Necmettin Erbakan Üniversitesi
Ahmet Keleşoğlu Eğitim Fakültesi Dergisi (AKEF)
Journal of Ahmet Keleşoğlu Education Faculty
E-ISSN 2687-1750

Cilt: 2 Sayı:1 Yıl: 2020 Araştırma Makelesi / Research Article

Kimlik Doğrulama Şemalarının Üniversite Öğrencileri Tarafından Tercih Edilme Durumlarının İncelenmesi

Şemseddin Gündüz[1] **Canan Yazıcı**[2]

[1] Necmettin Erbakan Üniversitesi, Ahmet Keleşoğlu Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Meram, Konya, Türkiye, semsedding@gmail.com *(Sorumlu Yazar/Corresponding Author)*

[2] Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Meram, Konya, Türkiye, cananyazici5561@gmail.com

Makale Bilgileri

Makale Geçmişi

Geliş: 31.01.2020
Kabul: 20.04.2020
Yayın: 28.06.2020

Anahtar Kelimeler:
Kimlik Doğrulama,
Şemaları,
Kullanılabilirlik,
Parola,
Parmak izi,
Gizlilik,
Güvenlik.

ÖZ

Bireylerin bilgi güvenliğini sağlayarak, çeşitli cihazlara ya da platformlara erişimlerine olanak sağlayan farklı kimlik doğrulama şemaları geliştirilmiştir. Kullanıcıların yüksek bilişsel yük gibi sorunlarını azaltmak ve veri güvenliğini sağlamak amacıyla geliştirilen bu kimlik doğrulama şemaları arasından en yaygın kullanılan dokuz farklı şema belirlenerek araştırmaya dahil edilmiştir. Bu araştırmanın amacı, bireylerin günlük hayatlarında farklı platformlara erişim sağlarken kullanmak istedikleri kimlik doğrulama şemalarını belirlemektir. Araştırma 2019 yılı aralık ayında Konya'da 188 üniversite öğrencisi ile yürütülmüştür. Birinci aşamada katılımcılara on altı platform (sosyal medya, internet bankacılığı, kütüphaneler, vb.) sunularak, bu ortamlara girişlerde hangi kimlik doğrulama şemalarını (parola, parmak izi, fiziksel aygıt, vb.) tercih ettiklerini işaretlemeleri istenmiştir. İkinci aşamada kullanıcılar bilgi güvenliğinin üç unsuru olan kullanılabilirlik, gizlilik ve güvenlik açısından uygun ve uygun olmayan kimlik doğrulama şema tercihlerini belirtmişlerdir. Katılımcılar %52 oranında bilgi faktörünü (parola, PIN, vb.), %34 oranında kalıtım faktörünü (parmak izi, retina taraması, vb.) ve %13 oranında sahiplik faktörünü (fiziksel aygıt) tercih etmişlerdir. Bilgi faktörünü tercih eden kullanıcıların üçte ikisi parola şemasını tercih etmiştir. Kullanıcıların değerlendirmeleri sonucunda parmak izi doğrulama şeması; kullanılabilirlik, gizlilik ve güvenlik bakımından en yüksek tercih edilme oranına sahipken, fiziksel aygıt doğrulama şeması en düşük tercih edilme oranına sahip olmuştur. Kullanıcıların platformlara erişim sağlamaları için tercih ettikleri şemaların, günümüzde kullanıcıların çoğu tarafından bilinen ve yaygın olarak kullanılan şemalar ile aynı olduğu gözlemlenmiştir. Yapılan bu çalışmada kullanıcılar tarafından en çok parola ve parmak izi şeması tercih edilmiştir. Bu şemaların tercih edilme nedenlerinin bilinmesi için, konu hakkında nitel araştırmalar yapılabilir.

Investigation of Preference Status of Authentication Schemes of University Students

Article Info

Article History

Received: 31.01.2020
Accepted: 20.04.2020
Published: 28.06.2020

Keywords:
Authentication schemes,
Usability,
Password,
Finger print,
Privacy,
Security.

ABSTRACT

The Various authentication systems have been developed that enable individuals to access information and platforms by providing information security. Among these developed authentication schemes, the nine most common schemes used were determined and included in the study. The purpose of this research is to identify the authentication schemes that individuals prefer to access different platforms in their daily lives. The research was carried out with 188 university students in Konya in December 2019. In the first stage, participants were presented with sixteen platforms (social media, internet banking, libraries, etc.) and asked to indicate which authentication schemes (password, fingerprint, physical device, etc.) they preferred in entering these environments. In the second stage, users have specified the appropriate and ineligible authentication scheme preferences in terms of usability, privacy and security, which are the three elements of information security. The participants preferred 52% information factor (password, PIN, etc.), 34% inheritance factor (fingerprint, retina scan, etc.) and 13% ownership factor (physical device). Two-thirds of the users who prefer the information factor preferred the password scheme. Fingerprint verification scheme as a result of users' reviews; The physical device verification scheme had the lowest preferred rate, while it had the highest preferred rate in terms of availability, privacy and security. It has been observed that the schemes that users prefer to access the platforms are the same schemes that are known and widely used by most users today. In this study, the most preferred password and fingerprint scheme were preferred by the users. Qualitative research can be done on the subject in order to know the reasons why these schemes are preferred.

Atıf/Citation: Gündüz, Ş. ve Yazıcı, C. (2020). Kimlik doğrulama şemalarının üniversite öğrencileri tarafından tercih edilme durumlarının incelenmesi, *Ahmet Keleşoğlu Eğitim Fakültesi Dergisi*, *2*(1), 1-11.

