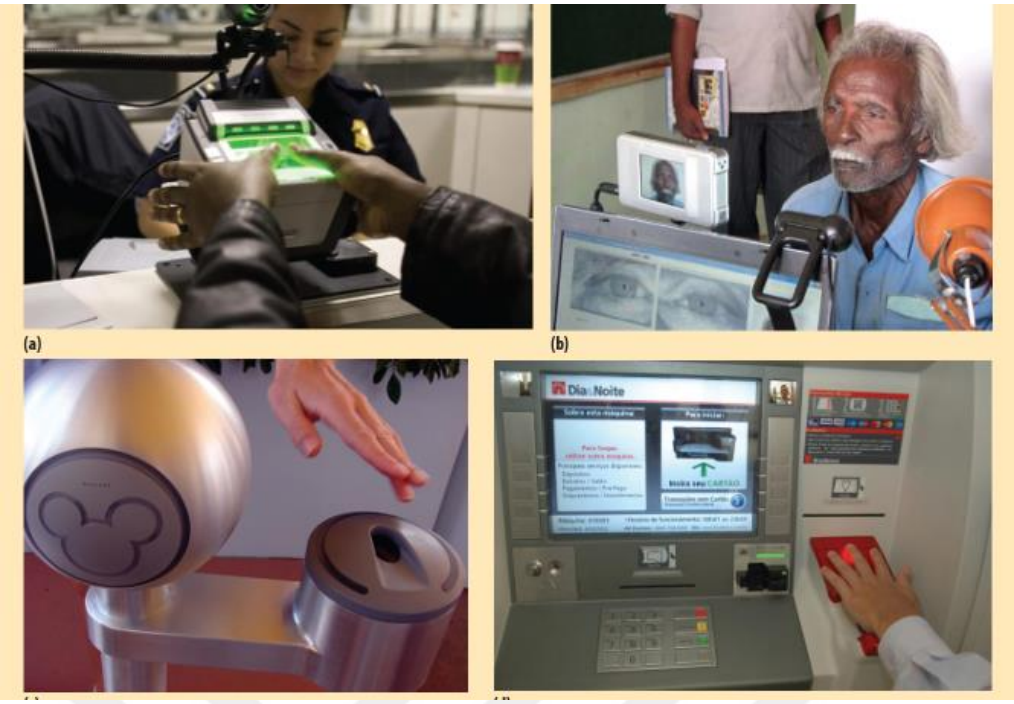


Şekil 2.3 Tek Kullanımlık Şifre Kimlik Doğrulama Şeması (Necmettin Erbakan Üniversitesi, 2023).

2.4.2 Kalıtım Faktörü (Biyometrik Faktör)

Biyometrik tabanlı kimlik doğrulama, diğer kimlik doğrulama yöntemlerine göre çeşitli avantajlar sunduğundan, son yıllarda kullanıcı kimlik doğrulaması için biyometrik tabanlı kimlik doğrulamanın kullanımında önemli bir artış olmaktadır (Nalini K. Ratha, 2001). Bu tür biyometrik tabanlı kimlik doğrulama sistemlerinin, uzaktan eğitim ve e-sınav gibi gözetimsiz uygulamalarda kullanıldığında güvenlik açısından saldırılara dayanacak şekilde tasarlanması önem arz etmektedir.

Kalıtım faktörü, kullanıcının benzersiz biyometrik imzasının olduğu kimlik doğrulama şemalarını içerir (Moody, 2004). Kalıtım faktörleri, kullanıcının biyometrik verilerine bağlı olarak sisteme erişim sağlarken kullandıkları kimlik doğrulama şemalarını kapsamaktadır. Bunlar; parmak izi, avuç içi tarama, yüz tanıma ve retina taraması vb.dir. Kalıtım faktörüne bağlı kimlik doğrulama şemaları, bireyleri anatomik özelliklerine (parmak izi, yüz, avuç izi, iris, ses) ya da davranış özelliklerine (imza, yürüyüş) göre tanır. Bu tür özellikler kullanıcıyla fiziksel olarak bağlantılı olduğundan, biyometrik tanıma yalnızca yetkili kullanıcıların bir sisteme girebilmesini sağlayan doğal ve daha güvenilir bir mekanizmadır.



Şekil 2.4 Kullanılan Biyometrik Kimlik Doğrulama Şemaları (Kimery, 2018).

Erişim sağlamak istenilen sistem, kullanıcıları biyometrik verilerine göre tanımlayabildiğinde, kalıtım faktörü, en güvenli kimlik doğrulama faktörlerinden biri olabilir. Bu faktörün sınırlılığı ise, erişim sağlamak için parmak izi taraması gerektiren bir sisteme ve mutlaka bu kimlik doğrulama faktörünü destekleyen bir donanıma sahip aygıta ihtiyaç olunmasıdır.

Parmak İzi (Fingerprint)

Bu biyometrik şema, kullanıcıların kimliklerini benzersiz parmak izleri ile doğrulamaktadır. Parmak izleri, yaygın olmaları ve kullanılabilirlikleri nedeniyle en yaygın kullanılan biyometrik şemadır (AL-Harby, Qahwaji, & Kamala, 2010). Biyometrik tabanlı sistem, insanların farklı fiziksel özelliklerini veri tabanlarında şablon şeklinde saklamaktadır.

Parmak izleri kesikler ve morlukların olması dışında değişmeyen ayırt edici bir özelliğe sahiptir. Kimlik doğrulama sürecinde ilk adım olarak, tipik mürekkepsiz bir tarayıcı kullanılarak kullanıcının parmak izinin bir örneği alınmaktadır. Optik sensör kullanan tarayıcı ile parmak izi alınır ve dijital görüntüsü sisteme kaydedilmektedir. Son olarak kullanıcı parmak izi ile sistemdeki parmak izinin benzerlik oranı belirlenmektedir ve bu puan olarak nitelendirilmektedir. Puan belirlenen oranın altındaysa, parmak izinin eşleşmediğini; puan belirlenen oranın üzerindeyse, doğru bir eşleşmenin gerçekleştiğini sistem bildirmektedir.

Şekil 2.5 Parmak İzi Kimlik Doğrulama Şeması (Erkılıç, 2022)

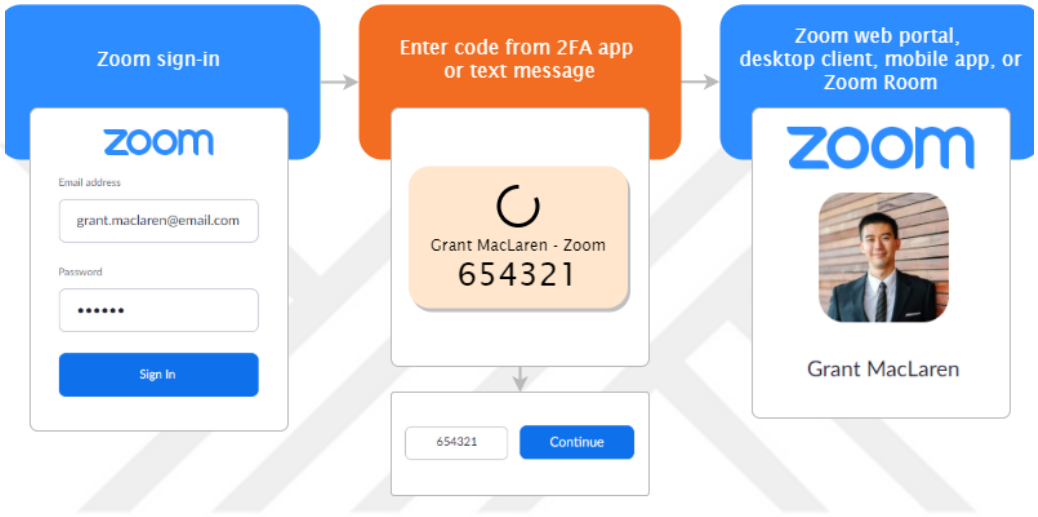
Yüz Tanıma (Face Recognition)

Yüz tanıma, popüler biyometrik kimlik doğrulama yöntemlerinden biridir. Giderek daha fazla bulunabilen ve uygun fiyatlı kameralar kullanılarak gerçekleştirilebilir. Örneğin, herhangi bir ekstra donanıma ihtiyaç duymadan bir kullanıcının kimliğini doğrulamak için bir akıllı telefon kamerası ya da bilgisayar kamerası potansiyel olarak kullanılabilir. Parmak izi kimlik doğrulama şemasının aksine, yüz tanıma fiziksel temas gerektirmemektedir (Mayron, Hausawi, & Bahr, 2013).

Şekil 2.6 Yüz Tanıma Kimlik Doğrulama Şeması (DHA, 2018)

2.4.3 Sahiplik Faktörü

Sahiplik faktörleri, sisteme erişim izni verilmeden önce kullanıcının belirli bir cihaza/aygıta sahip olmasını gerektirmektedir. Bu faktörde sistem tek tabanlı ve iki tabanlı olmak üzere iki farklı kimlik doğrulama şemasına sahiptir. İki tabanlı kimlik doğrulama şemasında örneğin; kullanıcı, bir kullanıcı adı ve şifre ile hesap oluşturarak giriş yaptıktan sonra, istenilen ara yüze ulaşması için tek seferlik bir şifre üretilir ve kullanıcının cep telefonu numarasına gönderilir. Kullanıcı gönderilen yeni oluşturulan tek seferlik şifreyi girer ve sisteme erişim sağlar.



Şekil 2.7 İki Tabanlı Kimlik Doğrulama Şeması (Zoom Video Communications, 2022)

2.5. Bilgi Güvenliği

Güvenlik uygulamaları, bilgilerin gizliliğini, güvenliğini ve kullanılabilirliğini koruyan teknik kontrollere odaklanmaktadır. Saltzer ve Schroeder, "Bilgisayar Sistemlerinde Bilginin Korunması" başlıklı makalelerinde, güvenliğin birincil endişesinin, yalnızca bilgisayar sisteminin kendisini korumaktan ziyade, bilgisayar sistemlerinde tutulan bilgilerin korunması olması gerektiği fikrini savunmuşlardır. Belgenin ilk bölümü, gizlilik, güvenlik ve kullanılabilirlik üçlüsünü içeren bilgilerin korunması için "temel ilkeleri" tanıtmıştır. Bu temel ilkeler, bilgisayar donanımını ve yazılımını korumayı içermektedir. Ancak zamanla gizlilik, güvenlik ve kullanılabilirlik bir bütün olarak ele alınmış ve bilgi güvenliği sürecine dahil edilmiştir.

Siber ortamda kullanıcılar için arayüz kullanılabilirliği, gizliliklerinin korunması ve erişim sağladıkları sistemin güvenliğinin sağlanması bilgi güvenliğinin çalışma prensibini

oluşturmaktadır. Birçok unsura sahip bu çalışma prensibinin üç tanesine araştırmada yer verilmiştir. Bunlar; kullanılabilirlik, gizlilik ve güvenliktir.

2.5.1 Kullanılabilirlik

Kullanılabilirlik, web sitesi ya da yazılım araçlarını kullanılabilir ve kaliteli kılan önemli özelliklerden biridir. Bir sistemin ya da yazılımın kalitesini belirleyen birçok özellik vardır. Kullanılabilirlik, oluşturulan bir sistemin değerlendirilmesinde en önemli faktördür. Günümüzde web sitesi, bilgi ya da hizmetlere yönelik iletişim ortamı olarak tüm dünyada yaygın olarak kullanılmaktadır. Bu bağlamda kullanılabilirlik ilkeleri sadece yazılım için değil, web ortamında da uygulanmaktadır. Kullanıcılar, erişim sağladıkları bir web sitesinde istediği hizmetleri hızlı, kolay ve etkili bir şekilde kullanabiliyorsa ve hedeflerini gerçekleştirebiliyorsa, bu web sitesinin kullanılabilirlik kalitesinin yüksek olduğunu göstermektedir.

ISO 9241 – 11'e dayalı olarak kullanılabilirlik, "bir ürünün belirli kullanıcılar tarafından belirli bir kullanım bağlamında etkililik, verimlilik ve memnuniyet ile belirli hedeflere ulaşmak için ne ölçüde kullanılabildiği" olarak tanımlanır (Fernandez, Insfran, & Abrahão, 2011). Tanıma bakıldığında, kullanılabilirliğin kriterleri etkililik, verimlilik ve memnuniyettir. Bu tanım, kullanılabilirliğin ne anlama geldiğini daha net ifade etmektedir ve birçok araştırmacı bu tanımı kullanmaktadır. Kullanılabilirlik bu üç kriterin alt şemaları olan işlevsellik, güvenilirlik, sürdürülebilirlik ve taşınabilirlik gibi 4 özelliğe sahiptir.

2.5.2 Gizlilik

Gizlilik ve güvenlik birbiri ile ilişkili ancak birbirinden farklı unsurlardır. Veri gizliliği, hassas bilgileri ya da kişisel bilgileri yetkisiz varlıklardan korumayı amaçlar (Das, 2015). Çalışmada yer alan öğrenci gizliliği, çevrim içi sınavlara erişim sağlamak amacıyla kullanılacak kimlik doğrulama şemalarının, öğrencinin paylaştığı ve sahip olduğu kişisel bilgilerinin sistem tarafından nasıl kullanılacağını belirten bir politikadır.

2.5.3 Güvenlik

Var olan sistemlerin bütünlüğünü sağlamak, verileri korumak ve üçüncü kişilerin erişimini önlemek amacıyla geliştirilen önemli bir parametredir.

Sistem güvenliği çevrim içi sınavlara erişim sağlamak amacıyla kullanılacak ve öğrenci kişisel verilerinin de bulunduğu kimlik doğrulama şemalarının, sistem tarafından korunmasını belirten bir unsurdur.

2.6. İlgili Araştırmalar

Huazhong Normal Üniversitesi'nde yapılan bir çalışmada öğrencilerin çevrim içi sınava katılmak için kişisel hesaplarını bir başkası ile paylaşması gibi durumlara karşı yüz tanıma sistemi geliştirilmiş, uygulanmış ve kullanılabilirliği araştırılmıştır. Araştırmanın sonunda, geliştirilen yüz tanıma yöntemi ile aynı hesaba birden fazla kişinin erişebilmesi engellenerek, uzaktan eğitimde ölçme değerlendirme sonuçlarının güvenilirliğini artırabileceği sonucuna ulaşılmıştır (Zhao & Ye, 2010).

Uzaktan eğitim sistemlerine yönelik yapılan bir çalışmada, uzaktan eğitim sistemindeki öğretim elemanlarının ölçme ve değerlendirme sürecine ilişkin görüşlerini anlamak ve örgün eğitim bağlamında gözlemleri ile karşılaştırmak amaçlanmıştır. Bu doğrultuda hem uzaktan eğitim hem de örgün eğitim çerçevesinde görev yapan 4 öğretim elemanı ile görüşmeler gerçekleştirilmiştir. Katılımcılar, uzaktan eğitimde ölçme ve değerlendirme sürecinde en çok sınav ve ödevlerin kullanıldığını, bu süreçte karşılaşılan en önemli sorunların ise gözlem yapamama, dolayısıyla öğrencilerin sınava girmesi gereken öğrenci olup olmadığını saptayamama gibi problemlerle karşılaştıklarını belirtmişlerdir. Bu çalışmanın sonuçları, uzaktan eğitim sisteminde en yaygın kullanılan ölçme-değerlendirme yöntemlerinin sınavlar ve ödevler olduğunu ortaya koymaktadır (İskenderoğlu, İskenderoğlu, & Palancı, 2012). Ancak değerlendirme sürecinde karşılaşılan bazı sorunlar vardır. Öğretim elemanlarına göre, uzaktan eğitimde yaşanan iletişim sorunları, öğrenci ve öğretmenlerin birbirlerini tanımada başarısız olmalarına ve ayrıca ölçme ve değerlendirme konusunda karşılıklı beklentilerin (ödev, proje vb.) farklı algılanmasına yol açmaktadır. Ayrıca katılımcı görüşlerine göre, öğrencilerin sınava girecekleri ortamlar online sınavlara elverişli olmalıdır. Uzaktan eğitim çerçevesinde ölçme ve değerlendirme yöntemlerinden en uygun olanının seçilmesi ve sürecin daha etkin hale getirilmesi öğrencilerin öğrenme oranlarının belirlenmesinde yardımcı olabilir (Karal, Çebi, & Pekşen, 2010).

National American Üniversitesi'nde (National American University) Acxiom Şirketi ile ortak yapılan bir çalışmada üniversitenin çevrim içi öğrenci kimliğini en iyi şekilde doğrulamak amacıyla bir araştırma yürütülmüştür. Üniversite bu iş birliği sayesinde, günümüzdeki çevrim içi ölçme değerlendirme sürecinin güvenilirliğini artırmayı amaçlamıştır. Araştırma sonucunda öğrencilerin kimliklerini doğrulamaya yönelik yapılan projeler başarıyla denenmiştir. Kullanıcı kimlik doğrulama projelerinde yer alan akademik kurumların, bu projelerin başarısına,

dünyanın her yerinde bulunan çevrim içi öğrencilerin kimlik doğrulamasına yönelik bir adım daha ekleyerek, giderek daha fazla katkıda bulunacağını ummaktadır (Bailie, 2009).

Yapılan bir diğer çalışmada uzaktan eğitim sürecinde kullanılan kimlik doğrulama şemalarına yönelik öğrenci görüşleri alınmıştır. Araştırma sonuçlarına göre öğrenciler çoğunlukla bilgi tabanlı kimlik doğrulama ve biyometrik tabanlı kimlik doğrulama yöntemlerini tercih etmişlerdir (Aras Bozkurt, 2018). Bununla birlikte öğrencilerin, uzaktan eğitim ve e-sınav platformlarına erişim sağlamak için kullanılan kimlik doğrulama yöntemlerine karşı güvenlik ile ilgili bazı endişelere sahip olduğu görülmüştür.

