

T.C.  
GEBZE TEKNİK ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DİJİTAL DOĞRULAMA TEKNOLOJİLERİNİN  
VATANDAŞLAR TARAFINDAN KAMU HİZMETLERİNDE  
KULLANIMINI ETKİLEYEN FAKTÖRLER

ŞEYMA NUR KONYAR

YÜKSEK LİSANS TEZİ  
İŞLETME ANABİLİM DALI

DANIŞMAN: DOÇ. DR. FARİD HUSEYNOV

ŞUBAT 2024

T.C.  
GEBZE TEKNİK ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DİJİTAL DOĞRULAMA TEKNOLOJİLERİNİN  
VATANDAŞLAR TARAFINDAN KAMU HİZMETLERİNDE  
KULLANIMINI ETKİLEYEN FAKTÖRLER

ŞEYMA NUR KONYAR

YÜKSEK LİSANS TEZİ  
İŞLETME ANABİLİM DALI

DANIŞMAN: DOÇ. DR. FARİD HUSEYNOV

ŞUBAT 2024

**T.R.**  
**GEBZE TECHNICAL UNIVERSITY**  
**GRADUATE SCHOOL**

**FACTORS AFFECTING THE USE OF DIGITAL  
VERIFICATION TECHNOLOGIES BY CITIZENS IN  
PUBLIC SERVICES**

**ŞEYMA NUR KONYAR**

**A THESIS OF MASTER OF SCIENCE**  
**DEPARTMENT OF BUSINESS ADMINISTRATION**

**ADVISOR: DOÇ. DR. FARID HUSEYNOV**

**FEBRUARY 2024**

## YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun 12/02/2024 tarih ve 2024/13 sayılı kararıyla oluşturulan jüri tarafından 28/02/2024 tarihinde tez savunma sınavı yapılan ŞEYMA NUR KONYAR 'ın tez çalışması İŞLETME Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

### JÜRİ

ÜYE  
(TEZ DANIŞMANI) : DOÇ. DR. FARİD HUSEYNOV

ÜYE : PROF. DR. İLKAY KARADUMAN

ÜYE : DR. ÖĞR. ÜYESİ İLHAN ÇAM

ÜYE :

ÜYE :

### ONAY

Gebze Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun  
...../...../..... tarih ve ...../..... sayılı kararı.

İMZA/MÜHÜR



*İthaf / Dedication*  
*Annem, babam, kardeşim*  
*ve*  
*eşime*

## ÖZET

Dijital doğrulama, bir kişinin veya işlemin dijital dünyada kimlik ve yetkilendirme işlemlerinin yapılması için kullanılan bir teknoloji ve süreçtir. Bu süreç, kişilerin kimliklerini ve haklarını dijital platformlarda kanıtlamalarını sağlar. Bir kişinin veya cihazın kimliğini veya yetkisini çevrimiçi bir platformda veya işlemde doğrulamak için kullanılan yöntemler ve teknolojiler bütünüdür. Bu tür doğrulama, gizliliği ve güvenliği artırmak, kimlik hırsızlığını önlemek ve dijital ortamda güvenilirlik sağlamak amacıyla kullanılır. Dijital doğrulama için kullanılan bazı temel teknolojiler şunlardır: Şifreler ve Parolalar, İki Faktörlü Kimlik Doğrulama (2FA), Biyometrik Kimlik Doğrulama, Akıllı Kartlar ve Kimlik Belgeleri, Blok Zincir Tabanlı Kimlik Doğrulama. Dijital doğrulama teknolojileri çeşitlilik gösterir ve her teknoloji farklı güvenlik seviyeleri ve kullanım senaryoları sunar. Genel olarak, üç temel doğrulama kategorisi vardır: bilgiye dayalı, sahiplik temelli ve ikinci faktör tabanlı. Dijital doğrulama teknolojileri çevrimiçi alışveriş, bankacılık işlemleri, hükümet hizmetleri, sağlık kayıtları, eğitim platformları ve daha birçok alanda kullanılabilir. Dijital kimlik doğrulama teknolojileri dünya genelinde yaygın olarak kullanılmaktadır. Her ülke kendi dijital kimlik doğrulama sistemlerini geliştirebilir veya benimseyebilir. Özellikle gelişmiş ülkeler ve dijital altyapıya sahip ülkeler, bu teknolojileri daha yaygın olarak kullanmaktadır. Araştırma, bu teknolojilerin kabul edilme sürecini, yaygınlaşma seviyelerini ve vatandaşların bu teknolojileri kullanmalarını teşvik eden veya engelleyen unsurları anket çalışması yapılarak ortaya koymayı hedeflemektedir. Bu çalışmada kullanım kolaylığı ve kullanıcı güveninin, algılanan fayda üzerinde anlamlı bir etkisi olduğu görülmüştür. Teknoloji yetkinliğinin, bu teknolojileri kullanım niyeti üzerinde anlamlı bir etkisi olduğu görülmüştür. Bu çalışma ilgili alanda çalışan akademisyenlere ve uygulama geliştiricilerine faydalı bilgiler sunmaktadır.