GİRİŞ

Teknoloji, hayatı daha kolay, daha erişilebilir ve daha güvenli bir biçime dönüştürerek, insanlara konforlu bir yaşam sunmaktadır. Günümüzde geliştirilen teknolojik aygıtlar, yalnızca insanların birbiri ile iletişime geçmelerini sağlayan araçlar olarak değil, aynı zamanda diğer akıllı cihazlarla ve ortamlarla da etkileşime girmemize olanak sağlayan araçlardır. Akıllı cihaz kullanımının yaygınlaşmasıyla birlikte, aygıtların birbiri ile iletişime geçmesini sağlayacak yöntemlere duyulan ihtiyaçlar da gün geçtikçe artmaktadır. Bu ihtiyaçların karşılanması amacıyla 1991 yılında Cambridge Üniversitesi'ndeki yaklaşık 15 akademisyenin kahve makinesini görebilmek için kurduğu kameralı sistem o günün koşullarında değerlendirildiğinde olağanüstü bir uygulama olarak görülmüştür (Stafford, 1995). Çalışmadaki sistem çevrimiçi olması nedeniyle "nesnelerin interneti" kavramının ilk örneği olarak görülmektedir. İnterneti kullanarak diğer cihazların birbiri ile iletişime geçmesini sağlayan nesnelerin interneti, her şekil ve büyüklükteki cihazların diğer cihazlarla iletişim kurmasını, etkileşime girmesini ve veri alışverişi yapmasını sağlayan bir teknoloji olarak tanımlanabilmektedir (Bandyopadhyay, 2011).

Farklı cihazların birbiri ile iletişim kurması, etkileşime girmesi ve veri alışverişinde bulunması, bilgi güvenliğinin üç unsuru olan gizlilik, güvenlik ve kullanılabilirlik açısından çeşitli ihtiyaçlar ortaya çıkarmıştır (McCumber, 1991). Kullanıcıların bilgi güvenliğini sağlayarak, çeşitli cihazlara ya da platformlara erişimlerine izin veren, onların kişisel verilerini ya da diğer önemli verileri üçüncü şahısların yetkisiz erişimlerinden koruyan bazı kimlik doğrulama sistemleri geliştirilmiştir. Bu sistemler kullanıcılara, kişisel verilerine ya da kişisel cihazlarına erişim sağlamaları için birçok kimlik doğrulama giriş seçeneği sunmaktadırlar. Alanyazında kimlik doğrulama giriş seçenekleri; bilgi, kalıtımsal özellikler (Parmak izi, retina tarama gibi), bulunduğu konum, içinde bulunduğu zaman ve sahiplik olmak üzere beş kategoride sınıflandırılmıştır (Kayrancıoğlu, 2019).

Günümüzde yaygın olarak kullanılan bilgi faktörü; kullanıcıların sahip olduğu bilgilerden oluşan parola, gizli soru, tek kullanımlık şifre ve PIN gibi kimlik doğrulama şemalarını içermektedir (Kayrancıoğlu, 2019). Kalıtım faktörü, kişiye özel fiziksel özellik verilerini kapsayan; parmak izi, retina taraması, yüz tanıma ve avuç içi gibi kimlik doğrulama şemalarını içermektedir (Riley, 2009). Sahiplik faktörü ise; kullanıcıların sisteme erişim sağlarken kimlik doğrulama amacıyla kullandıkları fiziksel aygıtlar olarak açıklanabilir. Diğer faktörler ile birlikte kullanılan konum ve zaman faktörleri ise, kullanıcıların sisteme yalnızca belirli konumlardan erişebilmelerine ve birbirleri ile uyumlu zaman dilimine izin vermektedir (Mannan ve Van Oorschot, 2011).

Kullanılan bu faktörlerin bilgi güvenliği için önemli olduğu düşünülmektedir. Son yıllarda kredi kartı dolandırıcılığı ve kimlik hırsızlığı konusundaki artış, toplum tarafından da büyük endişelere neden olmaktadır (Chan ve ark. 1999). Kullanılan kimlik doğrulama şemalarını içeren kimlik doğrulama faktörleri, güvenliği artırarak, olabilecek siber saldırıları azaltmayı ve veri kaybını en düşük seviyeye düşürmeyi amaçlamaktadır.

Kimlik doğrulama, verileri üçüncü şahısların yetkisiz erişimlerinden korumak amacı ile geliştirilen önemli bir sistemdir. Özellikle e-posta hizmetleri, sosyal medya ve çevrimiçi alışveriş siteleri gibi bilgisayar ve web uygulamaları için alfasayısal şifre, en yaygın kimlik doğrulama şeması olarak kullanılmaktadır (Zimmermann ve Gerberb, 2019). Ancak güvenlik sorunları ve her hesap için farklı bir parola ezberleme ihtiyacı bakımından şifre kullanımında, yüksek bilişsel yük gibi birçok sorun görülmektedir. Birçok kullanıcı yüksek efor gerektiren şemalardan kaçınmak için kolayca tahmin edilebilecek basit parola seçme, farklı hesaplarda şifreleri tekrar kullanma ya da şifreleri güvenli olmayan yerlerde saklama eğilimine sahiptirler (Huang ve ark., 2011).