Biyometri tabanlı kimlik doğrulama sistemlerine yönelik yapılan bir çalışmada, güvenliği ve gizliliği artırmaya yönelik bir araştırma yapılmıştır (Nalini K. Ratha, 2001). Yapılan çalışmada, biyometri tabanlı kimlik doğrulama şemalarının zayıf yönleri ve hırsızlığa karşı direncine bağlı olarak çözümler geliştirilmiştir. Buffalo Üniversite'sinde yapılan araştırma sonucunda, biyometrik kimlik doğrulamada ihmal edilen mahremiyet sorunlarına ve bunun sonucunda biyometrinin yürürlükten kaldırılmasına değinilmiştir. Biyometrinin en büyük avantajının zaman içinde değişmemesinin yanı sıra en büyük dezavantajının da bu olması araştırmacılar tarafından ironik bulunmuştur. Yine de araştırmacılar, biyometri tabanlı kimlik doğrulamanın, parolalar gibi geleneksel sistemlere göre birçok kullanılabilirlik avantajına sahip olduğu ile ilgili değerlendirmelerde bulunmuşlardır. Ayrıca araştırmada kullanıcıların biyometrilerini kaybetmelerinin ve biyometrik sinyalin çalınması ya da taklit edilmesinin zor olduğu belirtilmiştir. Bir biyometrik sinyalin içsel bit gücünün, parolayla karşılaştırıldığında, özellikle parmak izleri için oldukça iyi olabileceğini göstermişlerdir. Araştırmacılar, genel bir biyometrik sistemdeki sekiz güvenlik açığı noktasını vurgulayarak olası saldırıları tartışmışlardır. Bu güvenlik tehditlerinden bazılarını hafifletmek için birkaç yol önermişlerdir. Bilgisayar korsanlarının saldırıları, parmak izi görüntüsüne doğrudan ulaşılmasını engellemek amacıyla ikincil bir kimlik doğrulama gerektirmektedir. Böylece sistem verilerine ulaşılması daha güç hale getirilmiştir. Akıllı bir sensörden alınan sinyalin canlılığını kontrol etmek için bir meydan okuma/yanıt yöntemi önerilmiştir. Yine de biyometrik sistem de dahil olmak üzere herhangi bir sistem, bilgisayar korsanları tarafından saldırıya uğradığında savunmasızdır sonucuna ulaşılmıştır (Nalini K. Ratha, 2001).

Sağlık hizmetleri alanında yapılan bir araştırmada ise, karşılaşılan hile yapma durumlarına yönelik biyometrik kimlik doğrulama şemalarının kullanımı ile meydana gelebilecek hileleri önlemek amaçlanmıştır. Sağlık hizmeti veren kişi ya da kurumlar, tedavi

uygulamadıkları halde bir kişi üzerinden tedavi masrafı faturası çıkararak sigorta şirketlerine masraf faturası göndermektedirler. Bu sayede sigorta şirketinden hiç uygulanmamış bir tedavi üzerinden kazanç sağlamaktadırlar (Tarhan Mengi, 2013). Bunun engellenebilmesi için kişinin kimlik bilgilerinin yanı sıra biyometrik verileri ile işlem yapılması bu tür hilelerin en az seviyeye indirilmesine yardımcı olacaktır sonucuna ulaşılmıştır.

Patras Üniversitesi ve Kıbrıs Üniversitesi'nin hazırladığı bir makale, yaygın olarak kullanılan kimlik doğrulama şemalarının güvenlik ve kullanılabilirlik yönlerini kapsayan, bilgiye dayalı kullanıcı kimlik doğrulamasındaki çalışmaların kapsamlı bir incelemesini sunmaktadır. Güvenlik açısından, mevcut tehditleri kullanıcı ve sistem bakımından analiz etmişlerdir. Kullanıcı deneyimi açısından her bir kimlik doğrulama şemasının kullanılabilirlik ve güvenliğini tartışarak analiz etmişlerdir. Yapılan analiz sonucunda, literatürde çok sayıda alternatif kullanıcı kimlik doğrulama şeması önerilmiş olmasına ve kullanıcıların çeşitli kimlik doğrulama şemalarıyla farklı şekilde etkileşime girmesine rağmen, çevrim içi hizmet sağlayıcıların henüz bilgi tabanlı kimlik doğrulama şemalarına karşılık diğer alternatifleri benimsemediği sonucuna ulaşılmıştır (Katsini, Belk, Fidas, Avouris, & Samaras, 2016).

Kalasalingam Üniversitesi'nde yapılan bir çalışmada, çevrim içi sınavlarda öğrenci kimlik doğrulamasına yönelik tehditleri ve mevcut kimlik doğrulama yaklaşımlarının faydaları ve sınırlılıkları araştırılmıştır. Yapılan araştırmaya göre çevrim içi sınavlarda öğrenciler, sınava kendileri için başka birinin girmesini sağlayarak puanlarını artırmaya çalışabilmektedirler. Çalışma sonucunda çevrim içi sınav sürecini güvence altına almak amacıyla öğrencilerin biyometrik ve bilgi tabanlı olmak üzere iki tabanlı kimlik doğrulama faktörü (çift doğrulama) kullanılması önerilmiştir (Thanganayagam & Arivoli, 2013).

Hertfordshire Üniversitesi'nde yapılan bir çalışmada, çevrim içi sınavlarda kimlik doğrulama zorlukları araştırılmış, mevcut kimlik doğrulamanın faydalarını ve kısıtlamalarını gözden geçirerek alternatif yöntemler bulunması amaçlanmıştır. Çevrim içi sınavlar sırasında öğrencilerin kimlik doğrulaması için kullanıcı kimliği ve parola ile birlikte profil tabanlı bir kimlik doğrulama sistemi (Profike Based Authentication Framework, PBAF) kullanılması önerilmiştir. Önerilen çözüm, e-öğrenme ortamına erişim sağlamak için ilk olarak öğrencinin kullanıcı kimliği ve parola ile giriş yapmasını, doğrulandığı takdirde profil tabanlı sorgulama sorularını cevaplayarak giriş yapmasını sağlamaktadır (Ullah, Xiao, & Lilley, 2012).

Çevrim içi öğrenmenin hızla yaygınlaşmasıyla birlikte öğrenciler, seçtikleri yer ve zamanda öğrenme içeriğine kolay ve esnek erişim talep etmektedir. Bu ortamlarda, halka açık İnternet ya da diğer güvenli olmayan ağlar aracılığıyla bağlanan uzak kullanıcıların, testler ya da kişisel/özel kayıtlar gibi hassas içeriklerine erişim verilmeden önce kimliklerinin doğrulanması gerekmektedir. Bugün, çevrim içi öğrenme sistemlerinin büyük çoğunluğu, yalnızca her oturumun başında uzak kullanıcıların kimliğini doğrulamak için yetersiz kimlik doğrulama mekanizmalarına güvenmektedir. Parola, kişisel kimlik numarası (PIN) ve hatta donanım belirteçleri kullanılarak yapılan tek seferlik kimlik doğrulama, uzaktan kullanıcı kimliğine bürünme ya da bu kimlik doğrulama şemalarının yasa dışı paylaşımı ve ifşası dahil olmak üzere içeriden saldırılara karşı savunma sağlayamamaktadır. Moini ve Madni'nin (2009) çalışması, çevrim içi öğrenme ortamlarında uzaktan kimlik doğrulama sorununu incelemekte ve kullanıcının her zaman bilgisayarın önünde bulunduğunu onaylayarak kullanıcı kimliğine bürünme saldırılarına karşı savunma yapmak için biyometrik teknolojiyi kullanmanın zorluklarını ve seçeneklerini araştırmaktadır. Çözüm önerisi olarak kullanıcının kimlik doğrulama gereksinimlerini karşılamasını sağlamaya yönelik 5 adımlı bir sistem yaklaşımından yararlanılmıştır. Araştırma, e-sınav ve e-öğrenme ortamlarında kullanıcının kimliğini doğrulaması için biyometri tabanlı bir istemci-sunucu mimarisi önerisinde bulunarak sonuçlanmıştır (Moini & Madni, 2009).

Manipal Üniversitesi'nde yapılan bir çalışma, çevrim içi sınavlarda öğrenci kimlik doğrulamasına yönelik potansiyel tehditleri araştırmayı ve mevcut kimlik doğrulama yaklaşımlarının faydalarını ve sınırlamalarını analiz etmeyi amaçlamıştır. Çevrim içi sınavlar, gerçek kullanıcı kimlik doğrulaması sağlamanın çok zor olabilmesi nedeniyle benzersiz bir sorun teşkil etmektedir. Çevrim içi olmanın doğasında var olan anonimlik nedeniyle, öğrenciler sınıf ortamında sınava girmeye kıyasla, sınava kendileri için başka bir kişinin girmesini sağlayarak puanlarını yükseltmeye çalışabilmektedirler (Flior & Kowalski, 2010). Bu nedenle çalışmada, çevrim içi sınavlarda güvenli biyometrik öğrenci kimlik doğrulaması çerçevesini önermişlerdir. Bu çerçeve, çevrim içi incelemeyi güvence altına almak için çok modlu bir kimlik doğrulama yaklaşımı kullanmaktadır. Çözüm olarak, iki kimlik doğrulama (çift doğrulama) katmanından oluşan bir kimlik doğrulama sistemidir. Bu sistem biyometrik kimlik doğrulama ve bilgi tabanlı kimlik doğrulamayı içermektedir. Araştırmacılar bu sistemin öğrencilerin iki farklı kimlik doğrulama kullanarak sınava erişim sağlaması nedeniyle hileye başvurma eylemlerini zorlaştıracakları sonucuna ulaşmıştır (Ramu & Arivoli, 2013).

Son yıllarda e-öğrenme alanındaki gelişmelere rağmen, kopya çekmeyi önlemek için uygun önlemler bulunmamaktadır. Mevcut Eğitim Yönetim Sistemleri (EYS-Learning Management System), öğrencinin çevrim içi sınava kendi başına girip girmediğini kontrol etmek, hatta tüm oturumu bilgisayar başında geçirip geçirmediğini bilmek için gerekli özellikleri sağlamamaktadır. İspanya Vigo Üniversitesi'nde yapılan bu çalışma, yüz tanımaya dayalı biyometrik kimlik doğrulama içeren web tabanlı bir uygulama sunmaktadır. Mevcut EYS'lere kolayca entegre edilebilen bu uygulama, erişim kontrolü, izleme ve değerlendirme sırasında yüz tanıma özelliğini kullanabilmektedir. Böylece, öğrenme sürecindeki kritik aşamalarda (örneğin, ölçme değerlendirme) güvenliği artırmak mümkün olacaktır sonucuna ulaşılmıştır (Agulla, Rifón, Castro, & Mateo, 2008).

E-sınav katılımcı kimliğinin doğrulanması, sınav sürecinin adil bir şekilde yürütülmesi için birincil öneme sahiptir. Southampton Üniversitesi'nde yapılan çalışmada yetkisiz kişilerin sınavlara girmesine izin verilmemesi için yeni bir yaklaşım önerilmiştir. Herhangi bir biyometrik tanıma sistemindeki ilk süreç, e-sınava girmesi gereken tüm öğrencilerin ilgili e-öğrenme sunucusu tarafından veri tabanında biyometrik verinin saklanması için parmak izlerini kaydetmesi gereken "kayıt" işlemi olacaktır. Yapılacak herhangi bir değişikliği önlemek için tüm parmak izi taramaları şifreli bir biçimde sisteme kaydedilecektir. Sunucu e-sınavı başlattığında, akıllı ajan öğrenci kimliğine bir IP adresi atadığında, öğrenci başka bir PC'den oturum açamayacaktır (Alotaibi, 2010).

E-öğrenme sistemleri yeni bir öğrenme biçimini temsil ederken her geçen gün daha yaygın hale gelmektedir. Dolayısıyla, e-öğrenmede güvenlik temel bir gereklilik haline gelmiştir. Ancak e-öğrenme sistemleriyle ilgili sorun, güvenlik için çok az bütçe yatırımının olmasıdır. Ayrıca, e-sınavlar söz konusu olduğunda, bir öğrenicinin kimliğinin doğrulanması, e-öğrenme ortamında büyük ölçüde zorluk oluşturmaktadır. Yapılan çalışma kötü niyetli kullanıcılar tarafından yetkisiz erişimin önlenmesi için kimlik doğrulama tekniklerinin daha önemli hale geldiğinden bahsetmektedir. Kullanıcı kimlik doğrulama yöntemleri üç kategoriye ayrılmaktadır: (1) parolalar gibi insan belleğine dayalı yöntemler, (2) manyetik veya IC kartları gibi fiziksel cihazlara dayalı yöntemler ve (3) parmak izi, iris gibi biyometriye dayalı yöntemler. Araştırmacılar ilk iki kategoriyi unutkanlık ya da kayıpların neden olduğu zafiyetlerden kaçamamasından bahsederken, üçüncü kategori için son dönemde çok ilgi gördüğünden bahsetmişlerdir. Onlara göre biyometrik kimlik doğrulamanın önemli bir sorunu, insan özelliklerinin çıkarılması ve biyometrik verilerin karşılaştırılması sürecinde hatasız

olmamasıdır. Çoklu biyometri, tek bir biyometrik kimlik doğrulama teknolojisinin gerekli güvenilirlik düzeyini karşılayamadığı durumlarda, biyometrik kimlik doğrulamanın güvenilirliğini artırmak için kullanılabilir sonucuna ulaşılmıştır. Bu çalışma kullanıcı kimlik doğrulamasının gerekli olduğu e-öğrenmedeki çeşitli hizmetleri desteklemek için çoklu biyometriye sahip bir kimlik doğrulama sistemi önermektedir (Chellappan & Asha, 2008).

Nova Southeastern Üniversite'sinde e-öğrenme ortamları, birçok üniversitede olduğu gibi e-öğrenme derslerinin verilmesi için sisteme dahil edilmiştir. Bununla birlikte, e-öğrenmeye karşı olanlar, bu tür bir öğretim ortamının temel dezavantajının, bu tür ortamlarda giderek artan etik dışı davranış olduğunu iddia etmektedir. Özellikle e-öğrenme karşıtları, sınava girenlerin kimliğinin doğrulanamamasının e-öğrenme ortamlarının en büyük eksikliği olduğunu savunmaktadır (Levy & Ramim, 2007). Sonuç olarak, bazı kurumlar öğrencilerden gözetmen merkezlerinde sınava girmelerini istemek ve hatta kurumlarında e-öğrenme dersleri vermeyi tamamen bırakmak dahil olmak üzere aşırı önlemler almayı teklif etmektedir. Bu makale, e-öğrenme sınavlarına girerken etik olmayan davranışları engellemek için e-öğrenme ortamlarıyla birlikte mevcut parmak izi biyometrik kimlik doğrulama teknolojilerini içeren teorik bir yaklaşım önererek bu önemli sorunu ele almaya çalışmaktadır. Önerilen yaklaşım, e-öğrenme kurslarında sınava girerken rastgele bir parmak izi biyometrik kullanıcı kimlik doğrulamasını içerebilen pratik bir çözüm önermektedir. Bunu yapmanın, e-öğrenme ortamlarında kopya çekmeyi engelleyeceği varsayılmaktadır.

BÖLÜM 3

3. YÖNTEM

Bu bölümde araştırma modeli, çalışma grubu, veri toplama araçları, artırılmış gerçeklik materyalleri, uygulama ve veri analizi hakkında bilgi verilmiştir.

3.1. Araştırmanın Modeli

Bu çalışma, öğretim elemanı ve üniversite öğrencilerinin çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin görüşlerini belirlemek amacıyla yapılmıştır. Uzaktan eğitimin ölçme değerlendirme sürecinde kimlik doğrulama şemaları hakkındaki görüşlerini, güvenlik ve kullanılabilirlik algısını ortaya çıkaran bir araştırmadır. Nitel araştırma yöntemlerinden yarı yapılandırılmış görüşme formu kullanılarak katılımcıların kimlik doğrulama şemaları hakkındaki görüşleri alınmıştır.

3.2. Araştırmanın Evreni ve Örneklemi

Çalışma grubunu, Kocaeli Üniversitesi, Marmara Üniversitesi, Yıldız Teknik Üniversitesi, Ankara Hacı Bayram Veli Üniversitesi, Niğde Ömer Halisdemir Üniversitesi, Nişantaşı Üniversitesi, Karabük Üniversitesi, Ankara Sosyal Bilimler Üniversitesi, Kahramanmaraş Sütçü İmam Üniversitesi 2022-2023 Öğretim Yılı Güz Dönemi'nde uzaktan eğitim gerçekleştiren 10 öğretim elemanı ve İstanbul Üniversitesi, Selçuk Üniversitesi, Eskişehir Osmangazi Üniversitesi, Isparta Süleyman Demirel Üniversitesi, Necmettin Erbakan Üniversitesi, Konya Gıda ve Tarım Üniversitesi, Karadeniz Teknik Üniversitesi 2022-2023 Öğretim Yılı Güz Dönemi'nde uzaktan eğitim gerçekleştiren 8 üniversite öğrencisi oluşturmaktadır. Araştırmaya katılan öğretim elemanlarının demografik özelliklerine ilişkin bilgiler aşağıda tablolar halinde gösterilmiştir.

Tablo 3.2.1. Öğretim Elemanlarının Cinsiyet Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Cinsiyet	Kadın	4	40
	Erkek	6	60
	Toplam	**10**	**100,0**

Öğretim elemanlarının %40'ı kadın, %60'ı erkektir.

Tablo 3.2.2. Öğretim Elemanlarının Akademik Unvan Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Akademik Unvan	Prof. Dr.	3	30
	Doç. Dr.	1	10
	Yrd. Doç. Dr.	1	10
	Dr. Öğr. Üyesi	3	30
	Arş. Gör.	2	20
	Toplam	**10**	**100,0**

Öğretim elemanlarının %30'ı Doktor Öğretim Üyesi, %30'u Profesör Doktor, %10'u Doçent, %10'u Yardımcı Doçent ve kalan %20'si ise Araştırma Görevlisi akademik unvanına sahiptir.

Tablo 3.2.3. Öğretim Elemanlarının Bölüm Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Bölüm	Bilgisayar ve Öğretim Teknolojileri Eğitimi	2	20
	Gastronomi ve Mutfak Sanatları	1	10
	İngiliz Dili ve Edebiyatı	1	10
	İslam Tarihi ve Sanatları	1	10
	Mimarlık	1	10
	Tıbbi Biyoloji	1	10
	Tıbbi Mikrobiyoloji	2	20
	Türk Dili ve Edebiyatı	1	10
	Toplam	**10**	**100,0**

Öğretim elemanlarının %20'si Bilgisayar ve Öğretim Teknolojileri Eğitimi ve Tıbbi Mikrobiyoloji bölümü, %10'u Gastronomi ve Mutfak Sanatları, İngiliz Dili ve Edebiyatı, İslam Tarihi ve Sanatları, Mimarlık, Tıbbi Biyoloji ve Türk Dili ve Edebiyatı bölümüne mensuptur.

Tablo 3.2.4. Üniversite Öğrencilerinin Cinsiyet Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Cinsiyet	Kadın	4	50
	Erkek	4	50
	Toplam	**10**	**100,0**

Üniversite öğrencilerinin %50'si kadın, %50'si erkektir.

Tablo 3.2.5. Üniversite Öğrencilerinin Sınıf Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Sınıf Düzeyi	1. Sınıf	3	37
	2. Sınıf	1	13
	3. Sınıf	2	25
	4. Sınıf	2	25
	Toplam	**10**	**100,0**

Üniversite öğrencilerinin %37'si 1. Sınıf, %13'ü 2. Sınıf, %25'i 3. Sınıf ve %25'i 4. Sınıf öğrencisidir.

Tablo 3.2.6. Üniversite Öğrencilerinin Bölüm Dağılımı

Tanımlayıcı Özellik	Grup	*N*	%
Bölüm	Çocuk Gelişimi	1	10
	Arapça Mütercim Tercümanlık	1	10
	Ziraat Mühendisliği	1	10
	Bitki Islahı ve Genetiği	1	10
	Sağlık Yönetimi	1	10
	Beslenme ve Diyetetik	1	10
	Bilgisayar Mühendisliği	1	10
	Tıp Fakültesi	1	10
	Toplam	**10**	**100,0**

Üniversite öğrencilerinin %10'u Çocuk Gelişimi, %10'u Arapça Mütercim Tercümanlık, %10'u Ziraat Mühendisliği, %10'u Bitki Islahı ve Genetiği, %10'u Sağlık Yönetimi Beslenme ve Diyetetik, %10'u Bilgisayar Mühendisliği, %10'u Tıp Fakültesi bölümünde öğrenim görmektedir.

3.3. Veri Toplama Araç ve/veya Teknikleri

Araştırmacı tarafından geliştirilen, katılımcıların kimlik doğrulama şemaları hakkında bilgilendirileceği bir video-animasyon tasarlanmıştır. Animasyonun yeterli olup olmadığı BÖTE (Bilgisayar ve Öğretim Teknolojileri Eğitimi) bölümünde görev alan 3 uzman öğretim elemanına gösterilerek gerekli düzenlemeler yapılmıştır. Yapılan animasyon araştırmaya dahil edilerek, çalışmaya katılan öğretim elemanlarına ve üniversite öğrencilerine izletilmiştir. Ardından yarı yapılandırılmış bir görüşme formu uygulanmıştır. Görüşme formunda, katılımcıların çevrim içi ölçme değerlendirme sürecinde belirlenen kimlik doğrulama

şemalarının (Parola, Tek Kullanımlık Şifre, Parmak İzi, Yüz Tarama, Fiziksel Aygıt) kullanımı ile ilgili görüşleri alınmıştır. Görüşme formunun ilk bölümünde katılımcılardan demografik bilgileri istenmiştir. Demografik bilgiler:

- Cinsiyet
- Sınıf
- Unvan
- Bölüm

İkinci bölümde ise katılımcılardan çevrim içi sınavlara erişim sağlarken kullanmak istedikleri kimlik doğrulama şemalarını belirlemeleri, bu şemaları tercih etme nedenlerini açıklamaları ve bilgi güveliği unsurlarına göre değerlendirmeleri istenmiştir.

3.3.1 Öğretim Elemanlarına Uygulanacak Görüşme Formu Soruları

S1. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından öğrenci gizliliğini sağlayabilecek en uygun şema hangisidir? Neden?

S2. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından sistem güvenliği için en uygun şema hangisidir? Neden?

S3. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından kullanılabilirliği (kullanımı) en yüksek olan şema hangisidir? Neden?

S4. Ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, en uygun bulduğunuz, beğendiğiniz kimlik doğrulama şemasını belirtiniz ve 10 puan üzerinden puanlayınız. (1 puan en düşük, 10 puan en yüksek değer anlamına gelmektedir.)

S5. Ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, uygun olmadığını düşündüğünüz, beğenmediğiniz kimlik doğrulama şemasını belirtiniz.

S6. Size göre, öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını en çok kolaylaştırabilecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S7. Size göre, öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurma eylemini en az seviyeye indirecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S8. Şu an sahip olduğunuz akıllı telefonunuzun kilit ekranında, hangi kimlik doğrulama şemasını kullanıyorsunuz? Nedenini açıklayınız.

S9. Bu çalışmada yer almayan ancak kullanmak istediğiniz başka bir kimlik doğrulama şeması var mı? Varsa belirtiniz ve tercih etme nedeninizi kısaca açıklayınız.

3.3.2 Üniversite Öğrencilerine Uygulanacak Görüşme Formu

S1. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından öğrenci gizliliğini sağlayabilecek en uygun şema hangisidir? Neden?

S2. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından sistem güvenliği için en uygun şema hangisidir? Neden?

S3. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından kullanılabilirliği (kullanımı) en yüksek olan şema hangisidir? Neden?

S4. Çevrim içi sınavlarda kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, en uygun bulduğunuz, beğendiğiniz kimlik doğrulama şemasını belirtiniz ve 10 puan üzerinden puanlayınız. (1 puan en düşük, 10 puan en yüksek değer anlamına gelmektedir.)

S5. Çevrim içi sınavlarda kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, uygun olmadığını düşündüğünüz, beğenmediğiniz kimlik doğrulama şemasını belirtiniz.

S6. Size göre, çevrim içi sınavlara erişim sürecinde hileye başvurulmasını kolaylaştıracak kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S7. Size göre, çevrim içi sınavlara erişim sürecinde hileye başvurma eylemini en az seviyeye indirecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S8. Şu an sahip olduğunuz akıllı telefonunuzun kilit ekranında, hangi kimlik doğrulama şemasını kullanıyorsunuz? Nedenini açıklayınız.

S9. Bu çalışmada yer almayan ancak kullanmak istediğiniz başka bir kimlik doğrulama şeması var mı? Varsa belirtiniz ve tercih etme nedeninizi kısaca açıklayınız.

3.4. Verilerin Toplanması

Katılımcıların bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik ögelerine göre kimlik doğrulama şemalarını değerlendirdikleri bu çalışmada, veri toplanması için araştırmacı tarafından hazırlanan bir görüşme formu uygulanmıştır. İlk olarak, tüm katılımcılara çalışmadaki araştırma süreci hakkında bir açıklama sağlanmış, konu ile ilgili olarak araştırmacı tarafından hazırlanan bilgilendirme video-animasyonu izletilerek konu hakkında bilgilendirilmiş olduklarına dair onayları alınmıştır. Çalışmadan sonra çalışmanın amaçlarına ilişkin daha ayrıntılı bir açıklama yapılmıştır. Katılım isteğe bağlı gerçekleştirilmiştir. Katılımcıların verileri yalnızca araştırma amaçlı analiz edilmiştir ve anonimleştirilmiştir. Katılımcıların uygulama için verdikleri kişisel bilgileri ve görüşme sorularına verdikleri cevaplar, katılımcıların gizliliğini korumak amacıyla yalnızca araştırmacıya teslim edilmiştir. Çalışma esnasında katılımcıların soru sormalarına izin verilmiştir ve çalışmadan sonra istenilen sorular için iletişim bilgileri verilmiştir.

3.5. Verilerin Analizi

Analiz edilen tüm kimlik doğrulama şemalarının objektif derecelendirmeleri bir tabloda verilmiştir. Şemalar gizlilik, güvenlik ve kullanılabilirlik bakımından değerlendirilerek karşılaştırılmıştır (Butler, 2020). Araştırma sonunda elde edilen sonuçlar içerik ve frekans çözümleme yöntemleri kullanılarak analiz edilmiştir.

BÖLÜM 4

4. BULGULAR

4.1. Öğretim Elemanlarına Ait Bulgular ve Yorumlar

Araştırmacı tarafından hazırlanan yarı yapılandırılmış "kimlik doğrulama görüşme formu"na yönelik öğretim elemanlarının verdiği yanıtların çözümlenmesi sonucunda elde edilen bulgular, araştırma sorularının sırasına uygun olarak açıklamalarıyla birlikte verilmiştir.

4.1.1 "Öğretim Elemanlarının Ölçme Değerlendirme Sürecinde Öğrenci Gizliliği Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Araştırmada yer alan 5 adet kimlik doğrulama şemasının öğrenci gizliliği göz önüne alındığında öğretim elemanlarının görüşleri şöyledir:

Tablo 1. Öğrenci Gizliliği Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	6	60	**Parola**	3	30
			Tek Kullanımlık Şifre	3	30
Kalıtım Faktörü	2	20	**Parmak İzi**	-	-
			Yüz Tarama	2	20
Sahiplik Faktörü	2	20	**Fiziksel Aygıt**	2	20

Fiziksel aygıt, aynı şekilde tek kullanımlık şifre masumane duruyor. Kullanılan internet sayfasının güvenilir olmasına bağlı olarak da parola da öğrenci gizliliği bakımından kullanılabilir. Dolayısıyla burada parmak izi ve yüz tanıma dışındaki diğer üç seçenek (parola, tek kullanımlık şifre ve fiziksel aygıt) öğrenci gizliliği açısından kullanılabilir durumda. (K1)

Tek kullanımlık şifre bu noktada daha cazip görünüyor. En azından gizlilik noktasında sınav için üretiliyor ve öğrenciye gönderiliyor. Herhangi bir bilgi de içermiyor. (K2)

Öğrencilerin kişisel verilerinin gizliliğini koruma noktasında parola ve tek kullanımlık şifre daha uygun olur. (K3)

Öğrenci gizliliği için yüz tarama çok uygun. Üniversite sistemi olduğu için güvenilir bir alan o yüzden önemli bir data olsa da bu bilgiyi paylaştığı yer üniversite sistemi olduğu için gizlilik noktasında sorun yaşanmayacaktır diye düşünüyorum. (K4)

Ben burada yüz tarama diyeceğim. Kullanım noktasında yaygınlaştığını da düşünüyorum. Öğrenci gizliliğinin korunması noktasında herhangi bir ihlale sebebiyet verecek bir üniversite sistemi olduğunu düşünmüyorum. (K5)

> Burada parola tercih edilebilir. Bana göre yapılan sınavın güvenliği daha önemli. Aslında buradaki tüm kimlik doğrulama şemaları kullanılarak giriş yapılabilir. (K6)
>
> Tek kullanımlık şifrede şifreyi bir algoritmayla üretip sana gönderecek, bu gayet makul bir seçenek. Fiziksel aygıtı da tercih edebilirim, parola ve ardından telefona gelecek bir şifreyle giriş yapmak kişi gizliliği için gayet makul. Yüz tarama ve parmak izi bu noktada çok fazla kişisel bilgi içeriyor. Kullanmak istemezdim açıkçası. (K7)
>
> En yaygın olarak parola kullanıldığı için ben parolayı tercih ederim. (K8)
>
> Sanki fiziksel aygıt daha iyi gibi geliyor. Bir bilgi paylaşmadan iki kez doğrulama çok uygun bana göre. (K9)
>
> Bana en makulü ikili doğrulama sistemi geliyor. Kullanıcı nerde olursa olsun o kişinin kendine ait telefonunun ya da ikinci bir cihaz ne kullanıyorsa onun yanında olması gerekiyor. O yüzden bana fiziksel aygıt gizlilik noktasında daha mantıklı geliyor. (K10)

Araştırmaya katılan öğretim elemanlarının araştırmacı tarafından hazırlanan yarı yapılandırılmış görüşme formunda yer alan sorulara ilişkin verdikleri yanıtlar içerik analizi yapılarak görüşleri aktarılmış ve Tablo 1'de gösterilmiştir. Verilen yanıtlar incelendiğinde öğretim elemanlarının ölçme değerlendirme sürecinde öğrenci gizliliğini göz önünde bulundurarak çevrim içi sınavlara erişim sağlamak için kullanmayı en çok tercih ettiği kimlik doğrulama şemaları %30 oranla bilgi faktörüne bağlı parola ve tek kullanımlık şifre şemaları olmuştur. Bunları takiben %20 oranla yüz tarama ve fiziksel aygıt şemaları tercih edilmiştir.

Öğretim elemanlarının verdiği yanıtlara göre parola, tek kullanımlık şifre ve fiziksel aygıt öğrencilerin herhangi bir biyometrik bilgisini içermemesi nedeniyle öğrenci gizliliğini korumaktadır. Biyometrik faktöre bağlı parmak izi kimlik doğrulama şeması ise öğrenci gizliliği göz önüne alındığında katılım sağlayan 10 öğretim elemanı tarafından da tercih edilmemiştir. Bunun sebebi olarak parmak izi şemasının eşsiz ve kişiye özel olduğunu belirtmişlerdir. Buna bağlı olarak katılımcılar öğrencinin biyometrik faktöre bağlı parmak izi gibi önemli bir bilgisinin öğrenci gizliliğini sağlayamayacağına dair değerlendirmelerde bulunmuşlardır.

4.1.2 "Öğretim Elemanlarının Ölçme Değerlendirme Sürecinde Sistem Güvenliği Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının sistem güvenliğini düşünerek tercih ettikleri kimlik doğrulama şemaları için yapmış olduğu değerlendirmeler şöyledir:

Tablo 2. Sistem Güvenliği Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	1	10	**Parola**	1	10
			Tek Kullanımlık Şifre	-	-
Kalıtım Faktörü	7	70	**Parmak İzi**	2	20
			Yüz Tarama	5	50
Sahiplik Faktörü	2	20	**Fiziksel Aygıt**	2	20

Fiziksel aygıt bu anlamda herhangi bir şey depolamayı gerektirmiyor, çalınacak bir bilgi içermiyor bu nedenle fiziksel aygıtı tercih edebilirim. Aynı sebeplerden dolayı tek kullanımlık şifre de tercih edebilirim. (K1)

Güvenlik bakımından parmak izi ve yüz tarama diğerlerine göre daha güvenli olacaktır. Diğerlerinde güvenlik ihlali olma olasılığı daha yüksek olacaktır. (K2)

Sistem güvenliği parmak izi ve yüz tarama ile yüksek koruma sağlayabilir. Fiziksel aygıtı da üçüncü olarak söyleyebilirim. (K3)

Yüz tarama diyebilirim. Parmak izi dediğimde bunda da şöyle bir sıkıntı olabiliyor. Parmağınızda yara olduğunda ya da elin derisinde bir hasar olduğunda sistem sizi tanımada zorlanabiliyor. (K4)

Öğrenci gizliliği bakımından da sistem güvenliği bakımından da yüz tarama diyorum. Kişinin bizzat kendisinin olması ve doğrulanması noktasında yüz tarama çok uygun. Başkası tarafından fotoğrafla vs. başka şekilde erişim mümkün değil. (K5)

Yüz taramanın güvenlik açısından daha yüksek olduğunu düşünüyorum. Taklit edilmesi mümkün değil. (K6)

Sadece sistem güvenliği olarak baktığımda en sağlıklı olan yüz tarama olarak düşünüyorum, bu sistemin birileri tarafından tahrip edilmesi daha zor olur. Aynı şekilde iki doğrulama yapmak da bana çok güven veriyor. Bu yüzden fiziksel aygıt da diyebilirim. (K7)

Güvenliği düşündüğümde de parola yeterli bence. Diğer sistemler için parmak izi ve yüz tarama için harici cihazlara gereksinim olacaktır bu durum maliyeti de etkiler. (K8)

İki doğrulama gerektirdiği için bana göre fiziksel aygıt güvenlik için çok uygun gibi geliyor. (K9)

Bence yüz tarama olur. Çünkü ehliyet sınavlarında da yüz tarama sistemi kullanılıyor. Direkt kişinin kimliğini bu şekilde doğrulayabiliyorlar. (K10)

Araştırmaya katılan öğretim elemanlarının verdiği yanıtlar içerik analizi yapılarak görüşleri aktarılmış ve Tablo 2'de gösterilmiştir. Sistem güvenliğini göz önünde bulundurarak öğretim elemanlarının vermiş olduğu yanıtlar, ölçme değerlendirme sürecinde çevrim içi sınavlara

erişim sağlamak için kullanmayı en çok tercih ettiği kimlik doğrulama şeması %50 oranla kalıtım/biyometrik faktöre bağlı yüz tarama şeması olmuştur. Bunu takiben %20 oranla parmak izi ve fiziksel aygıt şemaları tercih edilmiştir. Tablo 2'de de görüldüğü gibi katılımcıların %70'i biyometrik tabanlı kimlik doğrulama şemaları olan yüz tarama ve parmak izini tercih etmiştir. Son olarak %10 oranla katılımcılardan yalnızca biri (K8) parolayı tercih etmiştir. Bunun nedeni olarak K8, parmak izi ve yüz tarama gibi sistemlerin harici bir cihaza gereksinim duyulması ve bu sistemlerin kurulması için maliyet gerektiği değerlendirmelerinde bulunmuştur. Tek kullanımlık şifre şeması ise sistem güvenliği göz önüne alındığında katılım sağlayan 10 öğretim elemanı tarafından da tercih edilmemiştir. Sonuç olarak Tablo 2'ye bakılarak sistem güvenliği düşünüldüğünde biyometrik faktöre bağlı kimlik doğrulama şemaları tercih edilen en uygun şemalar olarak belirlenmiştir.

4.1.3 "Öğretim Elemanlarının Ölçme Değerlendirme Sürecinde Kullanılabilirlik Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının kimlik doğrulama şemalarını kullanılabilirlik bakımından değerlendirerek yapmış olduğu yorumlar şöyledir:

Tablo 3. Kullanılabilirlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	7	70	**Parola**	4	40
			Tek Kullanımlık Şifre	3	30
Kalıtım Faktörü	2	20	**Parmak İzi**	-	-
			Yüz Tarama	2	20
Sahiplik Faktörü	1	10	**Fiziksel Aygıt**	1	10

Kullanım rahatlığı anlamında parolayı tercih ederdim. Fiziksel aygıtı internet bağlantımın olmadığı bir yerde kullanamıyorum. Bazen telefonun çektiği bir yere gitmem gerekiyor. Keşke şifre yazsaydım bununla giriş yapmış olmasaydım diyorum. (K1)

Sitem tarafından üretilen bir şifrenin öğrenciye gönderilmesi daha makul gibi görünüyor. Tek kullanımlık şifre bunun için uygun. Parmak izi belki evet kullanımı kolay gözükse de benim telefonumda parmak izi okuyucu var ama herkesin telefonunda olamayabilir bu kısım önemli. (K2)

Herkes kullandığı için kolay olduğu için parola kullanılabilirliği oldukça iyi. (K3)

Kullanılabilirlik açısından değerlendirdiğimde fiziksel aygıt kullanılabilir. Pandemi sürecinde Zoom tabanlı bir uzaktan öğrenme sistemi oluşturuldu. Parolayla giriş yaparak telefonlarına doğrulama kodu gönderildi. Öğrenciler bu şekilde erişim sağladı. (K4)

> Günümüzde baktığımız zaman herkesin bir telefonu olduğunu düşünürsek tek kullanımlık şifre herkes için kullanılabilir olur. (K5)
>
> Bana göre tek kullanımlık şifre kullanım bakımından daha kolaylık sağlar. (K6)
>
> Parola derdim rahat bir şekilde erişim sağlayabiliyorsun her sistemde. Çünkü diğerlerinde sanki problem çıkabilirmiş gibi düşünüyorum. Özellikle yüz tarama sisteminde. Ben kendi telefonumu bile bazen parmak iziyle açamıyorum. İkinci bir seçenek olarak da tek kullanımlık şifre kullanımı oldukça kolay. (K7)
>
> Kullanım açısından yüz tarama olabilir. Yaşlı bireyler bile kolay bir şekilde bunu kullanabilir. Engelli bireyler için düşündüğümde eli olmayan biri için parmak izi sistemini kullanamayabilir. (K8)
>
> Normalde parola diyebilirim ama ben telefonumda ilk defa yüz tarama kullanmaya başladım ve gerçekten çok kolay bir kullanımı var ben çok beğeniyorum. (K9)
>
> Aslında parmak izi dışındaki diğer dört kimlik doğrulama şeması da olabilir. En yüksek olarak bir tane söylemem gerekirse parola diyebilirim. Her yerden her an erişim sağlamayı düşündüğümde parmak izi ya da yüz tarama çok uygun görünmüyor. Harici bir cihaza ya da uygulamaya ihtiyaç duyulabilir. Fiziksel aygıtta da iki farklı cihaza sahip olmak gerekiyor dolayısıyla kullanımı parolaya göre geride kalıyor. (K10)

Tablo 3'te öğretim elemanlarının verdiği yanıtlar gösterilmiştir. Kullanılabilirlik bakımından değerlendirilerek öğretim elemanlarının vermiş olduğu yanıtlar, ölçme değerlendirme sürecinde çevrim içi sınavlara erişim sağlamak için kullanmayı en çok tercih ettiği kimlik doğrulama şeması %40 oranla bilgi faktörüne bağlı parola şeması olmuştur. Bunu takiben %30 oranla yine bilgi faktörüne bağlı olan tek kullanımlık şifre şeması tercih edilmiştir. Toplamda %70 oranla bilgi faktörü kullanılabilirlik bakımından en uygun görülen kimlik doğrulama şemalarını içermektedir. Yapılan değerlendirmelere göre parola ve tek kullanımlık şifre yaygın olması ve kolay kullanıma sahip olması nedeniyle katılımcılar tarafından tercih edilmiştir. Biyometrik faktöre bağlı yüz tarama şeması ise %20 oranında tercih edilmiştir. Katılımcılardan iki öğretim elemanı (K8 ve K9) yüz tarama şemasının kullanılabilirlik düzeyinin yüksek olduğunu, genç ve yaşlı bireyler tarafından da rahatlıkla kullanılabileceği yönünde değerlendirmelerde bulunmuştur. Son olarak %10 oranla katılımcılardan yalnızca biri (K4) fiziksel aygıt şemasını tercih etmiştir. Bunun nedeni olarak K4, pandemi sürecinde Zoom uygulaması üzerinden yapılan derslerde öğrencilerin çift doğrulama yaparak erişim sağladıklarını belirtmiştir. Öğretim üyeleri yaptıkları değerlendirmelerde kullanılabilirlik bakımından parmak izi şemasını uygun olarak görseler de kullanılabilirliğin alt şemalarından olan erişilebilirliğin bu şemalar için olumsuzluk içerdiği yönünde yanıtlar vermişlerdir.