Alanyazında görülen güvenlik ve gizlilik sorunlarına karşı kimlik doğrulama şemalarının teknik yönlerini karşılaştırmak ve şemaları geliştirmek için birçok araştırma yapılmıştır. Bonneau, Herley, Van Oorschot, ve Stajano (2012) yaptıkları çalışmada güvenlik, konuşlandırılabilirlik ve kullanılabilirlik özellikleri açısından çok sayıda kimlik doğrulama şemasını birbirleriyle karşılaştırarak, gelecekteki web kimlik doğrulama şemaları hakkında bir değerlendirme taslağı oluşturmuşlardır. Özkaya (2014), biyometrik tabanlı kimlik doğrulama sistemlerinde meydana gelen güvenlik açıklarını gözden geçirip, bunların üstünlük ve sınırlılıklarını incelemiştir. Mengi (2013) kişinin fiziksel özelliklerine göre kimlik doğrulamasını sağlayan biyometrik (kalıtımsal) sistemlerin, önemli verilere üçüncü şahısların ya da kurumların erişimini kısıtlandırarak siber saldırıların mümkün olduğunca azaltılmasını ve verilerin korunmasını sağlayan üst düzey sistemler olduğunu savunmuştur. Mannan ve Oorscho (2008) daha güçlü parola kimlik doğrulaması için kişisel aygıtlardan yararlanmaya yönelik bir çalışma yürütmüştür. Bu çalışmalarda araştırmacılar, var olan kimlik doğrulama şemalarının üstünlük ve sınırlılıklarını güvenlik ve gizlilik bakımından incelemişlerdir.

Bu araştırmanın amacı, kullanıcıların fiziksel platformlarda ve sanal ortamlarda tercih ettikleri kimlik doğrulama şemalarını belirlemektir. Bu kapsamda aşağıdaki araştırma sorularına yanıt aranmıştır.

• Farklı siber ortamlarda ve platformlarda hangi doğrulama şemaları tercih edilmektedir?

• Bilgi güvenliğinin üç unsuru olan kullanılabilirlik, güvenlik ve gizlilik bakımından, kullanıcılar için en uygun seçilen kimlik doğrulama şeması hangisidir?

• Bilgi güvenliğinin üç unsuru olan kullanılabilirlik, güvenlik ve gizlilik bakımından en az tercih edilen kimlik doğrulama şeması hangisidir?

YÖNTEM

Bu araştırma tarama modelinde tasarlanmıştır. Bu modelde varolan durum olduğu gibi betimlenmeye çalışılmaktadır. Karasar (2002), tarama modellerini, geçmişte ya da halen var olan bir durumu olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımları olarak tanımlamıştır. Araştırmaya konu olan birey, konu ya da nesne, kendi koşulları içinde, var olduğu şekliyle tanımlanmaya çalışılır.

Örneklem

Araştırmanın evrenini Necmettin Erbakan Üniversitesi Ahmet Keleşoğlu Eğitim Fakültesi'nde öğrenim görmekte olan kullanıcılar oluşturmaktadır. Araştırmanın örneklemini ise aynı fakültede öğrenim gören rastgele seçilmiş 126 kadın, 62 erkek olmak üzere toplamda 188 kullanıcı oluşturmaktadır.

Katılımcıların yaklaşık üçte ikisi Anadolu Lisesi mezunudur. Araştırmaya katılan kullanıcıların akademik başarıları üç kategoride toplanmıştır. Katılımcıların %63.8'i orta seviye akademik başarıya sahiptir. Araştırmaya katılan kullanıcıların tamamı eğitim fakültesinde öğrenim görmektedirler.

Veri Toplama Araçları

Çalışmada veri toplama aracı, araştırmacılar tarafından geliştirilmiştir. Veri toplama aracı üç bölümden oluşmaktadır. Birinci bölümde kamusal alan ve özel alan başlıkları altında toplam 16 maddeden oluşan farklı platformlar yer almaktadır. Bu platformlar sosyal medya, internet bankacılığı, e-posta hizmetleri, alışveriş siteleri, GSM operatörleri mobil uygulamaları, PC (bilgisayar, tablet), sağlık kurumlarına giriş, spor salonlarına giriş, konaklama (ev, özel yurt, vb.), e-devlet, ÖSYM (Ölçme Seçme ve Yerleştirme Merkezi), OBS (Öğrenci Bilgi Sistemi), e-sağlık hizmetleri, kampüs

girişi, konaklama (devlet yurdu) ve kütüphane işlemlerinin olduğu maddelerdir. Kullanıcılardan bu platformlara giriş yaparken kullanmak istedikleri kimlik doğrulama şemasını belirtmeleri istenmiştir. Bu kimlik doğrulama şemaları ise dokuz maddeden oluşmaktadır. Bunlar; parola, gizli soru, tek kullanımlık şifre, PIN, parmak izi, retina taraması, yüz avuç içi ve fiziksel aygıtlardır. Birinci bölüme ait örnek veri giriş formu Tablo 1'de belirtilmiştir.

Tablo 1. *Veri Giriş Formu*

Madde	1. Parola	2. Gizli soru	3. Tek kullanımlık şifre	4. PIN	5. Parmak izi	6. Retina	7. Yüz tarama	8. Avuç içi	9. Kişisel aygıt
İnternet Bankacılığı									
Kampüs Girişi									
...									

İkinci bölümde kullanıcılardan "en uygun" kimlik doğrulama şemalarını bilgi güvenliğinin üç unsuru olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirmeleri istenmiştir. Üçüncü bölümde ise kullanıcılardan "uygun olmayan" kimlik doğrulama şemalarını bilgi güvenliğinin üç unsuru olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirmeleri istenmiştir. İkinci ve üçüncü bölümde kullanılan veri giriş formu Tablo 2'de belirtilmiştir.

Tablo 2. *Veri Giriş Formu*

Bilgi Güvenliği	1. Parola	2. Gizli soru	3. Tek kullanımlık şifre	4. PIN	5. Parmak izi	6. Retina	7. Yüz tarama	8. Avuç içi	9. Kişisel aygıt
Kullanılabilirlik									
Güvenlik									
Gizlilik									

Veri toplama aracını uygulamak amacıyla katılımcıların ders saatlerinde sınıf ortamında on beş dakika süre verilerek, anket formunu doldurmaları istenmiştir. Anket formunda yer alan maddeler hakkında kullanıcılara gerekli bilgiler verilmiştir. Anket formunun son bölümünde yer alan bilgi güvenliğinin unsurları ile ilgili önemli ve gerekli bilgiler araştırmacılar tarafından kullanıcılara sunulmuştur. Kullanıcıların bu bilgiler doğrultusunda verilen her bir platforma erişim sağlarken kullanmak istedikleri kimlik doğrulama şemasını (her bir platform için 1 seçenek) belirlemeleri istenmiştir. Ayrıca kullanıcıların kimlik doğrulama şemalarını bilgi güvenliği unsurları bakımından değerlendirerek, uygun buldukları şemayı (her bir bilgi güvenliği unsuru için 1 seçenek) tercih etmeleri istenmiştir.

Verilerin Analizi

Araştırma kapsamında toplanan verilerin analizinde betimsel istatistikler kullanılmıştır. Verilerin analizinde ortalama, standart sapma, frekans ve yüzde hesaplamalarına yer verilmiştir. Elde edilen bulgular tablo olarak sunulmuştur. Ayrıca elde edilen veriler grafik aracılığı ile somutlaştırılmıştır.

BULGULAR

Kullanıcıların kimlik doğrulama şemalarını tercih durumlarını belirlemek için yapılan bu çalışmada elde edilen bulgular tablo ve grafiklerle açıklanmıştır. Araştırma bulguları üç başlıkta toplanmıştır.

Kullanıcıların Kimlik Doğrulama Şemalarını Tercih Etme Durumları

Uygulama sonucunda analiz edilen kimlik doğrulama şemalarının her bir madde için tercih edilme sayısı Tablo 3'te verilmiştir.

Tablo 3. *Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri*

	Maddeler	1. Parola	2. Gizli soru	3. Tek kullanımlık şifre	4. PIN	5. Parmak izi	6. Retina	7. Yüz tarama	8. Avuç içi	9. Kişisel aygıt	**Bilgi faktörü (1-4)**	**Kalıtım faktörü (5-8)**	**Sahiplik faktörü (9)**
Özel Alan	Sosyal medya	130	6	6	5	32	7	1	1	0	**147**	**41**	**0**
	İnternet bankacılığı	61	11	35	19	41	10	8	0	1	**126**	**59**	**1**
	E-posta hizmetleri	132	8	7	9	20	5	4	0	0	**156**	**29**	**0**
	Alışveriş siteleri	97	13	28	14	24	6	2	1	2	**152**	**33**	**2**
	GSM Operatörleri	63	15	29	27	40	3	4	0	4	**134**	**47**	**4**
	PC, cep telefonu	44	6	4	18	89	8	13	1	2	**72**	**111**	**2**
	Sağlık kurumları	37	6	14	8	56	7	13	13	32	**65**	**89**	**32**
	Spor salonları	26	2	8	10	55	4	10	5	65	**46**	**74**	**65**
	Konaklama (özel)	21	7	6	6	82	7	15	4	40	**40**	**108**	**40**
Kamusal Alan	E-devlet	109	7	12	11	30	11	5	1	2	**139**	**47**	**2**
	ÖSYM	116	6	13	13	18	9	6	1	3	**148**	**34**	**3**
	OBS	123	3	8	17	29	4	3	0	1	**151**	**36**	**1**
	E-sağlık hizmetleri	1	6	18	12	36	5	7	4	6	**37**	**52**	**6**
	Kampüs Giriş	11	2	2	5	55	2	9	3	97	**20**	**69**	**97**
	Konaklama (Kamu)	13	4	3	7	86	5	8	4	55	**27**	**103**	**55**
	Kütüphane	32	4	12	6	38	3	3	6	83	**54**	**50**	**83**
Oran (%)		**35.2**	**3.7**	**7.1**	**6.5**	**25.3**	**3.3**	**3.8**	**1.5**	**13.6**	**52.4**	**34**	**13.6**

Tablo 3'te kullanıcıların belirtilen platformlarda tercih ettikleri kimlik doğrulama şemalarının toplamları verilmiştir. Bilgi faktörü sütununda ilk dört sütuna ait (parola, gizli soru, tek kullanımlık şifre ve PIN) kimlik doğrulama şemalarının tercih sayılarının toplamı verilmiştir. Kalıtım faktörü sütununda 5-8. sütunlarda yer alan (parmak izi, retina, yüz tarama, avuç içi) kimlik doğrulama şemalarının tercih sayılarının toplamı verilmiştir. Son olarak sahiplik faktörü sütununda 9. sütunda yer alan (fiziksel aygıt) kimlik doğrulama şemalarının tercih sayısı verilmiştir.