4.1.4 "Öğretim Elemanlarının Ölçme Değerlendirme Sürecinde Bilgi Güvenliği Unsurları Olan Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir? 1 ile 10 Arasında Puanlama Yapınız." Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının ölçme değerlendirme sürecini bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirerek yaptıkları yorumlar ve puanlamaları şöyledir:

Tablo 4. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	3	30	**Parola**	2	20
			Tek Kullanımlık Şifre	1	10
Kalıtım Faktörü	4	40	**Parmak İzi**	1	10
			Yüz Tarama	3	30
Sahiplik Faktörü	3	30	**Fiziksel Aygıt**	3	30

İnternet hızım iyi; bunları düşündüğüm zaman ve sitenin de güvenilir olduğunu düşündüğüm zaman en hızlı giriş yapabileceğim seçenekleri öncelikle söyleyeceğim. Parmak izi, yüz tarama bunlar ilk etapta hızlı bir şekilde girilebilecek durumda ve zahmetsiz. Mesela bazen o kadar çok parola hafızamızda tutmamız gerekiyor ki aslında burada parolayı da tercih edebiliriz ama unutulma ihtimalini de düşünerek burada en kolaylık sağlayacak yüz tarama. Parmak izi 9, yüz tarama 9, fiziksel aygıt 8, parola 5, tek kullanımlık şifre 5 puan. (K1)

Herkesin yani öğrencilerin bir mail adresi var ve herkese mail gönderilebilir. Tek kullanımlık şifre bu noktada yaygın kullanılmasından dolayı da böyle düşünüyor olabilirim problemsiz bir şekilde kullanılabilirlik gizlilik ve güvenlik için yeterlidir diye düşünebiliriz. (K2)

Fiziksel aygıt üçü bakımından değerlendirdiğimde ilk sırada olabilir. Parmak izi, yüz tarama biraz daha kullanım açısından zor; parola ve tek kullanımlık şifre de güvenlik bakımından zayıf kalacaktır. Fiziksel aygıt 8, parmak izi 6, yüz tarama 5, tek kullanımlık şifre 4 parola 3. (K3)

Fiziksel aygıt, parola diyeceğim ama aslında yüz tanıma daha uygun fakat bunu sisteme entegre etmek çok zor, o sistemin özel cihazları var dolayısıyla o sistemi oluşturmak zor. Fiziksel aygıt 10, parmak izi 9, yüz tarama 8, tek kullanımlık şifre 7, parola 6 puan. (K4)

Yüz tarama herkes için uygun olacaktır. Öğrencilerin hepsinin akıllı cihazı var dolayısıyla kamerası da var. Bu yüzden üçü için de uygun gözüküyor. Yüz tarama 10, parmak izi 7, fiziksel aygıt 6, tek kullanımlık şifre 4, parola 3. (K5)

> Herkesin kamerasının olduğunu da düşünürsek yüz tarama da bir merkeze bağlanarak kolaylaştırılabilir. Yüz tarama 8, fiziksel aygıt 8, parmak izi 7, tek kullanımlık şifre 6, parola 5. (K6)
>
> Sanırım fiziksel aygıt. Kullanılabilirliği paroladan ve tek kullanımlık şifreden bir tık daha zor ikinci bir cihaza ihtiyaç var, en azından iki aşamalı bir doğrulama gerektiriyor bu noktada gizlilik ve güvenlik bakımından daha iyi diyebilirim. (K7)
>
> En uygun parola 9, yüz tarama 7, parmak izi 6, tek kullanımlık şifre 4, fiziksel aygıt 3. (K8)
>
> Sanırım herkesin rahatlıkla kullanacağı güvenli de kabul edeceğim parola yeterli gibi geliyor. Eğer yüz tarama sistemde iyi bir şekilde çalışırsa o da olabilir. Parola 9, yüz tarama 8, fiziksel aygıt 7, tek kullanımlık şifre 6, parmak izi 5. (K9)
>
> Bana en yakın yüz tarama geliyor. Kullanılabilirliği çok zor değil, güvenirlik bakımından zaten kişinin o kişi olması gerekiyor. Üç unsur için değerlendirdiğimde ben yüz tarama kullanmanın daha uygun olduğunu düşünüyorum. Yüz tarama 9, fiziksel aygıt 8, tek kullanımlık şifre 6, parola 5, parmak izi 4. (K10)

Tablo 4'te öğretim elemanlarının verdiği yanıtlar sayısal olarak belirtilmiştir. Katılımcıların bilgi güvenliği unsurlarından kullanılabilirlik, gizlilik ve güvenlik bakımından kimlik doğrulama şemalarını değerlendirilerek sıralama yapmaları ve puanlamaları istenmiştir. Yapılan sıralamalara göre ölçme değerlendirme sürecinde çevrim içi sınavlara erişim sağlamak için kullanılabilirlik, gizlilik ve güvenlik bakımından kullanmayı en çok tercih ettiği kimlik doğrulama şemaları %30 oranla yüz tarama ve fiziksel aygıt şeması olmuştur. %20 oranla bilgi faktörüne bağlı olan parola şeması tercih edilmiştir. %10 oranla ise tek kullanımlık şifre ve parmak izi tercihinde bulunmuşlardır. Toplamda %40 oranla kalıtım faktörü kullanılabilirlik, gizlilik ve güvenlik bakımından en uygun görülen kimlik doğrulama şemalarını içermektedir. Yapılan değerlendirmelere göre öğretim üyeleri yüz tarama şemasını tercih etme nedeni olarak, öğrencilerin tamamının bir akıllı cihazı olduğunu ve bu cihazların her birinin kamerasının da bulunduğunu belirtmişlerdir. K9 yüz tarama şemasının sistemde doğru bir şekilde çalışamayacağı endişesi taşımaktadır bu nedenle parolayı tercih etmiştir. %30 orana sahip fiziksel aygıt içinse öğretim üyeleri, parola ve tek kullanımlık şifreye göre gizlilik ve güvenliği daha yüksek; yüz tarama ve parmak izine göre kullanılabilirliği daha yüksek olduğu bu nedenle tercih ettiklerini ifade etmişlerdir.

Tablo 5. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Madde	**Katılımcılar**											
Kimlik Doğrulama Şemaları	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***K7***	***K8***	***K9***	***K10***	$\bar{X}$	**%**
Parola	5	5	3	6	3	5	6	9	9	5	5,6	17
Tek Kullanımlık Şifre	5	8	4	7	4	6	7	4	6	6	5,7	17
Parmak İzi	9	6	6	9	7	7	9	6	5	4	6,8	20
Yüz Tarama	9	7	5	8	10	8	8	7	8	9	7,9	24
Fiziksel Aygıt	8	4	8	10	6	8	10	3	7	8	7,2	22

Katılımcılar kimlik doğrulama şemalarını 1 ila 10 puan arasında değerlendirmiştir.

Katılımcıların kimlik doğrulama şemaları için 1 ila 10 (1 en düşük, 10 en yüksek) arasında verdiği puanlar ve her bir kimlik doğrulama şeması için verilen puanların ortalaması Tablo 5'te gösterilmiştir. Kullanılabilirlik, gizlilik ve güvenlik bakımından yüz tarama şeması ($\bar{X}$=7,9) puan ortalaması ile en çok tercih edilen, ölçme değerlendirme süreci için en uygun bulunan kimlik doğrulama şeması olmuştur. Fiziksel aygıt şeması ($\bar{X}$=7,2) puan ortalaması ile yüz taramadan sonra en çok tercih edilen ve uygun görülen şema olmuştur. Sıralamada üçüncü olarak parmak izi şeması ($\bar{X}$=6,8) puan ortalamasına sahiptir.

Tablo 6. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	***Genel %***	$\bar{X}$	**%**	**Kimlik Doğrulama Şemaları**
Bilgi Faktörü	34	5,6	17	**Parola**
		5,7	17	**Tek Kullanımlık Şifre**
Kalıtım Faktörü	44	6,8	20	**Parmak İzi**
		7,9	24	**Yüz Tarama**
Sahiplik Faktörü	22	7,2	22	**Fiziksel Aygıt**

Katılımcılar kimlik doğrulama şemalarını 1 – 10 puan arasında değerlendirmiştir.

Tablo 6'da kimlik doğrulama faktörlerinin genel yüzdelik değerleri gösterilmiştir. Buna göre bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirildiğinde %44 oranla kalıtım faktörü en çok tercih edilen kimlik doğrulama şemalarını içermektedir. Tercihen ikinci olarak %34 oranla bilgi faktörü ve üçüncü olarak %22 oranla sahiplik faktörü olmuştur.

4.1.5 "Öğretim Elemanlarının Ölçme Değerlendirme Sürecinde Bilgi Güvenliği Unsurları Olan Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Uygun Olmayan, Beğenmedikleri Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının ölçme değerlendirme sürecini bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirerek uygun bulmadıkları kimlik doğrulama şemalarına yönelik yaptıkları yorumlar şöyledir:

Tablo 7. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Madde	**Katılımcılar**											
Kimlik Doğrulama Şemaları	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***K7***	***K8***	***K9***	***K10***	$\bar{X}$	**%**
Parola	5	5	3	6	3	5	6	9	9	5	5,6	17
Tek Kullanımlık Şifre	5	8	4	7	4	6	7	4	6	6	5,7	17
Parmak İzi	9	6	6	9	7	7	9	6	5	4	6,8	20
Yüz Tarama	9	7	5	8	10	8	8	7	8	9	7,9	24
Fiziksel Aygıt	8	4	8	10	6	8	10	3	7	8	7,2	22

Katılımcılar kimlik doğrulama şemalarını 1 – 10 puan arasında değerlendirmiştir.

> Çok kullanmadığım için ve telefonuma tek kullanımlık bir şifre geldiğinde, onu alıp klavyeden yazmak zor olacağı için en son tercih edeceğim o olur. (K1)

> Burada aslında belli noktalarda öğrenci gizliliğinden mi ödün verilmeli yoksa öğrencilerden teknik yapılarını geliştirmeleri mi istenmeli düşünüyorum. Parola ve tek kullanımlık şifre güvenlik için zayıf, yüz tarama ve parmak izi güvenlik için yüksek bir düzeyde ama kullanılabilirlik için oldukça zayıf. İki cihaza sahip olunması herkes için mümkün olmayabilir bu yüzden fiziksel aygıt diyeceğim. (K2)

> Parmak izi, yüz tarama biraz daha kullanım açısından zor. Güvenlik ve gizlilik biraz daha geri planda kalıyor bu iki kimlik doğrulamada, kullanılabilirlik daha önemli olduğu için bunu değerlendirerek parmak izi ve yüz tarama diyebilirim. (K3)

> Parola kullanılabilir olsa da gizlilik ve güvenlik açısından yetersiz. Zaman zaman unutma da söz konusu. (K6)

> Parmak izi ve yüz tarama bence çok fazla data içeriyor ve sisteme bunu veriyorsunuz. Ben bunu tasvip etmiyorum. Ama çok net bir şekilde kullanıcının da o kullanıcı olup olmadığını gösteriyor. Şöyle bir şey olabilir yüz tarama sisteminin algoritması bozulabilir, mesela yüzüne bir şey olabilir öğrencinin bu gibi sorunlar yaşanabilir diye düşünüyorum. Açıkçası öğrencilerin parmak izi ve yüz tarama sistemi kullandığında birçok bahane üreterek sınava giremedim savunmasını duyacakmışım gibi geliyor. (K7)

> Fiziksel aygıt benim için uygun değil. İki aşamalı olduğu için tercih etmeyeceğimi düşünüyorum. Her zaman yanınızda ikinci bir cihaz olması gerekiyor. (K8)

> Parmak izi bana şöyle geliyor, çok fazla kriminal bir şeymiş gibi geliyor. Bunu kullanmak beni ürkütüyor. Fiziksel aygıt için de herkesin o anda yanında ikinci bir cihazı olmayabilir. Yüz tarama için mesela gözlüğümü unutmuş olabilirim o zaman algılamayabilir. (K9)

> Ben en son seçenek olarak parmak izini kullanırdım. Yüz taramayı ilk seçerken parmak izini son olarak tercih etme nedenim, parmak izi için ekstra bir cihaz gerektiğini düşünüyorum. Ama yüz taramada herkesin kullandığı cihazlarda kamera olduğu günlük kullandığımız telefon kameralarımızla bile artık çeşitli uygulamalar indirerek maliyeti sıfıra düşürecek şekilde yüz tarama programlarından faydalanılabilir. (K10)

Tablo 7 incelendiğinde parola şeması ($\overline{X}$=5,6) ve tek kullanımlık şifre şeması ($\overline{X}$=5,7) puan ortalamasıyla en az tercih edilen, ölçme değerlendirme süreci için uygun bulunmayan kimlik doğrulama şeması olmuştur. Katılımcılardan bazıları parolanın gizlilik ve güvenlik için yetersiz olduğunu ve zaman zaman unutma ya da kaybetme gibi durumlar nedeniyle kullanılabilirlik bakımından da yeterli bulunmadığını ifade etmişlerdir. Ayrıca öğretim üyelerinden bazıları kalıtım faktörüne bağlı kimlik doğrulama şemalarının (parmak izi, yüz tarama) sisteme entegre edilmesinin zorluklarını ve bu sistemin doğru bir şekilde çalışması konusunda endişeleri olduğunu belirtmişlerdir. Ayrıca parmak izi gibi bir kimlik doğrulama şemasının kullanıcıya ait önemli ve büyük bir biyometrik bilgi içermesi nedeniyle sisteme böyle bir veri tanımlamanın uygun olmadığını belirtmişlerdir. Öğretim üyeleri tarafından kalıtım faktörüne bağlı kimlik doğrulama şemalarının (parmak izi ve yüz tarama) gerekli organı kaybetme, yaralanma gibi durumlarda sisteme erişimin zor olması ya da erişim sağlanamaması gibi sorunlara yola açacağı değerlendirmelerinde bulunmuşlardır. Araştırmaya katılan üç öğretim elemanı (K2, K8, K9) ise iki aşamalı bir kimlik doğrulama şeması sunması ve herkesin her an yanında ikinci bir aygıt taşımasının mümkün olmadığını belirterek fiziksel aygıt şemasını uygun bulmadıklarını belirtmişlerdir.

4.1.6 "Öğrencilerin Çevrim İçi Sınavlara Erişim Sürecinde Hileye Başvurmalarını En Çok Kolaylaştırabilecek Kimlik Doğrulama Şeması Hangisidir?" Sorusuna Yönelik Elde Edilen Yorumlar

Yapılan çevrim içi sınavlara erişim sağlarken, öğrencilerin kimlik doğrulama seçenekleri arasından hileye başvurmalarını kolaylaştırabilecek kimlik doğrulama şemalarına yönelik yapılan yorumlar şöyledir:

Tablo 8. Hileye Başvurmayı Kolaylaştıracak Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	10	100	**Parola**	7	70
			Tek Kullanımlık Şifre	3	30
Kalıtım Faktörü	-	-	**Parmak İzi**	-	-
			Yüz Tarama	-	-
Sahiplik Faktörü	-	-	**Fiziksel Aygıt**	-	-

En kolaylaştıracak parola olur. Kolay bir şekilde paylaşılabilir. (K1)

Mail adresine ya da telefona gelen tek kullanımlık bir şifre kolay bir şekilde paylaşılabilir. Ben parolayı paylaşma konusunda öğrencinin çok rahat olmayacağını düşünüyorum. Bu anlamda tek kullanımlık şifre paylaşmak daha kolay olabilir. (K2)

Parola ve tek kullanımlık şifre bu hileye başvurma durumuna ortam sağlayabilir. (K3)

Hileye başvurmalarını kolaylaştıracak olan parola olur. Tek kullanımlık şifreyi de paylaşabilir. (K4)

Parolasını belki herkesle paylaşmak istemeyebilir diye düşündüğümde tek kullanımlık şifre hileye başvurmada kolaylık sağlar diyebilirim. Aslında öğrencinin kendisi dışında sınava sokacağı kişi eğer yanındaysa bu beş kimlik doğrulama da onun için aynı ölçüde olacaktır. (K5)

Parola kolaylaştırır. Herkesle paylaşılabilir olması nedeniyle parola. (K6)

Kesinlikle parolayla bunu yapabilir. (K7)

Tek kullanımlık şifre diyorum. Çünkü öğrenci onu istediği bir kişiye mesaj olarak atabilir. Tek kullanımlık şifreyi bir şekilde kolay bir şekilde ulaştırır. (K8)

Öğrencinin her zaman kullandığı parola ve tek kullanımlık şifre çok kolay bir şekilde paylaşılabilir bir başkası sınava giriş yapabilir. (K9)

Sınav için daha yetkin olduğunu düşündüğü birine parolasını verebilir. Uzak ya da yakınlık bir şey ifade etmiyor parolada. (K10)

Tablo 8'de öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını kolaylaştıracak kimlik doğrulama şemalarının değerleri verilmiştir. Öğretim elemanlarının tamamı %100 oranla bilgi faktörünün hileye başvurma eylemini kolaylaştıracağını belirtmişlerdir. Katılımcıların 7'si parolanın uzakta ya da yakında olan herhangi bir kişiyle kolay bir şekilde paylaşılabileceğini bu nedenle öğrencilerin hileye başvurma eylemini de kolaylaştıracağını ifade etmişlerdir. 3 katılımcı parolanın paylaşımında, kendileri dışında bir başkasına gönderilmesi hususunda öğrencilerin çekimser davranabileceğini ancak tek

kullanımlık şifrenin daha paylaşılabilir, daha kolay bir şekilde gönderilebilir olduğunu belirtmişlerdir. Öğretim üyeleri Tablo 8'de görüldüğü gibi parmak izi, yüz tarama ve fiziksel aygıt şemalarını hileye başvurma eylemini kolaylaştıracak kimlik doğrulama şemalarından biri olarak görmemişlerdir.