Katılımcıların verilen platformlara girişlerde %52.4 oranında bilgi faktöründen, %34 oranında kalıtım faktöründen ve %13.6 oranında ise sahiplik faktöründen bir kimlik doğrulama şeması tercih ettikleri görülmüştür. Bilgi faktöründen kimlik doğrulama şeması tercih edenlerin %67'si parolayı tercih etmişlerdir. Bilgi faktörü kullanıcılar tarafından sosyal medya, e-posta hizmetleri, alışveriş siteleri, ÖSYM ve OBS sitemlerine girişte (%75'den fazla) yüksek oranda tercih edilirken; kampüs girişi, konaklama, e-sağlık hizmetlerinde (%20'den az) düşük oranda tercih edilmiştir. Kalıtım faktöründen kimlik doğrulama şeması tercih edenlerin %75'i parmak izini tercih etmişlerdir. Kalıtım faktörü kullanıcılar tarafından PC, cep telefonu ve konaklama sitemlerine girişte (%50'den fazla) yüksek oranda tercih edilirken; e-posta hizmetleri, alışveriş siteleri, ÖSYM ve OBS sistemlerinde (%20'den az) düşük oranda tercih edilmiştir. Sahiplik faktörü kullanıcılar tarafından kampüs girişlerinde (%50'den fazla) yüksek oranda tercih edilirken; sosyal medya, internet bankacılığı, e-posta hizmetleri, alışveriş siteleri, GSM operatörleri, PC &cep telefonu, e-devlet, ÖSYM, OBS, e-sağlık hizmet sistemlerinde (hiç ya da %5'ten az) düşük oranda tercih edilmiştir.

Kullanıcıların Bilgi Güvenliği Bakımından Uygun Buldukları Kimlik Doğrulama Şemaları

McCumber, (1991), bilgi güvenliğini kullanılabilirlik, gizlilik ve güvenlik olarak üç başlıkta toplanmıştır. Bu çalışmada katılımcılardan kimlik doğrulama şemalarını bu öğelere göre en uygun bulunan kimlik doğrulama şemasını tercih etmeleri istenmiştir. Katılımcıların seçimleri analiz edilerek Tablo 4'te sunulmuştur.

Tablo 4. *Uygun Bulunan Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri*

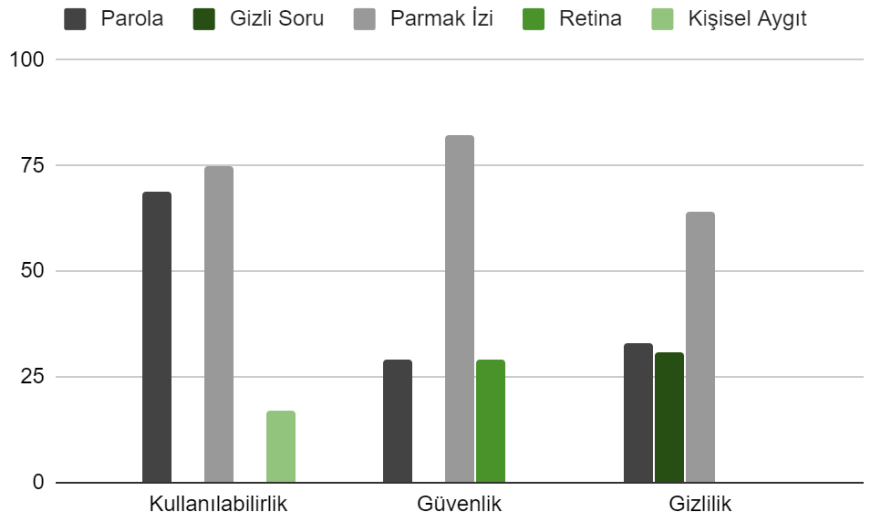
Bilgi Güvenliği	1. Parola	2. Gizli soru	3. Tek kullanımlık şifre	4. PIN	5. Parmak izi	6. Retina	7. Yüz tarama	8. Avuç içi	9. Kişisel aygıt	**Bilgi faktörü (1-4)**	**Kalıtım faktörü (5-8)**	**Sahiplik faktörü (9)**
Kullanılabilirlik	69	2	11	9	75	3	2	0	17	**91**	**80**	**17**
Güvenlik	29	10	12	5	82	29	12	4	5	**56**	**127**	**5**
Gizlilik	33	31	15	4	64	20	13	2	5	**83**	**99**	**5**
Oran (%)	**23.3**	**7.6**	**6.7**	**3.2**	**39.3**	**9.2**	**4.8**	**1.1**	**4.8**	**40.9**	**54.4**	**4.8**