4.1.7 "Öğrencilerin Çevrim İçi Sınavlara Erişim Sürecinde Hileye Başvurma Eylemini En Az Seviyeye İndirecek Kimlik Doğrulama Şeması Hangisidir?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının yapılan çevrim içi sınavlara erişim sağlarken, öğrencilerin kimlik doğrulama seçenekleri arasından hileye başvurmalarını zorlaştırabilecek kimlik doğrulama şemalarına yönelik yaptığı yorumlar şöyledir:

Tablo 9. Hileye Başvurmayı Zorlaştıracak Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	-	-	**Parola**	-	-
			Tek Kullanımlık Şifre	-	-
Kalıtım Faktörü	7	70	**Parmak İzi**	3	30
			Yüz Tarama	4	40
Sahiplik Faktörü	3	30	**Fiziksel Aygıt**	3	30

Yüz taramaya göre parmak izini tercih ederim. Birine parmak izinizi vererek kullanmasını söyleyemezsiniz bu nedenle en çok zorlaştıracak da parmak izi olur. (K1)

Fiziksel aygıt olabilir. İki cihazdan da doğrulama sağlanması ve doğrulama işleminin belli bir sürede gerçekleşmesi noktasında bu durumu biraz da olsa engelleyecektir. (K2)

Yüz tarama ve parmak izini ihlal etmeleri çok zor o yüzden bu ikisini söyleyebilirim. (K3)

Parmak izi zorlaştırır ama parmak izi için de kullanılan alanın bozulması öğrencinin sınava girişini engelleyebilir ya da geciktirebilir. Bu nedenle fiziksel aygıt diyebilirim, hileye başvurmayı aza indirebilir. (K4)

Dediğim gibi öğrenci eğer iyi niyetli değilse bu beş kimlik doğrulamasını da hileye başvurmada bir şekilde kullanır. Ama en aza indirmeden bahsettiğimiz için yüz taramayı tercih edeceğim. (K5)

Yüz tarama zorlaştıracaktır. Tamamen kişinin kendisinin olması gerekiyor bu sistemde. (K6)

Ya parmak izi ya da yüz tarama. Bu çok zor gerçekten hatta öğrenci kendi bile giremeyebilir. (K7)

Parmak izi diyorum. Tamamen kişiye özel bir bilgi parmak izi. Onun olması şart. (K8)

Zorlaştırması için iki doğrulamanın olması daha mantıklı dolayısıyla fiziksel aygıt iyi olabilir. Aynı şekilde yüz tarama da eğer dediğim sorunları aşmış olursa o da zorlaştıracaktır. (K9)

Yüz tarama olur. Eğer bir ikiz kardeşi yoksa tamamen kişinin o kişi olduğunu doğrulayacak sistem yüz tarama olur. (K10)

Tablo 9'da öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını zorlaştıracak kimlik doğrulama şemalarının değerleri verilmiştir. Öğretim elemanlarının %70'i kalıtım/biyometrik faktörün hileye başvurma eylemini zorlaştıracağını belirtmiştir. Katılımcıların bazıları yüz tarama şeması kullanıldığında öğrencinin kendisi dışında bir başkasını sınava dahil edemeyeceğini, sınava bizzat kendisinin girmesi gerektiğini ifade etmişlerdir. Aynı şekilde parmak izinin kişiye özel bir biyometrik özelliğe sahip olması nedeniyle öğrencilerin bu tür bir bilgiyi paylaşma konusunda tereddüt yaşayacağını belirtmişlerdir. %30 orana sahip tek kullanımlık şifre için öğretim üyeleri iki kimlik doğrulama içermesi nedeniyle hileye başvurma eylemini tamamen ortadan kaldırmasa da aza indirebileceği konusunda değerlendirmelerde bulunmuşlardır. Ayrıca katılımcılar parmak izi ve yüz tarama şemasına göre fiziksel aygıt şemasında daha az sorunlar ortaya çıkacağını da paylaşmışlardır. Öğretim üyeleri Tablo 9'da da görüldüğü gibi parola ve tek kullanımlık şifre şemalarını paylaşılabilir ve gönderilebilir olması nedeniyle hileye başvurma eylemini zorlaştıracak şemalardan biri olarak görmemişlerdir.

4.1.8 "Şu An Sahip Olduğunuz Akıllı Telefonunuzun Kilit Ekranında, Hangi Kimlik Doğrulama Şemasını Kullanıyorsunuz?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim elemanlarının sahip olduğu akıllı telefonların kilit ekranında kullanılan kimlik doğrulama şemaları şöyledir:

Tablo 10. Katılımcıların Kilit Ekranında Kullandığı Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	4	40	**Parola**	4	40
			Tek Kullanımlık Şifre	-	-
Kalıtım Faktörü	6	60	**Parmak İzi**	4	40
			Yüz Tarama	2	20
Sahiplik Faktörü	-	-	**Fiziksel Aygıt**	-	-

Desen ve parmak izi kullanıyorum. (K1)

Parola kullanıyorum. (K2)

> Telefonumda hızlı işlem yapmak için parola kullanıyorum, parola ve yüz taramada bazen sorunlar yaşayabiliyorum. Farklı cihazlarımda farklı kimlik doğrulamalar da kullanıyorum, yüz tarama, parmak izi gibi. (K3)
>
> Parmak izi kullanıyorum. (K4)
>
> Parolaya alıştım onu kullanıyorum. (K5)
>
> Ben laboratuvarda çalıştığım için herhangi bir doğrulama kullanmıyorum. Önceden yüz taramayı tercih ediyordum. Pandemide maske kullandığımız sıralarda yüz tarama fonksiyonunda sıkıntı yaşadım. Eldiven kullandığım için parmak izi de kullanamadım. En sonunda tamamen doğrulamayı kaldırdım. Kullanacak olsam yine yüz taramayı kullanırım. (K6)
>
> Parmak izini kullanıyorum. (K7)
>
> Parola kullanıyorum. (K8)
>
> Yüz tarama kullanıyorum. Çok kolay bir kullanımı var ve ben çok beğenerek kullanıyorum. (K9)
>
> Kolaylık sağladığı için desen ve parmak izi kullanıyorum ben. (K10)

Tablo 9'da öğretim elemanlarının sahip olduğu akıllı telefonlarının kilit ekranında kullandığı kimlik doğrulama şemaları verilmiştir. Parola ve parmak izi şeması katılımcılar tarafından %40 oranında kullanılmaktadır. Parola şeması geçmişten bugüne yaygın olarak kullanılan bir şema olmasına rağmen bu çalışmada, parmak izi şeması parola ile aynı yüzdeye sahip olmuştur. Genel olarak bakıldığında kalıtım faktörüne bağlı kimlik doğrulama şemaları %60 oranla katılımcıların akıllı telefonunda tercih ettiği kimlik doğrulama şemalarından (parmak izi, yüz tarama) olmuştur. Bunun nedeni kolay kullanım ve yüksek güvenlik önlemi içermesi tercih edilme sebeplerindendir.

4.1.9 "Bu Çalışmada Yer Almayan Ancak Kullanmak İstediğiniz Başka Bir Kimlik Doğrulama Şeması Var mı?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğretim üyeleri çalışmada yer almayan ancak kendilerinin önereceği kimlik doğrulama şemalarını belirtmişlerdir. Öneriler şöyledir:

> Yok ama ben mümkün olduğunca öğrencinin varlığından emin olmak isterim. O anlamda öğrencinin fiziki olarak orada bulunduğunu gösteren bir kimlik doğrulama olarak parmak izini tercih ederim. Fotoğraftan tanımlanabilme ihtimalini düşündüğüm için yüz tarama demeyeceğim. Parmak izi dışındaki diğer dört kimlik doğrulama öğrencinin bilgisayar başında olmadan da başka birisini sınava sokabileceği bir yöntem gibi geliyor. Dolayısıyla ben burada bir tek parmak izini tercih edebilirim. Parmak izi dışındaki

diğer dört kimlik doğrulama öğrencinin bilgisayar başında olmadan da başka birisini sınava sokabileceği bir yöntem gibi geliyor. Dolayısıyla ben burada bir tek parmak izini tercih edebilirim. (K1)

Öğrencinin giriş yaparken 365 derece bulunduğu yerdeki tüm alanı gösteren ve onun yüzünü algılayarak erişim sağlayan bir sistem olabilir. (K5)

Yok. Çevrim içi yapılan sınavların en büyük problemi aslında internetin her yerde ideal düzeyde olmaması. Ama kullanmak için bana göre yüz tarama uygun. (K6)

İzlediğim bir filmde görmüştüm. Bu sistem uygulanırsa bence hileye başvurma ya da benzeri sorunlar yaşanmaz. Cihaza parmağını yerleştiriyor birkaç saniye içinde kanını test ederek kişinin o olup olmadığını gösteriyor. (K7)

Biz üniversitemizde QR kod kullanıyoruz. Öğretim üyelerine bir uygulama tasarladılar. Sınav esnasında öğrencilerin her birinin kendine ait QR kodu bulunuyor. Sistemde kayıtlı telefon numaralarına QR kod gönderiliyor. Biz ekranımızdan o kodları okutarak öğrencilerin kimliğini tespit etmiş oluyoruz. (K8)

Aklıma gelmiyor. Benim sınavlarıma başka birilerini dahil etmeleri yani hileye başvurmaları bir kazanç sağlamaz. Çünkü tamamen kendilerinin düşünüp yorum yapmalarını gerektiren, benim ders sırasında verdiğim bilgileri de içeren sorular soruyorum. Cevapları bir yerden bulmaları mümkün değil. (K9)

Şu an bilemiyorum. Çalışmadaki şemalardan ben olsam yüz taramayı kullanırdım. Ehliyet sınavında uygulandığını görmüştüm bence sınavlar için çok uygun. Maliyet bakımından da çok masraf olacağını düşünmüyorum. Bu uygulama bence sınav güvenirliğini de artırır. (K10)

Katılımcılar genel olarak sınava girecek öğrencilerin fiziki olarak sınavda bulunduğundan emin olmak istediklerini ifade etmişlerdir. Ayrıca öğretim üyelerine göre çevrim içi yapılan sınavların en büyük problemi, her yerdeki internet çekim gücünün ideal düzeyde olmamasıdır. Verilen yanıtlardan bazıları, parmak izi kimlik doğrulaması dışında diğer 4 kimlik doğrulama şemasının öğrencinin bilgisayar başında olmadan da bir başkasını sınava sokabileceği yönündedir.

4.2. Üniversite Öğrencilerine Ait Bulgular ve Yorumlar

Araştırmacı tarafından hazırlanan yarı yapılandırılmış "kimlik doğrulama görüşme formu"na yönelik üniversite öğrencilerinin verdiği yanıtların çözümlenmesi sonucunda elde edilen bulgular, araştırma sorularının sırasına uygun olarak açıklamalarıyla birlikte verilmiştir.

4.1.1 "Üniversite Öğrencilerinin Ölçme Değerlendirme Sürecinde Öğrenci Gizliliği Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Araştırmada yer alan 5 adet kimlik doğrulama şemasının öğrenci gizliliği göz önüne alındığında üniversite öğrencilerinin görüşleri şöyledir:

Tablo 11. Öğrenci Gizliliği Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	2	25	**Parola**	1	12,5
			Tek Kullanımlık Şifre	1	12,5
Kalıtım Faktörü	5	62,5	**Parmak İzi**	1	12,5
			Yüz Tarama	4	50
Sahiplik Faktörü	1	12,5	**Fiziksel Aygıt**	1	12,5

Gizlilik için bence parmak izi çok uygun. Gizliliğin güvenliğini düşünerek parmak izi demek istedim. (Ö1)

Bence yüz tanıma. Parmak izi daha özel o yüzden yüzün paylaşımı sorun olmaz diye düşünüyorum. (Ö2)

Yüz tanıma uygun. Çok önemli değil yüzün paylaşımı. (Ö3)

Yüz tanıma diye düşünüyorum. Paylaşılamaz bir doğrulama. (Ö4)

Gizlilik açısından parmak izi ya da yüz tarama daha mantıklı. (Ö5)

Parola. Hem şu anda onu kullanıyorum ve hem de benimle ilgili özel bilgiye sahip değil. (Ö6)

Öğrencinin kendi bilgilerinin gizliliği açısından tek kullanımlık şifre diyorum. Çünkü diğer tüm doğrulamalar için kendimle ilgili bir bilgi paylaşmam gerekecek. Tek kullanımlık şifrede herhangi bir data kaydetmiyor. (Ö7)

Öğrenci gizliliği için fiziksel aygıt yeterli. (Ö8)

Araştırmaya katılan öğrenciler araştırmacı tarafından hazırlanan yarı yapılandırılmış görüşme formunda yer alan sorulara ilişkin verdikleri yanıtlar içerik analizi yapılarak görüşleri aktarılmış ve Tablo 11'de gösterilmiştir. Verilen yanıtlar incelendiğinde öğrencilerin öğrenci gizliliğini göz önünde bulundurarak çevrim içi sınavlara erişim sağlamak için kullanmayı en çok tercih ettiği kimlik doğrulama şeması %50 oranla kalıtım faktörüne bağlı yüz tarama şeması olmuştur. Yapılan yorumlara göre öğrencilerin sistemle yüz paylaşılması konusunda herhangi bir endişe taşımadığı sonucuna ulaşılmıştır. Yüz tarama şeması katılımcılar için öğrenci gizliliğini ihlal eden bir durum olarak görülmemiştir. Üniversitenin öğrenci bilgi sisteminde öğrencilerin

fotoğraflarının olması yüz tarama kimlik doğrulama şemasının benimsenmesinde önemli bir etkendir. Ayrıca yüz taramanın öğrenci gizliliğinin ihlali olarak görülmemesinin nedeni kullanımı milyonlarca kullanıcıyı kapsayan sosyal medya olarak görülmüştür. Sosyal medya gibi mecralarda fotoğraf paylaşımının normal olarak karşılanması, yüz tarama şeması için verilecek yüz verisinin kullanıcılar için önemli bir biyometrik veri olarak görülmemesine neden olmuştur. Parola, tek kullanımlık şifre, parmak izi ve fiziksel aygıt %12,5 oranında tercih edilmiştir. Kalıtım faktörünün bir diğer şeması olan parmak izi ise kullanıcının en önemli biyometrik bilgisi olan parmak izini içerdiğinden yalnızca bir katılımcı tarafından tercih edilmiştir. Sonuç olarak Tablo 11 değerlendirildiğinde kalıtım faktörü %62,5 oranla öğrenci gizliliği için uygun bulunmuştur.

4.1.2 "Üniversite Öğrencilerinin Ölçme Değerlendirme Sürecinde Sistem Güvenliği Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Üniversite öğrencilerinin sistem güvenliğini düşünerek tercih ettikleri kimlik doğrulama şemaları için yapmış olduğu değerlendirmeler şöyledir:

Tablo 12. Sistem Güvenliği Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	3	37,5	**Parola**	1	12,5
			Tek Kullanımlık Şifre	2	25
Kalıtım Faktörü	1	12,5	**Parmak İzi**	-	-
			Yüz Tarama	1	12,5
Sahiplik Faktörü	4	50	**Fiziksel Aygıt**	4	50

Sistemi düşünürsek o zaman fiziksel aygıt derim. Fiziksel aygıt güvenliği rahatça sağlar. (Ö1)

Aslında bakarsanız hiçbirinin güvenli olduğunu düşünmüyorum. Eğer bir tane söylemem gerekirse tek kullanımlık şifre olabilir. (Ö2)

Tek kullanımlık şifre daha güvenli olabilir, parolayı başkaları ezberleyebilir bulabilir o yüzden tek kullanımlık şifre diyorum. (Ö3)

Üniversite sistemini düşündüğüm zaman fiziksel aygıt derim diye düşünüyorum. İki doğrulama yapacak ve büyük bir data kaydetmeyecek. (Ö4)

Şu an kendi üniversite sistemimde kullanıcı mail adresimiz ve parolamız var. Bu tür bir girişin güvenli olduğunu düşünüyorum bu yüzden parola diyorum. (Ö5)

Fiziksel aygıt diyeceğim. İki doğrulama yapmam gerekiyor çok güvenli bence. (Ö6)

> Bence yüz tarama. Fiziksel aygıtta şöyle bir durum var: Parolam ve harici cihazım bir başkasında olabilir. Bu aşılabilecek bir şey. Maliyet açısından belki zorlayıcı olabilir ama yine de yüz tarama diyorum. (K7)
>
> Bunda da aynı şekilde hem öğrenci gizliliği hem güvenlik için fiziksel aygıt dediğiniz çift doğrulama yeterli. (Ö8)

Araştırmaya katılan öğrencilerin verdiği yanıtlar içerik analizi yapılarak görüşleri aktarılmış ve Tablo 12'de gösterilmiştir. Sistem güvenliğini göz önünde bulundurarak öğrencilerin vermiş olduğu yanıtlar, çevrim içi sınavlara erişim sağlamak için kullanmayı en çok tercih ettiği kimlik doğrulama şemasının %50 oranla sahiplik faktörüne bağlı fiziksel aygıt şeması olduğunu göstermektedir. Öğrenciler fiziksel aygıt şemasının çift doğrulama/iki kimlik doğrulama seçeneği sunması sebebiyle sistem güvenliği için uygun olduğu değerlendirmelerinde bulunmuşlardır. Bunu takiben %25 oranla tek kullanımlık şifre şeması tercih edilmiştir. Verilen yanıtlara göre parola bir başkası tarafından ezberlenebilir ve kullanılabilir yönündedir. Ancak tek kullanımlık şifrenin parola şeması ile karşılaştırıldığında daha yüksek bir güvenliğe sahip olduğu algısı mevcuttur. Ayrıca öğrenciler sahip oldukları mevcut sistemde var olan parolanın güvenlik bakımından yeterli olduğunu ifade etmişlerdir.