Bilgi güvenliği açısından bakıldığında kullanıcıların %40.9 oranında bilgi faktöründen, %54.4 oranında kalıtım faktöründen ve %4.8 oranında ise sahiplik faktöründen bir kimlik doğrulama şeması tercih ettikleri görülmüştür. Bilgi güvenliği alt boyutlarından "güvenlik" ve "gizlilik" incelendiğinde katılımcılar en çok kalıtım faktörünü (%67.6) tercih etmişlerdir. Kullanılabilirlik incelendiğinde ise bilgi faktörünü tercih ettikleri görülmüştür. Bilgi faktöründen kimlik doğrulama şeması tercih edenlerin %67'si parolayı tercih etmişlerdir. Bilgi faktörü kullanıcılar tarafından sosyal medya, e-posta hizmetleri, alışveriş siteleri, ÖSYM ve OBS sitemlerine girişte (%75'den fazla) yüksek oranda tercih edilirken; kampüs girişi, konaklama, e-sağlık hizmetlerinde (%20'den az) düşük oranda tercih edilmiştir. Kalıtım faktöründen kimlik doğrulama şeması tercih edenlerin %75'i parmak izini tercih etmişlerdir. Kalıtım faktörü kullanıcılar tarafından PC, cep telefonu ve konaklama sitemlerine girişte (%50'den fazla) yüksek oranda tercih edilirken; e-posta hizmetleri, alışveriş siteleri, ÖSYM ve OBS sistemlerinde (%20'den az) düşük oranda tercih edilmiştir. Sahiplik faktörü kullanıcılar tarafından kampüs girişlerinde (%50'den fazla) yüksek oranda tercih edilirken; sosyal medya, internet bankacılığı, e-posta hizmetleri, alışveriş siteleri, GSM operatörleri, PC &cep telefonu, e-devlet, ÖSYM, OBS, e-sağlık hizmet sistemlerinde (hiç ya da %5'ten az) düşük oranda tercih edilmiştir.

Araştırmada elde edilen bulgulara göre "parmak izi" ve "parola", bilgi güvenliği unsurları bakımından en uygun bulunan ve tercih edilen şemalar olmuştur. Tablo 5 değerlendirildiğinde bilgi faktörünün tercih edilme oranı %40.9 iken, kalıtım faktörünün tercih edilme oranı %54.4 olarak görülmektedir. Verilen tabloya göre sahiplik faktörü %4.8 tercih edilme oranı ile en az tercih edilen faktör olmuştur.

Kimlik doğrulama şemaları arasında kullanılabilirlik, güvenlik ve gizlilik açısından bir karşılaştırma yapıldığında, en çok tercih edilen şemaların parola ve parmak izi kimlik doğrulama şemaları olduğu Grafik 1'de gösterilmiştir.

Grafik 1. *Uygun Bulunan Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri*



Kullanılabilirliğe bağlı olarak yapılan seçimlerde kullanıcılar gizli soru, retina ve yüz tarama şemalarını az sayıda tercih ederken, avuç içi şeması için tercihte bulunmamışlardır. Parola ve parmak izi şemaları kullanılabilirlik açısından birbirlerine yakın değerler alırken, güvenlik ve gizlilik açısından parmak izi, paroladan daha uygun görülen şema olmuştur. Kişisel aygıt şeması ise hem kullanılabilirlik hem güvenlik hem de gizlilik bakımından düşük değerler almıştır. Parmak izi şeması kullanılabilirlik, güvenlik ve gizlilik açısından yüksek ve birbirine yakın değerler alırken, parola şeması kullanılabilirlik açısından yüksek tercih edilme değerine sahipken güvenlik ve gizlilik bakımından düşük bir değere sahip olduğu görülmektedir.

Kullanıcıların Bilgi Güvenliği Bakımından Uygun Bulmadıkları Kimlik Doğrulama Şemaları

Tablo 5'de kimlik doğrulama şemaları Bonneau ve ark. (2012) tarafından önerilen şekilde kullanılabilirlik, güvenlik ve gizlilik bakımından karşılaştırılmıştır. Bu unsurlar bakımından uygun bulunmayan tüm kimlik doğrulama şemalarının analizi yapılarak tercih edilme değerleri Tablo 5'de verilmiştir. Katılımcılara sunulan kimlik doğrulama şemaları arasında kullanılabilirlik ve güvenlik açısından bir karşılaştırma yapıldığında en yaygın kullanılan ve aynı zamanda en çok tercih edilen şemalar parola ve parmak izi kimlik doğrulama şeması olarak Tablo 4'te verilmiştir.

Tablo 5. *Uygun Bulunmayan Kimlik Doğrulama Şemalarının Tercih Edilme Değerleri*

Bilgi Güvenliği	1. Parola	2. Gizli soru	3. Tek kullanımlık şifre	4. PIN	5. Parmak izi	6. Retina	7. Yüz tarama	8. Avuç içi	9. Kişisel aygıt	**Bilgi faktörü (1-4)**	**Kalıtım faktörü (5-8)**	**Sahiplik faktörü (9)**
Kullanılabilirlik	7	26	35	7	10	25	17	21	40	**75**	**73**	**40**
Güvenlik	25	31	19	17	7	6	17	10	54	**92**	**40**	**54**
Gizlilik	28	27	17	18	9	5	14	8	62	**90**	**36**	**62**
Oran (%)	**10.7**	**14.9**	**12.6**	**7.5**	**4.6**	**6.4**	**8.5**	**6.9**	**27.8**	**45.7**	**26.5**	**27.8**

Sonuçlar değerlendirildiğinde gizli soru, yüz tarama ve fiziksel aygıt şemaları bilgi güvenliği unsurları bakımından uygun bulunmayan ve tercih edilmeyen şemalar olmuşlardır. Tablo 5 değerlendirildiğinde bilgi faktörünün uygun olmama algısı oranı %45.7 iken, kalıtım faktörünün uygun olmama algı oranı %26.5 olarak görülmektedir. Verilen tabloya göre sahiplik faktörü %27.8 tercih oranı ile en uygun olmayan kimlik doğrulama yöntemi olmuştur.

SONUÇ

Bu araştırma dokuz farklı kimlik doğrulama şemasının kullanıcılar tarafından hangi platformlarda tercih edildiğini gösteren, nicel bir çalışmadır. Sonuçlar incelendiğinde, kullanıcılar için yüksek bilişsel yük gibi olumsuz yönlerine rağmen parolanın en çok tercih edilen kimlik doğrulama şeması olduğu görülmüştür.