Sonuç olarak Tablo 12'ye bakılarak sistem güvenliği düşünüldüğünde sahiplik faktörü %50 oranında tercih edilirken, bilgi faktörü %37,5 oranında tercih edilmiştir. Yalnızca bir öğrenci (K7) yüz tarama şemasını tercih etmiştir. K7'ye göre parola ve tek kullanımlık şifre kolay bir şekilde başkasına verilebilir ve çalınabilir nitelikte olduğunu; fiziksel aygıtın iki aşamalı doğrulama için parola ve harici cihazının bir başkasında olabileceğini, ancak yüz taramada bu tür durumların mevcut olmadığını ve yüz taramanın sistem güvenliği düşünüldüğünde daha uygun olduğunu ifade etmiştir.

4.1.3 "Üniversite Öğrencilerinin Ölçme Değerlendirme Sürecinde Kullanılabilirlik Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Üniversite öğrencilerinin kimlik doğrulama şemalarını kullanılabilirlik bakımından değerlendirerek yapmış olduğu yorumlar şöyledir:

Tablo 13. Kullanılabilirlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	4	50	**Parola**	2	25
			Tek Kullanımlık Şifre	2	25
Kalıtım Faktörü	3	37,5	**Parmak İzi**	3	37,5

			Yüz Tarama	-	-
Sahiplik Faktörü	1	12,5	**Fiziksel Aygıt**	1	12,5

Herkesin rahatça kullanabileceğini düşünürsem parola, şifre olur cevabım. (Ö1)

Sadece kullanılabilirlik için düşünürsem parmak izi uygun bence. (Ö2)

Tek kullanımlık şifre derim yine her açıdan uygun. (Ö3)

Günümüzde online alışverişin de çok yaygınlaşması sebebiyle örneğin harcama yaparken daha aşinayız fiziksel aygıt doğrulamasına. O yüzden öğrenci açısından kullanılabilirliği en yüksek fiziksel aygıt olur. (Ö4)

Parmak izi ya da yüz tanıma herkesin kullanabileceği bir sistem olur. (Ö5)

En rahat parola bence. Günlük hayatımızda her yerde kullanıyoruz. Tek kullanımlık şifre parolaya göre daha çabuk unutulabiliyor. Parmak izi ve yüz taramayı güvenirliği az olması nedeniyle tercih etmem. (Ö6)

Bunun için de parola ve tek kullanımlık şifre mantıklı. İkisi arasından seçersem tek kullanımlık şifre derim çünkü hatırlamak zorunda değilim. Yüz tarama için kamera olmak zorunda, parmak izi için parmak izi okuyucusu olmalı. Fiziksel aygıtta harici bir aygıt lazım. Bunlara her zaman sahip olmayabiliriz. (Ö7)

Parmak izi kullanım için çok uygun rahat. (Ö8)

Üniversite öğrencilerinin ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını kullanılabilirlik bakımından değerlendirmeleri istendiğinde, en çok tercih ettikleri şemanın kalıtım faktörüne bağlı parmak izi şeması olduğu görülmüştür. Öğrenciler yaptıkları değerlendirmelerde kullanılabilirlik bakımından yüz tarama şemasının kolaylık sağladığını ancak herkesin her yerden her an ulaşamayacağını dile getirmişlerdir. Bilgi faktörüne bağlı parola ve tek kullanımlık şifrenin herkes tarafından kullanılabileceğini ve her yerden erişim sağlanabileceği görüşünde olduklarını belirtmişlerdir. Tablo 13'e bakıldığında bilgi faktörü %50 oranında tercih edilmiştir. Bunun sebeplerinden biri kullanıcılar genel anlamda var olan yaygın kullanım dışında farklı bir kimlik doğrulama şeması tercih etmekte tereddüt yaşamaktadır. Diğer yandan parmak izinin de günümüzde yaygınlaştığını ve birçok akıllı cihazda parmak izinin yer aldığını söyleyerek, parmak izi şemasını %37,5 oranında tercih etmişlerdir.

4.1.4 "Üniversite Öğrencilerinin Ölçme Değerlendirme Sürecinde Bilgi Güvenliği Unsurları Olan Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından En Uygun Bulduğu Kimlik Doğrulama Şeması Nedir? 1 ile 10 Arasında Puanlama Yapınız." Sorusuna Yönelik Elde Edilen Yorumlar

Üniversite öğrencilerinin ölçme değerlendirme sürecini bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirerek yaptıkları yorumlar ve puanlamaları şöyledir:

Tablo 14. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	2	25	**Parola**	1	12,5
			Tek Kullanımlık Şifre	1	12,5
Kalıtım Faktörü	3	37,5	**Parmak İzi**	3	37,5
			Yüz Tarama	-	-
Sahiplik Faktörü	3	37,5	**Fiziksel Aygıt**	3	37,5

Ben yine parmak izi derdim buna. Çünkü en güvenilir olarak onu düşündüm, kullanımı da iyi ve kendi şahsıma ait olduğu için. Parmak izi 10, yüz tanıma 9, fiziksel aygıt 8, parola 7, tek kullanımlık şifre 6. (Ö1)

Galiba üçünü düşündüğümde yine parmak izi derim hem daha kolay hem daha güvenli olduğunu düşünüyorum. Parmak izi 8, yüz tanıma 7, fiziksel aygıt 7, tek kullanımlık 5, parola 3. (Ö2)

Yine tek kullanımlık şifre derim. Çünkü parolayı herkes ezberleyebilir ve giriş yapabilir ayrıca herkesle paylaşma durumu söz konusu. Parmak izi için sensörlü cihaza ihtiyacınız var ve her zaman yanınızda olmayabilir. Yüz tanımada tesettürlüyüm ben ve her zaman algılamayabiliyor. Gözlük bile taksak algılamayabiliyor. Fiziksel aygıtsa bir telefon ihtiyacınız var ama o an yanımızda olmayabilir ya da şarjı olmayabilir. O nedenle tek kullanımlık şifre en mantıklısı. Tek kullanımlık şifre 8, fiziksel aygıt 7, parmak izi 6, yüz tanıma 6, parola 5. (Ö3)

Parola çok sık kullanılan ama güvenlik bakımından çok iyi değil. Yüz tanımanın ya da parmak izinin ergonomik bakımdan çok yeterli olmadığını düşünüyorum öğrenicinin erişim için zorlanacağını düşünüyorum ve bunun yanında diğerlerine göre güvenlik bakımından üst seviyede. Fiziksel aygıt daha makul geliyor. Üçünü birlikte değerlendirirken de aslında daha çok kullanılabilirliği önemseyerek cevaplıyorum. Fiziksel aygıt diyeceğim hem güvenlik bakımından hem kullanılabilirliği çok yüksek, gizlilik için de bir sorun teşkil etmiyor. Fiziksel aygıt 10, tek kullanımlık şifre 8, parmak izi 7, yüz tarama 6, parola 5. (Ö4)

Hem kullanım açısından hem güvenlik için parmak izini tercih ederim daha sonra da yüz tanıma. Tek kullanımlık şifre biraz daha bence geri planda kalıyor. Parola parmak izinden bir tık geride kalabilir ama

o da uygun. Parolada ezberlediğin ve unutmadığın sürece sorun yaşanmaz. Fiziksel aygıtta da ayrıca bir kod gönderdiği için bu da çok uygun kullanılabilir güvenli ve gizliliği başarılı. Parmak izi 10, Yüz tanıma 10, parola 9, fiziksel aygıt 9, tek kullanımlık şifre 2. (Ö5)

Günlük hayatımızda fiziksel aygıtın kullanımı vakit kaybettirebilir. Bu yüzden ben yine parola diyeceğim. Yüz tarama ve parmak izini güvenlik bakımından endişe ediyorum ve kullanmayı tercih etmem. Ayrıca herkesin telefonu parmak izini desteklemeyebilir. Tek kullanımlık şifre de şöyle, parolaya göre kullanımı daha kolay ama tekrar tekrar almak gerekebiliyor. Bu yüzden ben her açıdan parolayı tercih ederim. Parola 10, fiziksel aygıt 9, tek kullanımlık şifre 8, parmak izi 5, yüz tanıma 3. (Ö6)

Fiziksel aygıt için bana ikinci bir cihaz gerekiyor. Fiziksel aygıt ve tek kullanımlık şifre kullanılabilirlik açısından aynı seviyede. Ama fiziksel aygıt ayrıca bir doğrulama daha istediği için güvenlik bakımından daha iyi. Fiziksel aygıt 8, yüz tarama 8, tek kullanımlık şifre 5, parmak izi 3, parola 1. (Ö7)

Yüz tarama parmak izine göre çok yaygın değil. Şu anki teknoloji için biraz daha zamanı var. Fiziksel aygıt 8, parmak izi 6, parola 5, yüz tarama 4, tek kullanımlık şifre 1. (Ö8)

Üniversite öğrencilerinin ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını kullanılabilirlik bakımından değerlendirmeleri istendiğinde, en çok tercih ettikleri şemanın kalıtım faktörüne bağlı parmak izi şeması ve sahiplik faktörüne bağlı fiziksel aygıt olduğu görülmüştür. Öğrenciler yaptıkları değerlendirmelerde kullanılabilirlik bakımından parmak izi ve yüz tarama şemasını uygun olarak görseler de bu şemalar için gerek parmak izi okuyucusuna ve gerekse yüz tanıma sistemine herkesin sahip olamayacağını belirterek erişilebilirlik için uygun olmadığı sonucuna ulaşmışlardır.

Tablo 15. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Madde	**Katılımcılar**									
Kimlik Doğrulama Şemaları	***Ö1***	***Ö2***	***Ö3***	***Ö4***	***Ö5***	***Ö6***	***Ö7***	***Ö8***	$\bar{X}$	**%**
Parola	7	3	5	5	9	10	1	5	5,625	17
Tek Kullanımlık Şifre	6	5	8	8	2	8	5	1	5,375	16
Parmak İzi	10	8	6	7	10	5	3	6	6,875	21
Yüz Tarama	9	7	6	6	10	3	8	4	6,625	20
Fiziksel Aygıt	8	7	7	10	9	9	8	8	8,25	25

Katılımcılar kimlik doğrulama şemalarını 1 ila 10 puan arasında değerlendirmiştir.

Katılımcıların kimlik doğrulama şemaları için 1 ila 10 (1 en düşük, 10 en yüksek) arasında verdiği puanlar ve her bir kimlik doğrulama şeması için verilen puanların ortalaması Tablo 15'te gösterilmiştir. Kullanılabilirlik, gizlilik ve güvenlik bakımından fiziksel aygıt şeması ($\overline{X}$=8,25) puan ortalaması ile en çok tercih edilen, ölçme değerlendirme süreci için en uygun bulunan kimlik doğrulama şeması olmuştur. Parmak izi şeması ($\overline{X}$=6,875) puan ortalaması ile fiziksel aygıttan sonra en çok tercih edilen ve uygun görülen şema olmuştur. Sıralamada üçüncü olarak yüz tarama şeması ($\overline{X}$=6,625) puan ortalamasına sahiptir.

Tablo 16. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Kimlik Doğrulama Faktörleri	*Genel %*	$\bar{X}$	%	Kimlik Doğrulama Şemaları
Bilgi Faktörü	33	5,625	17	**Parola**
		5,375	16	**Tek Kullanımlık Şifre**
Kalıtım Faktörü	41	6,875	21	**Parmak İzi**
		6,625	20	**Yüz Tarama**
Sahiplik Faktörü	25	8,25	25	**Fiziksel Aygıt**

Katılımcılar kimlik doğrulama şemalarını 1 ila 10 puan arasında değerlendirmiştir.

Tablo 16'da kimlik doğrulama faktörlerinin genel yüzdelik değerleri gösterilmiştir. Buna göre bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirildiğinde %41 oranla kalıtım faktörü en çok tercih edilen kimlik doğrulama şemalarını içermektedir. Tercihen ikinci olarak %33 oranla bilgi faktörü ve üçüncü olarak %25 oranla sahiplik faktörü olmuştur.

4.1.5 "Üniversite Öğrencilerinin Ölçme Değerlendirme Sürecinde Bilgi Güvenliği Unsurları Olan Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Uygun Olmayan, Beğenmedikleri Kimlik Doğrulama Şeması Nedir?" Sorusuna Yönelik Elde Edilen Yorumlar

Üniversite öğrencilerinin ölçme değerlendirme sürecini bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirerek uygun bulmadıkları kimlik doğrulama şemalarına yönelik yaptıkları yorumlar şöyledir:

Tablo 17. Kullanılabilirlik, Gizlilik ve Güvenlik Bakımından Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri.

Madde	Katılımcılar									
Kimlik Doğrulama Şemaları	***Ö1***	***Ö2***	***Ö3***	***Ö4***	***Ö5***	***Ö6***	***Ö7***	***Ö8***	$\bar{X}$	**%**
Parola	7	3	5	5	9	10	1	5	5,625	17

Tek Kullanımlık Şifre	6	5	8	8	2	8	5	1	5,375	16
Parmak İzi	10	8	6	7	10	5	3	6	6,875	21
Yüz Tarama	9	7	6	6	10	3	8	4	6,625	20
Fiziksel Aygıt	8	7	7	10	9	9	8	8	8,25	25

Katılımcılar kimlik doğrulama şemalarını 1 – 10 puan arasında değerlendirmiştir.

Tek kullanımlık şifreyi en son tercih ederdim. Gizlilik ve güvenlik için çok iyi gelmiyor bana göre. (Ö1)

Parola bunlara baktığımda yetersiz gibi. (Ö2)

Parola en uygun olmayan. Herkes ezberleyebilir ve giriş yapabilir ayrıca herkesle paylaşma durumu söz konusu. (Ö3)

Parolanın kullanımı kolay ancak erişilebilir ve yayılabilir. Ayrıca güvenli olduğunu düşünmüyorum, öğrenci gizliliğini koruduğunu düşünmüyorum. Paylaşılabilir, kolayca erişilebilir, bir başkasına verilebilir. Öğrencinin kopya çekme noktasında bir caydırıcılık özelliği olmadığını düşünüyorum. (Ö4)

Tek kullanımlık şifrede güvenlik ön plana çıkıyor ve güvenilir bulmuyorum tehlike olduğunu düşünüyorum. Hacklenme olabilir. Kullanılabilirlik bakımından da tercih etmem. (Ö5)

Yüz tarama ve parmak izini güvenlik bakımından endişe ediyorum ve kullanmayı tercih etmem. Ayrıca herkesin telefonu parmak izini desteklemeyebilir. (Ö6)

En uygun olmadığını düşündüğüm parola. Çünkü en esnek aşılabilir yöntem o. Kullanılabilirlik için iyi ancak gizlilik ve güvenlik için yetersiz. Sonrasında parmak izi. Bu her ne kadar güvenlik ve gizlilik için iyi bir şey sağlasa da kullanılabilirliği çok düşük. (Ö7)

Tek kullanımlık şifre çok zahmetli geliyor bana. (Ö8)

Tablo 17 incelendiğinde parola şeması ($\overline{X}$=5,625) ve tek kullanımlık şifre şeması ($\overline{X}$=5,375) puan ortalamasıyla en az tercih edilen, ölçme değerlendirme süreci için uygun bulunmayan kimlik doğrulama şeması olmuştur. Bunun nedeni olarak kullanıcılar parolanın her zaman hatırlamak zorunda oldukları bir kimlik doğrulama olması nedeniyle gizlilik ve güvenliği yetersiz bulmuşlardır. Öğrenciler için tek kullanımlık şifre ise birçok kez sistem tarafından gönderileceği için kullanım zorluğuna sebebiyet verecektir. Ayrıca öğrencilerden bazıları kalıtım faktörüne bağlı kimlik doğrulama şemalarının (parmak izi, yüz tarama) kullanım kolaylığı ve sisteme giriş işlemi için hızlı bir erişim sağladığı yönünde değerlendirmelerde bulunmuşlardır. Ancak kalıtım faktörüne bağlı kimlik doğrulama şemalarının kullanımı konusunda gizlilik ve güvenlik noktasında endişeleri olduğunu belirtmişlerdir.

Öğrencilerden bazıları kalıtım faktörüne bağlı kimlik doğrulama şemalarının (parmak izi, yüz tarama) sisteme entegre edilmesinin zorluklarını ve bu sistemin doğru bir şekilde çalışması

konusunda endişeleri olduğunu belirtmişlerdir. Ayrıca parmak izi gibi bir kimlik doğrulama şemasının kullanıcıya ait önemli ve büyük bir kişisel bilgi içermesi nedeniyle sisteme böyle bir veri tanımlamanın uygun olmadığını belirtmişlerdir. Öğrenciler tarafından kalıtım faktörüne bağlı kimlik doğrulama şemalarının (parmak izi ve yüz tarama) gerekli organını kaybetme, yaralanma gibi durumlarda sisteme erişimin zor olması ya da erişim sağlanamaması gibi sorunlara yola açacağı değerlendirmesinde bulunmuşlardır. Araştırmaya katılan iki öğretim elemanı ise iki aşamalı bir kimlik doğrulama şeması sunması ve herkesin her an yanında ikinci bir aygıt taşımasının mümkün olmadığını belirterek fiziksel aygıtı uygun bulmadıklarını belirtmişlerdir. Bir diğer değerlendirme ise parolanın gizlilik ve güvenlik için yetersiz olduğu ve zaman zaman unutma ya da kaybetme gibi durumlar nedeniyle kullanılabilirlik bakımından da yeterli bulunmadığı yönünde olmuştur.

4.1.6 "Öğrencilerin Çevrim İçi Sınavlara Erişim Sürecinde Hileye Başvurmalarını En Çok Kolaylaştırabilecek Kimlik Doğrulama Şeması Hangisidir?" Sorusuna Yönelik Elde Edilen Yorumlar

Yapılan çevrim içi sınavlara erişim sağlarken, öğrencilerin kimlik doğrulama seçenekleri arasından hileye başvurmalarını kolaylaştırabilecek kimlik doğrulama şemalarına yönelik yapılan yorumlar şöyledir:

Tablo 18. Hileye Başvurmayı Kolaylaştıracak Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	8	100	**Parola**	6	75
			Tek Kullanımlık Şifre	2	25
Kalıtım Faktörü	-	-	**Parmak İzi**	-	-
			Yüz Tarama	-	-
Sahiplik Faktörü	-	-	**Fiziksel Aygıt**	-	-

Parola tabii. Herkese kolay bir şekilde yayılabilir çünkü. (Ö1)

Parola bu tür durumları kolaylaştırır, kolaylaştırıyor da. (Ö2)

Parola derim. Yüz tanımada kimseyle paylaşamazsınız. Orada etkin olmanız gerekli. (Ö3)

Parola olduğunu düşünüyorum. Paylaşılabilir, kolayca erişilebilir, bir başkasına verilebilir. Öğrencinin kopya çekme noktasında bir caydırıcılık özelliği olmadığını düşünüyorum. (Ö4)

Bir başkası kimlik numarası ve parolayla rahatlıkla giriş yapabilir sınava girebilir. (Ö5)

Tek kullanımlık şifre en kolay o olur. Kolayca paylaşılır ve kopya çekilir. (Ö6)

Parola herkes tarafından kullanılabilir. Yanımda ya da uzaktaki birine verebilirim aynı şekilde tek kullanımlık şifre için de bu durum geçerli. (Ö7)

Tek kullanımlık şifreyi istediği zaman istediği yere gönderebilir. (Ö8)

Tablo 18'de öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını kolaylaştıracak kimlik doğrulama şemalarının değerleri verilmiştir. Çalışmaya katılan öğrencilerin tamamı %100 oranla bilgi faktörünün hileye başvurma eylemini kolaylaştıracağını belirtmiştir. Katılımcıların 8'i öğretim üyeleri ile benzer nitelikte yorumlar yaparak parolanın kendileri dışında biriyle kolay bir şekilde paylaşılabileceğini bu nedenle hileye başvurma eylemini de kolaylaştıracağını ifade etmişlerdir. 2 katılımcı tek kullanımlık şifre paylaşılırken ya da birine gönderilirken parolaya göre daha az endişe taşıdığını ve kolaylıkla gönderilebileceğini belirtmiştir. Öğrenciler de öğretim üyeleri gibi Tablo 18'de görüldüğü gibi parmak izi, yüz tarama ve fiziksel aygıt şemalarını hileye başvurma eylemini kolaylaştıracak kimlik doğrulama şemalarından biri olarak görmemişlerdir.

4.1.7 "Öğrencilerin Çevrim İçi Sınavlara Erişim Sürecinde Hileye Başvurma Eylemini En Az Seviyeye İndirecek Kimlik Doğrulama Şeması Hangisidir?" Sorusuna Yönelik Elde Edilen Yorumlar

Çalışmaya katılan öğrencilerin yapılan çevrim içi sınavlara erişim sağlarken, kimlik doğrulama seçenekleri arasından hileye başvurmalarını zorlaştırabilecek kimlik doğrulama şemalarına yönelik yaptığı yorumlar şöyledir:

Tablo 19. Hileye Başvurmayı Zorlaştıracak Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	-	-	**Parola**	-	-
			Tek Kullanımlık Şifre	-	-
Kalıtım Faktörü	8	100	**Parmak İzi**	2	25
			Yüz Tarama	6	75
Sahiplik Faktörü	-	-	**Fiziksel Aygıt**	-	-

İlk sırada parmak izi, ikinci olarak fiziksel aygıt olabilir. Çünkü parmak izini birine gönderemeyiz, paylaşamayız. (Ö1)

Yüz tanıma. Çünkü başka biri bizim yüzümüz olmadan giriş yapamaz. Ama parolada bunu yapabilir. (Ö2)

Dediğim gibi parmak izi paylaşılamaz herkes tarafından giriş yapılamaz o yüzden parmak izi. (Ö3)

Yüz tanıma üst düzey bir güveliğe sahip olduğu için bu eylemi gerçekleştirmek daha zor olacaktır. (Ö4)

Yüz tanıma ve parmak izi zorlaştırır bunu bizzat kendimizin yapması gerekiyor. (Ö5)

Yüz tanıma dışında diğerlerinde mutlaka hile olacaktır. Yüz tanıma benim kendimin sınava girdiğini daha çok doğrular niteliğe sahip. Tek zorlaştıracak yüz tanıma olur bence. (Ö6)

Yüz tarama güvenlik bakımında üst düzeyde olması nedeniyle onu seçerim. Kamera parmak izi okuyucusuna göre daha yaygın olduğundan yüz tarama derim. Parmak izini seçmeme nedenim öncelikle parmak iziyle sınava girmeye alışık değilim. Hem de her bilgisayarda parmak izi okuyucu olmayabilir. (Ö7)

Yüz tanıma ve parmak izinizle bir başkasının girmesi zordur o yüzden bunlar zorlaştırır. (Ö8)

Tablo 19'da öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını zorlaştıracak kimlik doğrulama şemalarının değerleri verilmiştir. Çalışmaya katılım sağlayan öğrencilerin tamamı %100 oranla kalıtım/biyometrik faktörün hileye başvurma eylemini zorlaştıracağını belirtmiştir. Öğrenciler yüz tarama şeması kullanıldığında öğrencinin kendisi dışında bir başkasını sınava dahil edemeyeceğini, sınava kendileri dışında birinin giremeyeceğini ifade etmişlerdir. Parmak izi şeması yüz tarama şemasına göre daha az tercih edilmiştir. Bunun nedeni olarak öğrencilerin bir kısmı telefonlarında parmak izi okuyucusu olduğunu ancak zaman zaman bu okuyucunun doğru bir şekilde çalışmadığını belirtmiştir. Bu nedenle çevrim içi bir sınava erişim sağlarken sorunlar yaşanabileceği konusunda endişeleri olduğunu söylemişlerdir.

4.1.8 "Şu An Sahip Olduğunuz Akıllı Telefonunuzun Kilit Ekranında, Hangi Kimlik Doğrulama Şemasını Kullanıyorsunuz?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğrencilerin sahip olduğu akıllı telefonların kilit ekranında kullanılan kimlik doğrulama şemaları şöyledir:

Tablo 20. Katılımcıların Kilit Ekranında Kullandığı Kimlik Doğrulama Şemalarının Değerleri.

Kimlik Doğrulama Faktörleri	*N*	%	Kimlik Doğrulama Şemaları	*f*	%
Bilgi Faktörü	3	37,5	**Parola**	3	37,5
			Tek Kullanımlık Şifre	-	-
Kalıtım Faktörü	3	37,5	**Parmak İzi**	3	37,5
			Yüz Tarama	-	-
Sahiplik Faktörü	-	-	**Fiziksel Aygıt**	-	-

Ben parola kullanıyorum. (Ö1)

Parmak izi kullanıyorum. Direkt olarak parmağımı okutarak giriş yapabiliyorum. Şifreyi unutabiliyorum bazen. (Ö2)

Hiçbirini kullanmıyorum. Daha önce parmak izi kullanıyordum. (Ö3)

Parola kullanıyorum. Parmak izi özelliği var ancak çok kullanılabilir gelmiyor. Bazen zorlayıcı olabiliyor. Desen güvenilir gelmiyor çabucak öğrenilebilir. Bu yüzden parola kullanıyorum daha makul geliyor. (Ö4)

Parolayla giriş yapıyorum. Parmak izi bazen algılamıyor. (Ö5)

Basit olduğu için kullanım açısından parmak izini kullanıyorum. (Ö6)

Kullanmıyorum. Dışarda başıma bir şey geldiğinde telefonumu rahatça kullanabilsinler diye bir doğrulama koymadım. (Ö7)

Parmak izi kullanıyorum kullanım rahatlığından dolayı. (Ö8)

Tablo 20'de öğrencilerin sahip olduğu akıllı telefonlarının kilit ekranında kullandığı kimlik doğrulama şemaları verilmiştir. Parola ve parmak izi şeması katılımcılar tarafından %37,5 oranında kullanılmaktadır. Parola şeması geçmişten bugüne yaygın olarak kullanılan bir şema olmasına rağmen bu çalışmada, parmak izi şeması parola ile aynı yüzdeye sahip olmuştur. Katılım sağlayan iki öğrenci (Ö3, Ö7) herhangi bir kimlik doğrulama şeması kullanmadığını belirtmiştir.

4.1.9 "Bu Çalışmada Yer Almayan Ancak Kullanmak İstediğiniz Başka Bir Kimlik Doğrulama Şeması Var mı?" Sorusuna Yönelik Elde Edilen Yorumlar

Öğrenciler çalışmada yer almayan ancak kendilerinin önereceği kimlik doğrulama şemalarını belirtmişlerdir. Öneriler şöyledir:

Yok. Parmak izini kullanırdım. (Ö1)

Fikrim yok. Parmak izi iyi olurdu. (Ö2)

Yok. (Ö3)

Yok. Buradaki seçeneklerden en ideal olanının fiziksel aygıt çift doğrulama olduğunu düşünüyorum. (Ö4)

Benim üniversitemin uygulaması var. Bu uygulamaya öğrenci kimlik numaranız ve parolayla giriş yaptıktan sonra telefonun giriş yapan kişiye ait olup olmadığını kontrol eden bir sistem var. Yani benim telefonumda sisteme benim kimliğim gibi kayıtlı başka bir telefondan o uygulamaya kendi kimliğimle giremiyorum. (Ö5)

Yok bence şu anki öğrenci kimliği ve parola sistemi yeterli. (Ö6)

Ben yüz taramayla girerdim ehliyet sınavında da girmiştim gayet başarılı. (Ö7)

Yok. Üniversite sistemindeki gibi parola kullanımı iyi bence. (Ö8)

Ö5 öğrenim gördüğü üniversitede çevrim içi sınavlar için fiziksel aygıt şemasını kapsayan bir uygulama kullandıklarını belirtmiştir. Öğrenciler genel olarak şu anda kullandıkları parola kimlik doğrulama şemasının yeterli olduğunu ifade etmişlerdir. Öğrenciler diğer kimlik doğrulama şemalarının yeterli alt yapı sağlanmadığı ve yeterli cihaza sahip olunmaması durumunda bu sistemlere erişim sağlarken zorluklar yaşayacakları konusunda endişelere sahiptir.

BÖLÜM 5

5. TARTIŞMA, SONUÇ VE ÖNERİLER

Bu araştırmada, öğretim elemanlarının ve üniversite öğrencilerinin kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, gizlilik ve güvenlik bakımından değerlendirmeleri incelenmiştir. Çalışmanın bu bölümünde araştırma bulgularına dayalı olarak elde edilen sonuçlar tartışılmıştır. Elde edilen sonuçlara göre araştırma için önerilerde bulunulmuştur.

5.1. Tartışma ve Sonuç

Uzmanlardan elde edilen bulgulara göre öğrencilerin ilgi ve motivasyonları, bilgisayar okuryazarlık düzeyleri ve teknolojik altyapıları (internet, bilgisayar donanımı) uzaktan eğitimde önemli rol oynamaktadır. Uzaktan eğitimde öğretmen ve öğrenci birbirini tanımaz. Baturay ve Bay'ın (2009) sonucu da bu durumu desteklemektedir. Testlere ya da yazılı sınavlara göre sürecin değerlendirilmesinin sağlıklı bir şekilde gerçekleştirilemediği öğrenci görüşlerinden anlaşılmaktadır. Altan ve Seferoğlu (2009) uzaktan eğitimin sonucunda yapılan çerim içi sınav sonuçlarının etkili olabilmesi için geri bildirimin önemli olduğunu vurgulamaktadır.

Çevrim içi sınavlarda klasik sınav kalıplarına göre başarıyı etkileyen bazı unsurlar bulunmaktadır. Bunlar öğrencilerin çevrim içi sınava girerken her bireyin farklı ortamlarda bulunması ile ilgilidir. Xuet (2007) çalışmasında çevrim içi sınavlara erişim sağlamanın bilgisayar bilgisi ve tutumundan etkilenmediğini ancak bu erişimlerin bilgisayar hakkında fazla bilgisi olmayanların üstesinden gelebileceği basit bir şekilde hazırlanması gerektiğini vurgulamıştır. Uzaktan eğitimin değerlendirme sürecinde öğrenciler kopya çekebilmektedir. King ve arkadaşlarının (2009) bulguları, öğrencilerin çevrim içi eğitimde daha kolay kopya çektiklerini göstermektedir. Bu da sistemin eksikliklerinden biridir. Erişim sürecinde öğrenciler tarafından başvurulan hileler ölçme değerlendirmeyi de olumsuz etkilemektedir.

Öğrenciler çevrim içi sınav deneyimine sahip olduklarında çevrim içi sınavları tercih etmektedirler (Donovan, 2007). Süreci değerlendirmek için uzaktan eğitim forumları, çevrim içi sohbetler vb. sürece dahil edilmeli ve süreç boyunca aktif olunmalıdır. Öğrencilerin çevrim içi sınavlara erişimi, bu süreçte uygunsuz davranışların önlenmesi amacıyla basit ve anlaşılır olmalıdır.

Bilgiye dayalı kimlik doğrulama, şu anda çevrim içi hizmetlerde erişim sağlamak için en yaygın kullanılan kimlik doğrulama şemalarını içermektedir. Kullanıcıların parolalarını hatırlamakta güçlük çekmeleri ya da unutma gibi artan ezberleme gereksinimleri kullanıcılar için kullanılabilirlik sorunlarını ortaya çıkarmaktadır.

Yapılan araştırma ile elde edilen sonuçlar parolalar ve tek kullanımlık şifre gibi yaygın kullanılan kimlik doğrulama şemalarının, kimlik hırsızlığıyla mücadele etmek ya da güvenliği sağlamak için yeterli olmadığı yönündedir. Bu tür kimlik doğrulama şemalarının kolay bir şekilde unutulabilir, kaybolabilir, tahmin edilebilir, çalınabilir ve paylaşılabilir olduğu sonucuna ulaşılmıştır.

Kalıtım faktörüne bağlı kimlik doğrulama şemaları, bir kişinin farklı isimler altında birden fazla kimlik kartına sahip olup olmadığını tespit etme gibi avantajlar da sunmaktadır. Bu nedenle, biyometrik sistemler, kullanıcı kimlik doğrulaması gerektiren uygulamalara uygun şekilde entegre edildiğinde daha yüksek bir güvenlik sağlamaktadır. Kalıtım faktörüne bağlı kimlik doğrulama şemalarının güvenliği ve kullanıcıların depolanan biyometrik verilerinin gizliliğinin ihlal edilme durumları hakkında süregelen endişeler bulunmaktadır. Diğer tüm kullanıcı kimlik doğrulama şemalarında olduğu gibi, bir biyometrik sistemde doğru koşullar, zaman ve kaynak sağlandığında nitelikli bir hacker tarafından alt edilebilir. Bu tür kullanıcı endişelerini azaltmak, kullanıcı güvenini kazanmak biyometrik teknolojinin kabulünü kazanmak için büyük önem arz etmektedir.

Sonuçlar, kullanıcılar için yüksek bilişsel yük gibi dezavantajlarına rağmen parolanın en çok tercih edilen kimlik doğrulama şeması olduğunu göstermiştir. Öte yandan yüz tarama şeması güvenlik bakımından incelendiğinde daha yüksek puan almıştır. Katılımcıların yüz tarama ve parmak izi şemalarını güvenli bulmasının yanında kimlik doğrulama için parmak izlerini ifşa etme endişesi olduğu görülmüştür. Bu durum öğrenci gizliliği bakımından düşünülerek parola ve tek kullanımlık şifrenin tercih edilmesine yol açmıştır. Kullanılabilirlik, gizlilik ve güvenlik bakımından yüz tarama ve fiziksel aygıt en çok tercih edilen kimlik doğrulama şemaları olmuştur. Çalışmada kullanıcıların kullanılabilirlik özelliklerine daha fazla önem vermeleri ve güvenmelerinin bir nedeni, güvenlik ve gizlilik özelliklerinin genellikle kullanıcı tarafından görülmemesi ve sistemden beklenmesi olduğu sonucuna ulaşılmıştır. Bu, özellikle sistem ve arayüz tasarımı düzeyinde geçerlidir.

5.2. Öneriler

Bu bölümde; elde edilen bulgulara göre, kimlik doğrulama şemalarının kullanımına yönelik öğretim elemanlarına, üniversite öğrencilerine ve araştırmacılara öneriler verilmiştir.

Araştırmada yer alan kimlik doğrulama şemaları uygulamaya konulmadan önce üniversite ortamında hizmet içi eğitim, seminer gibi farklı yollarla öğrencilere tanıtılabilir. Bu konuda öğrencilere danışmanlık hizmeti verilebilir. Danışmanlık hizmetleri ayrıca öğrenciler hakkında detaylı bilgi toplanmasına yardımcı olacak, bu da sistemin daha iyi işlemesine, öngörülebilmesine ve eksikliklerin önceden tamamlanmasına yardımcı olacaktır.

Biyometrik faktöre bağlı kimlik doğrulama şemaları ile ilgili gizlilik endişesinin en aza indirilmesi konusunda öğretim elemanı ve üniversite öğrencilerine bu tür biyometrik tabanlı sistemler hakkında danışmanlık hizmeti verilebilir.

Beş kimlik doğrulama şemasının (parola, tek kullanımlık şifre, parmak izi, yüz tarama, fiziksel aygıt) ölçme değerlendirme sürecinde kullanılması ile ilgili kullanılabilirlik, gizlilik ve güvenliği hakkında örnek öğretim ve değerlendirme videoları hazırlanabilir ve kılavuz kitaplar ile birlikte dağıtılabilir.

Kullanıcıların biyometrik faktöre bağlı kimlik doğrulama şemalarını benimseyebilmeleri için güvenirlik kazanılabilir ve sistemlere entegre edilerek denemelerde bulunulabilir. Bunun sonucunda çevrim içi sınavların, sınava girecek öğrenci tarafından gerçekleşmesiyle ölçme değerlendirme sonuçlarının güvenirliği artırılabilir. Çalışmada yer alan biyometrik faktöre bağlı parmak izi kimlik doğrulama şemasının kullanılabilirliği ile ilgili sorunlar, oluşturulacak demo sistemler ile öğrenci görüşleri alınarak ihtiyaçların belirlenmesini ve sistemin iyileştirilmesini sağlayabilir.

Kimlik doğrulama şemalarının özelliklerini, kullanılabilirlik, gizlilik ve güvenlik düzeylerini daha detaylı incelemek amacıyla bu şemaları kullanıcıların deneyebileceği laboratuvar ortamında gerçekleştirilecek bir nitel araştırma yapılabilir.

KAYNAKLAR

Agulla, E. G., Alba-Castro, J. L., Anido-Rifón, L. E., & García-Mateo, C. (2008). Is my student at the other side? Applying Biometric Web Authentication to elearning environments. *Eighth IEEE International Conference on Advanced Learning Technologies* (s. 551-553). Vigo: IEEE.

Agulla, E. G., Rifón, L. A., Castro, J. A., & Mateo, C. G. (2008). Eighth IEEE International Conference on Advanced Learning Technologies. *Is my student at the other side? Applying Biometric Web Authentication to elearning environments* (s. 551-553). Galicia: IEEE.

AL-Harby, F., Qahwaji, R., & Kamala, M. (2010). Users' Acceptance of Secure Biometrics Authentication. *Networked Digital Technologies* (s. 254-258). içinde Springer.