Parmak izi şeması platformlara erişim sağlarken, Zimmermann ve Gerberb'ın (2019) çalışmasında olduğu gibi paroladan sonra en çok tercih edilen kimlik doğrulama şeması olmuştur. Bilgi güvenliği unsurları olan kullanılabilirlik, güvenlik ve gizlilik bakımından değerlendirildiğinde parmak izi şeması, kullanımı en çok tercih edilen kimlik doğrulama şeması olmuştur.

Kimlik doğrulama şemaları genel olarak değerlendirildiğinde katılımcılar %52 oranında bilgi faktörünü, %34 oranında kalıtım faktörünü ve %13 oranında sahiplik faktörünü tercih etmişlerdir. Bilgi faktörünü tercih eden kullanıcıların üçte ikisi parola şemasını tercih etmiştir.

Günlük yaşantıda fiziksel ortamlara giriş sağlarken kullanılan fiziksel aygıt şeması (kart, sensör cihazı, vb.), anket formunda kullanıcılar tarafından fiziksel ortamlar için en çok tercih edilen kimlik doğrulama şeması olmuştur. Kullanıcılar, bilgi faktörüne bağlı kimlik doğrulama şemalarının bilgi güvenliğinin unsurları olan kullanılabilirlik, gizlilik ve güvenlik açısından uygun bulmadıklarını belirtmişlerdir.

Kullanıcıların platformlara erişim sağlamaları için tercih ettikleri şemaların, günümüzde kullanıcıların çoğu tarafından bilinen ve yaygın olarak kullanılan şemalar ile aynı olduğu gözlemlenmiştir. Bonnue (2012) yaptığı çalışmada kullanıcıların günlük yaşantısında kullandıkları şemalarla, tercih ettikleri şemaların benzerlik gösterdiğine dikkat çekmiştir.

• Yapılan bu çalışmada kullanıcılar tarafından en çok parola ve parmak izi şeması tercih edilmiştir. Bu şemaların tercih edilme nedenlerinin bilinmesi için, konu hakkında nitel araştırmalar yapılabilir.

• Kullanıcılara platformlara erişim sağlayabilmeleri için yaygın kullanımın dışında farklı kimlik doğrulama şemaları kullanma olanağı sağlanabilir.

• Kişisel aygıtların kullanılabilirlik, güvenlik ve gizlilik algısının düşük olmasının nedenlerini belirlemeye yönelik çalışmalar yapılabilir.

• Parola için gizlilik ve güvenlik algısını artırabilecek çalışmalar yapılabilir.

KAYNAKÇA

Bandyopadhyay, S. (2011). Internet of things: applications and challenges in technology and standardization. *Wireless Personal Communications, (58),* 49–69.

Bhagavatula, C., Ur, B., Iacovino, K., Kywe†, S., Lorrie Faith Cranor, Marios Savvides (2015, Şubat). Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. Kullanılabilir Güvenlik Çalıştayı toplantısında gerçekleştirilen sempozyum, United States.

Bonneau, J., Herley, C., P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," University of Cambridge Computer Laboratory, Tech Report 817, 2012, www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.html

Chan, P.K., Fan, W., Prodromidis, A., Stolfo, S.J., (1999). Distributed data mining in credit card fraud detection. *IEEE Intelligent Systems and their Applications,* 67-74.

Karasar, N. (2002). *Bilimsel araştırma yöntemleri*. Ankara: Nobel Yayıncılık.

Lee, J.R., Rao, S., Nass, C., Forssell, K., John, J.M. (2012). When do online shoppers appreciate security enhancement efforts? effects of financial risk and security level on evaluations of customer authentication. *International Journal of Human-Computer Studies (5),* 364–376. https://doi.org/10.1016/j.ijhcs.2011.12.002.

Mannan, M. and Van Oorschot, P.C. (2008). Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of Computer Security*, 703-750.

Mengi, B. (2013). Sağlık hizmetlerinde meydana gelebilecek hileleri önlemeye yönelik bir uygulama olarak biyometrik kimlik doğrulama sistemlerinin kullanımı. *Muhasebe ve Finansman Dergisi, (60),* 39-50.

Özkaya, N., & Sağıroğlu, Ş. (2014). *Açık anahtar altyapısı ve biyometrik teknikler.* 05.01.2020 tarihinde https://www.researchgate.net/profile/Necla_Ozkaya/publication/ adresinden alınmıştır.

Sun, C. (2012). *Application of RFID technology for logistics on the internet of things.* AASRI Procedia, 1(2012), 106-111.

University of Cambridge (1995). *About: Internet of things.* 06.01.2020 tarihinde http://www.cl.cam.ac.uk/coffee/qsf/coffee.html adresinden alınmıştır.

Zimmermann, V., Gerberb N. (2019). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies,* 26-44.

EXTENDED ABSTRACT

INTRODUCTION

Different devices' communicating, interacting and exchanging data have revealed various needs in terms of privacy, security and usability, which are the three elements of information security (McCumber, 1991). Authentication systems have been developed that allow users to secure information, allow access to various devices or platforms, and protect their personal data. These systems offer users many authentication logins options to access their personal data or personal devices. Authentication login options in the literature; information, hereditary characteristics (such as fingerprint, retina scanning), location, time and ownership are classified in five categories (Kayrancıoğlu, 2019).

The widely used information factor today; It contains authentication schemes such as password, secret question, single-use password and PIN consisting of information owned by users (Kayrancıoğlu, 2019). Heredity factor covers personal physical property data; It includes authentication schemes such as fingerprints, retinal scans, facial recognition and palms (Riley, 2009). The ownership factor is; It can be explained as physical devices that users use for authentication while accessing the system.

The purpose of this research is to determine the authentication schemes that users prefer in different environments. In this context, answers to the following research questions were sought.

• Which authentication schemes are preferred on different cyber environments and platforms?

• What is the most suitable authentication scheme for users in terms of usability, security and privacy, which are the three elements of information security?

• What is the least preferred authentication scheme in terms of usability, security and privacy, which are the three elements of information security?

METHOD

In this research was used screening model. The existing situation in this model is tried to be described as it is. Karataş (2012) has defined screening models as research approaches aiming to describe a situation as it is in the past or still. The individual, subject or object that is the subject of the research was tried to be defined as it exists within its own conditions.

Research Design

The research method and the reasoning behind it should be included in this section. The literature about the research method should be stated. Moreover, the design of the study should be stated.

Participants

The universe of the study is the users who are studying at Necmettin Erbakan University Ahmet Keleşoğlu Education Faculty. The sample of the research consists of 188 randomly selected users studying in the same faculty.

126 of the users participating in the research are women and 62 are men. Approximately two-thirds of the participants are graduates of Anatolian High School. The academic achievements of the users participating in the research are categorized into three categories. When their academic achievement score is less than 60, the participants have a low level of success, high when they are 90 or above, and a medium level of achievement when they have between 60 and 90. 63.8% of the participants have moderate academic success. 51 of the users participating in the study are studying in the field of information technologies and 137 are studying in other fields.

Data Collection Tools

The data collection tool was developed by the researchers in the study. The data collection tool consists of four parts. In the first part, users were asked about gender, high school type, academic achievement level, and department information.

In the second part, there are different platforms consisting of 16 items under the titles of public and private spaces. These items are social media, internet banking, e-mail services, shopping sites, mobile applications of GSM operators, PC (computer, tablet), entrance to health institutions, entrance to gyms, accommodation (home, private dormitory, etc.), e-government, ÖSYM (Measurement Selection and Placement Center), OBS (Student Information System), e-health services, campus entrance, accommodation (state dormitory) and library operations. Users were asked to specify their preferred authentication scheme when logging into these platforms. These authentication schemes consist of nine items. These; password, secret question, one-time password, PIN, fingerprint, retina scan, face scan, palm and physical devices.

In the third section, users were asked to evaluate “most appropriate” authentication schemes in terms of usability, security and privacy, which are the three elements of information security. In the fourth section, users were asked to evaluate “inappropriate” authentication schemes in terms of usability, security and privacy, which are the three elements of information security.

In order to apply the data collection tool, participants were asked to fill in the questionnaire by giving fifteen minutes in the classroom environment during class hours.

Data Analysis

Descriptive statistics were used to analyze the data collected within the scope of the research. Average, standard deviation, frequency and percentage calculations are included in the analysis of the data.

FINDINGS

Users' Preference for Authentication Schemes

It was seen that participants preferred 52.4% knowledge factor, 34% heredity factor and 13.6% ownership factor when entering the platforms. The information factor was highly preferred by users for access to social media, e-mail services, shopping sites, ÖSYM and OBS systems (more than 75%), but low in campus entrance, accommodation, e-health services (less than 20%). preferred. 75% of those who prefer the heredity factor preferred fingerprints. The inheritance factor was highly preferred by users (more than 50%) in accessing PC, mobile phone and accommodation systems. Ownership factor is highly preferred by users at campus entrances (more than 50%).

Authentication Schemes that Users Approve for Information Security

In terms of information security, users preferred a scheme of 40.9% information factor and it was observed that they preferred an authentication scheme of 54.4% inheritance factor. When “security” and “privacy” are examined among the information security sub-dimensions, the participants preferred the most inheritance factor (67.6%). 67% of those who preferred the information factor preferred the password. 75% of those who prefer the heredity factor preferred fingerprints.

According to the findings obtained in the research, "fingerprint" and "password" were the most suitable and preferred schemes in terms of information security elements. Ownership factor was the least preferred factor with 4.8% preference rate.

Authentication Schemes Users Do Not Approve for Information Security

While the rate of perception of the non-compliance of the information factor is 45.7%, the rate of inheritance of the inheritance factor is seen as 26.5%. Ownership factor was the most inappropriate authentication method with 27.8% preference rate.

DISCUSSION AND CONCLUSION

When the authentication schemes are evaluated in general, the participants preferred 52% information factor, 34% heredity factor and 13% ownership factor.

The physical device scheme (card, a sensor device, etc.) used when providing access to physical environments in daily life has been the most preferred authentication scheme for the physical environments by users.

It has been observed that the schemes that users prefer to access the platforms are the same schemes that are known and widely used by most users today. In his study, Bonnue (2012) pointed out that the schemes used by users in their daily lives are similar to the schemes they prefer.

• In this study, the password and fingerprint scheme were preferred most by the users. Qualitative research can be done on the subject in order to know the reasons why these schemes are preferred.

• Users can be given the opportunity to use different authentication schemes other than widespread use in order to access the platforms.

• Studies can be conducted to determine the reasons for the low perception of usability, security and privacy of personal devices.

• Studies that can increase the perception of privacy and security for the password can be done.