Alkan, C. (1997). *Eğitim Teknolojisi.* Ankara: Anı Yayıncılık.

Alotaibi, S. J. (2010). Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment. *The 4th Saudi International Conference.* Southampton: The 4th Saudi International Conference.

Altan, T., & Seferoğlu, S. (2009). UZAKTAN EĞİTİMDE DEĞERLENDİRME SÜRECİ: ÖĞRENCİ GÖRÜŞLERİNİN SİSTEMİN GELİŞİMİNE KATKILARI. *3rd COMPUTER & INSTRUCTIONAL INTERNATIONAL TECHNOLOGIES SYMPOSIUM 07-09 October 2009* (s. 861-865). Trabzon: Karadeniz Technical University Press.

Aras Bozkurt, H. U. (2018). E-Süreçlerinde Kimlik Doğrulama Yöntemlerine İlişkin Öğrenen Görüşlerinin İncelenmesi . *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 745-755.

Bailie, J. L. (2009). Online Learner Authentication: Verifying the Identity of Online Users. *MERLOT Journal of Online Learning and Teaching*, 197-207.

Brandom, R. (2017, Temmuz 10). *Two-factor authentication is a mess*. The Verge: https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess adresinden alındı

Butler, W. (2020). *Learning the language of cybersecurity*. Capitol Technology University Blog: https://www.captechu.edu/blog/learning-language-of-cybersecurity adresinden alındı

Charles, A., Adebiyi, A. A., & Ekong, U. (2007). The prospects of E-examination implementation in Nigeria. *Turkish Online Journal of Distance Education* (s. 125-134). Ota: Turkish Online Journal of Distance Education.

Chellappan, S., & Asha, S. (2008). Authentication of e-learners using multimodal biometric technology. *In 2008 International Symposium on Biometrics and Security Technologies* (s. 1-6). Isalambad: IEEE.

Das, M. L. (2015). Privacy and Security Challenges in Internet of Things. *Distributed Computing and Internet Technology* (s. 33-48). Gandhinagar: Springer International Publishing Switzerland.

DHA. (2018, Aralık 5). *T24 Gündem*. T24: https://t24.com.tr/haber/mahkeme-karari-verdi-yuz-tanima-sistemiyle-mesai-kontrolu-hukuka-uygun-degil,764405 adresinden alındı

Donovan, J. (2007). Online vs. Traditional Course Evaluation Formats: Student Perceptions. C. Mader , & J. Shinsky içinde, *Journal of Interactive Online Learning* (s. 158-180). Gary: JIOL.

Erkılıç, O. (2022, Aralık 25). *Türkiye Haberleri*. Cumhuriyet TV: cumhuriyet.com.tr/turkiye/hukuk-fakultesi-ogrencilerine-parmak-izi-uygulamasi-tepkilere-neden-oldu-2015323 adresinden alındı

Fernandez, A., Insfran, E., & Abrahão, S. (2011). Usability evaluation methods for the web: A systematic mapping study. G. Ruhe içinde, *Information and Software Technology* (s. 789-817). Valencia: Elsevier.

Flior, E., & Kowalski, K. (2010). Continuous Biometric User Authentication in Online Examinations. *In 2010 seventh International Conference on information technology: new generations* (s. 488-492). Las Vegas: IEEE.

İskenderoğlu, M., İskenderoğlu, T., & Palancı, M. (2012). Opinion of teaching staff in distance education systems, regarding the assessment and evaluation process . *Procedia - Social and Behavioral Sciences* (s. 4661-4665). Trabzon: Elsevier.

Karal, H., Çebi, A., & Pekşen, M. (2010). Student opinions about the period of measurement and evaluation in distance education: the difficulties. *Procedia Social and Behavioral Sciences 9 (2010)* (s. 1597-1601). Trabzon: WCLTA.

Katsini, C., Belk, M., Fidas, C., Avouris, N., & Samaras, G. (2016). Security and Usability in Knowledge-based User Authentication: A Review. *Proceedings of the 20th Pan-Hellenic Conference on Informatics* (s. 1-6). Patras Greece: Association for Computing Machinery.

Kaya, Z. (2002). *Uzaktan Eğitim.* Ankara: Pegem.

Kimery, A. (2018, Haziran 3). Customs and Border Protection (CBP). *CBP plans to expand biometric entry/exit program to include vehicles*.

Kör, H., Çataloğlu, E., & Erbay, H. (2012). Uzaktan ve Örgün Eğitimin Öğrenci Başarısı Üzerine Etkisinin Araştırılması. *Gaziantep University Journal of Social Sciences*, 267-279.

Levy, Y., & Ramim, M. M. (2007). A Theoretical Approach for Biometrics Authentication of e-Exams. *Nova Southeastern University, USA* (s. 93-101). Fort Lauderdale: Nova Southeastern University.

Luminita, D. C. (2011). Information Security in E-learning Platforms. *3rd World Conference on Educational Sciences-2011* (s. 2689-2693). Istanbul, Turkey: Procedia.

Mayron, L., Hausawi, Y., & Bahr, G. S. (2013). Secure, Usable Biometric Authentication Systems. *International Conference on Universal Access in Human-Computer Interaction* (s. 195-204). Las Vegas: Springer.

Menkus, B. (1988). Understanding the Use of Passwords. *Computers & Security*, 132-136.

Moini, A., & Madni, A. M. (2009). Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. A. G. Aghdam içinde, *IEEE Systems Journal, 3(4)* (s. 469-476). Los Angeles: IEEE Systems Council.

Moody, J. (2004). Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use. *IIssues in Informing Science and Information Technology (IISIT)*, (s. 753-762).

Nalini K. Ratha, J. H. (2001). Enhancing securityand privacy in biometrics-based authentication systems. *IBM Systems Journal*, 614-634.

Necmettin Erbakan Üniversitesi. (2023, Ocak 08). *Öğrenci Bilgi Sistemi*. Necmettin Erbakan Üniversitesi Öğrenci Bilgi Sistemi: https://obs.erbakan.edu.tr/oibs/ogrenci/login.aspx adresinden alındı

Necmettin Erbakan Üniversitesi. (2023, Ocak 8). *Tek Şifre | Necmettin Erbakan Üniversitesi*. Necmettin Erbakan Üniversitesi: https://teksifre.erbakan.edu.tr/cep-no-onay adresinden alındı

Ramu, T., & Arivoli, D. T. (2013). A framework of secure biometric based online exam authentication: an alternative to traditional exam. *International Journal of Scientific & Engineering Research* (s. 52-60). Krishnankoil: International Journal of Scientific & Engineering Research.

Roffe, I. (2004). *Innovation and e-learning: E-business for an educational enterprise.* Cardiff, UK: University of Wales Press.

Rolfe, A. (2019, Haziran 27). *Strong Customer Authentication: What matters most to online shoppers – security or convenience?* Payments Industry Intelligence: https://www.paymentscardsandmobile.com/strong-customer-authentication-what-matters-most-to-online-shoppers/ adresinden alındı

Schechter, S., Brush, A. J., & Egelman, S. (2009). It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions. *2009 30th IEEE Symposium on Security and Privacy* (s. 375-390). Oakland: IEEE Computer Society Technical Committee on Security and Privacy.

Shelton, K., & Salstman, G. (2005). *An Administrator's Guide to Online Education.* Greeen-wich: Information Age Publishing.

Smeureanu, I., & Isaila, N. (2008). The knowledge transfer through E-learning in business environment.

Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)* (s. 1-14). Newcastle: ACM.

Tarhan Mengi, B. (2013). Sağlık Hizmetlerinde Meydana Gelebilecek Hileleri Önlemeye Yönelik Bir Uygulama Olarak Biyometrik Kimlik Doğrulama Sistemlerinin Kullanımı. *Muhasebe ve Finansman Dergisi / The Journal of Accounting and Finance* (s. 39-50). İstanbul: Muhasebe ve Finansman Öğretim Üyeleri Bilim ve Araştırma Derneği.

Thanganayagam , R., & Arivoli, T. (2013). A framework of secure biometric based online exam authentication: an alternative to traditional exam. *International Journal of Scientific and Engineering Research, Volume 4, Issue 11,* (s. 52-60). Madurai: IJSER.

Ullah, A., Xiao, H., & Lilley, M. (2012). Profile Based Student Authentication in Online Examination. *International Conference on Information Society (i-Society 2012)* (s. 109-113). Hatfield: IEEE.

Uşun, S. (2006). *Uzaktan Eğitim.* Ankara: Nobel.

Wang, V. X. (2008). *Encyclopedia of Information Technology Curriculum Integration.* California, USA: Lawrence A. Tomei.

Yükseköğretim Kanunu. (2018, Şubat 22). *https://www.mevzuat.gov.tr/MevzuatMetin/*. https://www.mevzuat.gov.tr/MevzuatMetin/: https://webcache.googleusercontent.com/search?q=cache:z_xPPwQh7ZEJ:https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2547.doc&cd=4&hl=en&ct=clnk&gl=tr adresinden alındı

Zhao, Q., & Ye, M. (2010). The Application and Implementation of Face Recognition in Authentication System. *2010 International Conference on Networking and Digital Society* (s. 487-489). Wenzhou, China: IEEE Xplore.

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. D. P. Brumby içinde, *International Journal of Human-Computer Studies* (s. 22-44). Darmstadt: Elsevier.

Zoom Video Communications. (2022, Ekim 24). *Managing two-factor authentication (2FA).* Zoom Support: https://support.zoom.us/hc/en-us/articles/360038247071-Managing-two-factor-authentication-2FA- adresinden alındı

EKLER

EK-1: Veri Toplama Aracı

EK-2: Necmettin Erbakan Üniversitesi Etik Kurul Kararı

EK-3: Tez Başlık Değişikliği Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü Yönetim Kurulu Kararı

EK-1: Veri Toplama Aracı

Değerli Katılımcı;

Bu görüşme formu "Çevrim İçi Sınavlarda Uygulanabilecek Kimlik Doğrulama Şemalarına İlişkin Öğretim Elemanı ve Üniversite Öğrencilerinin Görüşlerinin İncelenmesi" konulu yüksek lisans tezi kapsamında, çevrim içi sınavlarda uygulanabilecek kimlik doğrulama şemalarına ilişkin öğretim elemanı ve üniversite öğrencilerinin görüşlerini belirlemek ve analiz etmek için tasarlanmıştır. Çalışmaya katılımınız gönüllülük esasına dayanmaktadır. Bu görüşme formu kapsamında vereceğiniz yanıtlar gizli tutulacak ve elde edilen sonuçlar sadece akademik çalışma amacı ile kullanılacaktır. Aşağıda sıralanan her bir maddeyi dikkatlice okuyarak objektif cevaplamanız çalışmanın amacına ulaşması bakımından büyük bir önem taşımaktadır.

Katkılarınız için teşekkür ederim.

Canan BATTAL
Merkez/KÜTAHYA

I. BÖLÜM (Öğretim Elemanlarına Uygulanacak Görüşme Formu)

Bu bölümdeki soruları sözlü olarak cevaplayınız.

1. Cinsiyetiniz?

2. Görev yaptığınız üniversite?

3. Bölümünüz?

4. Akademik unvanınız?

II. BÖLÜM (Öğretim Elemanlarına Uygulanacak Görüşme Formu)

Bu bölümdeki soruları sözlü olarak cevaplayınız.

S1. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından öğrenci gizliliğini sağlayabilecek en uygun şema hangisidir? Neden?

S2. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından sistem güvenliği için en uygun şema hangisidir? Neden?

S3. Size göre, ölçme değerlendirme süreci için kullanılan kimlik doğrulama şemalarından kullanılabilirliği (kullanımı) en yüksek olan şema hangisidir? Neden?

S4. Ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, en uygun bulduğunuz, beğendiğiniz kimlik doğrulama şemasını belirtiniz ve 10 puan üzerinden puanlayınız. (1 puan en düşük, 10 puan en yüksek değer anlamına gelmektedir.)

S5. Ölçme değerlendirme sürecinde kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, uygun olmadığını düşündüğünüz, beğenmediğiniz kimlik doğrulama şemasını belirtiniz.

S6. Size göre, öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurmalarını en çok kolaylaştırabilecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S7. Size göre, öğrencilerin çevrim içi sınavlara erişim sürecinde hileye başvurma eylemini en az seviyeye indirecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S8. Şu an sahip olduğunuz akıllı telefonunuzun kilit ekranında, hangi kimlik doğrulama şemasını kullanıyorsunuz? Nedenini açıklayınız.

S9. Bu çalışmada yer almayan ancak kullanmak istediğiniz başka bir kimlik doğrulama şeması var mı? Varsa belirtiniz ve tercih etme nedeninizi kısaca açıklayınız.

I. BÖLÜM (Üniversite Öğrencilerine Uygulanacak Görüşme Formu)

Bu bölümdeki soruları sözlü olarak cevaplayınız.

1. Cinsiyetiniz?

2. Öğrenim gördüğünüz üniversite?

3. Bölümünüz?

4. Sınıfınız?

II. BÖLÜM (Üniversite Öğrencilerine Uygulanacak Görüşme Formu)

Bu bölümdeki soruları sözlü olarak cevaplayınız.

S1. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından öğrenci gizliliğini sağlayabilecek en uygun şema hangisidir? Neden?

S2. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından sistem güvenliği için en uygun şema hangisidir? Neden?

S3. Size göre, çevrim içi sınavlara erişim sağlamak için kullanılan kimlik doğrulama şemalarından kullanılabilirliği (kullanımı) en yüksek olan şema hangisidir? Neden?

S4. Çevrim içi sınavlarda kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, en uygun bulduğunuz, beğendiğiniz kimlik doğrulama şemasını belirtiniz ve 10 puan üzerinden puanlayınız. (1 puan en düşük, 10 puan en yüksek değer anlamına gelmektedir.)

S5. Çevrim içi sınavlarda kullanılacak kimlik doğrulama şemalarını bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirerek, uygun olmadığını düşündüğünüz, beğenmediğiniz kimlik doğrulama şemasını belirtiniz.

S6. Size göre, çevrim içi sınavlara erişim sürecinde hileye başvurulmasını kolaylaştıracak kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S7. Size göre, çevrim içi sınavlara erişim sürecinde hileye başvurma eylemini en az seviyeye indirecek kimlik doğrulama şeması hangisidir? Nedenini kısaca açıklayınız.

S8. Şu an sahip olduğunuz akıllı telefonunuzun kilit ekranında, hangi kimlik doğrulama şemasını kullanıyorsunuz? Nedenini açıklayınız.

S9. Bu çalışmada yer almayan ancak kullanmak istediğiniz başka bir kimlik doğrulama şeması var mı? Varsa belirtiniz ve tercih etme nedeninizi kısaca açıklayınız.

EK-2: Necmettin Erbakan Üniversitesi Etik Kurul Kararı

NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER BİLİMSEL ARAŞTIRMALAR ETİK KURULU BAŞKANLIĞI
ETİK KURUL KARARI

Etik Kurul Toplantı Tarihi/Sayısı ve Karar No	**Tarih :09/07/2021** **Toplantı Sayısı :07** **Karar No :2021/407**
Araştırmanın Başlığı	Çevrim İçi Sınavlarda Uygulanabilecek Kimlik Doğrulama Şemalarına İlişkin Öğretim Elemanı ve Üniversite Öğrencilerinin Görüşlerinin Değerlendirilmesi
Sorumlu Araştırmacı	Doç. Dr. Şemseddin GÜNDÜZ
Yardımcı Araştırmacılar	Yüksek Lisans Öğrencisi Canan YAZICI
Etik Kurul Kararı	Başvurunuz değerlendirilmiş olup araştırmanız Etik Kurul tarafından uygun görülmüştür.
Uygun Değil ise gerekçeleri	

ASLI GİBİDİR
16/07/2021

Doç. Dr. Ahmet KURNAZ
Etik Kurul Başkanı

EK-3: Tez Başlık Değişikliği Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü Yönetim Kurulu Kararı

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Sayı : E-71052239-050-346032 25.05.2023
Konu : Tez Başlık Değişikliği (Canan BATTAL)

DAĞITIM YERLERİNE

Estitümüz yönetim kurulu karar sureti aşağıda çıkarılmıştır.
Bilgilerinizi ve gereğini rica ederim.

TARİH	**23.05.2023**
TOPLANTI	**27**
KARAR NO	**11**
KONU	**Tez Başlık Değişikliği (Canan BATTAL)**
KARAR	
Enstitümüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı Tezli Yüksek Lisans Programı **19830501130** numaralı öğrencisi **Canan BATTAL** ile ilgili Bilim Dalı Başkanlığının 22.05.2023 tarih ve E.344836 sayılı yazısı ile ekleri görüşüldü. Adı geçen öğrencinin **Tez savunma jüri önerisiyle tez başlık değişikliğinin aşağıdaki tabloya göre değiştirilmesine**, kararın öğrenciye, danışmanına ve Bilim Dalı Başkanlığına bildirilmesine oy birliği ile karar verildi.	
Eski Tez Adı	Çevrim İçi Sınavlarda Uygulanabilecek Kimlik Doğrulama Şemalarına İlişkin Öğretim Elemanı ve Üniversite Öğrencilerinin Görüşlerinin Değerlendirilmesi
Yeni Tez Adı	Çevrim İçi Sınavlarda Uygulanabilecek Kimlik Doğrulama Şemalarına İlişkin Öğretim Elemanı ve Üniversite Öğrencilerinin Görüşlerinin İncelenmesi
Yeni İngilizce Adı	Analyzing of the Opinions of Instructors and University Students in Regards to Authentication Schemes that can be Applied in Online Exams
Danışmanı	Doç.Dr. Şemseddin GÜNDÜZ

Prof.Dr. Bünyamin AYDIN
Enstitü Müdürü

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Kodu : 8098-BZD0-07L2 Belge Doğrulama Adresi : https://ebyssorgu.erbakan.edu.tr

Adres: AKEF Eğitim Bilimleri Enstitüsü A1 BLOK NO:146 MERAM/KONYA
Telefon No : 0332 324 76 60 Fax No : 0332 324 55 10
e-Posta : İnternet Adresi : http://www.erbakan.edu.tr
Bilgi İçin :Hasan Hüseyin UZAR
Mühendis
Telefon No:0332 324 76 60

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Dağıtım:
Eğt. Bil. Enst. Bilgisayar ve Öğretim Teknolojileri Bilim Dalına
Sayın Doç. Dr. Şemseddin GÜNDÜZ

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu : 8098-BZD0-07L2 Belge Doğrulama Adresi : https://ebyssorgu.erbakan.edu.tr

Adres: AKEF Eğitim Bilimleri Enstitüsü A1 BLOK NO:146 MERAM/KONYA
Telefon No : 0332 324 76 60
Fax No : 0332 324 55 10
e-Posta :
İnternet Adresi : http://www.erbakan.edu.tr
Bilgi İçin :Hasan Hüseyin UZAR
Mühendis
Telefon No:0332 324 76 60