**Anahtar Kelimeler: Dijital Doğrulama, Kimlik Doğrulama, Biyometrik, Blok Zincir, Güvenlik, İki Faktörlü Doğrulama**

## SUMMARY

Digital authentication is a technology and process used for verifying the identity and authorization of an individual or transaction in the digital world. This process enables individuals to prove their identities and rights on digital platforms. It encompasses the methods and technologies used to verify the identity or authorization of a person or device in an online platform or transaction. Such authentication is employed to enhance privacy and security, prevent identity theft, and establish reliability in the digital realm. Some fundamental technologies used for digital authentication include Passwords, Two-Factor Authentication (2FA), Biometric Authentication, Smart Cards and Identity Documents, and Blockchain-Based Identity Verification. Digital authentication technologies vary in diversity, offering different security levels and usage scenarios. Generally, there are three main authentication categories: knowledge-based, possession-based, and second-factor-based. Digital authentication technologies can be utilized in various fields such as online shopping, banking transactions, government services, health records, educational platforms, and many more. Digital identity authentication technologies are widely used worldwide. Each country may develop or adopt its own digital identity authentication systems. Particularly, advanced and digitally infrastructure-rich countries tend to employ these technologies more widely. The research aims to reveal the acceptance process, levels of proliferation, and factors that encourage or hinder citizens' use of these technologies through survey studies. It has been observed in this study that ease of use and user confidence have a significant impact on perceived benefits. Additionally, technology proficiency has a significant influence on the intention to use these technologies. This study provides valuable insights to academics and application developers in the field.

**Keywords: Digital Authentication, Identity Verification, Biometric, Blockchain, Security, Two-Factor Authentication**

## TEŞEKKÜR

Yüksek lisans ve tez yazım sürecim boyunca; bilgi ve deneyimiyle yol gösterici olan, desteklerini hiç esirgemeyen tez danışmanım Doç. Dr. Farid HUSEYNOV ‘a sonsuz teşekkürlerimi sunarım. Başarılarımda ve bu günlere gelmemde en büyük emeğe sahip olan, anneme ve babama; yorulduğum dönemlerde hayat enerjimi yükselten eşime ve yüksek lisansım boyunca beni motive edip bilgileriyle besleyen yöneticilerime teşekkürlerimi sevgiyle sunarım.



# İÇİNDEKİLER

|                                                                        | <b><u>Sayfa</u></b> |
|------------------------------------------------------------------------|---------------------|
| ÖZET                                                                   | vi                  |
| ABSTRACT                                                               | vii                 |
| TEŞEKKÜR                                                               | viii                |
| İÇİNDEKİLER                                                            | ix                  |
| SİMGELER ve KISALTMALAR DİZİNİ                                         | xi                  |
| ŞEKİLLER DİZİNİ                                                        | xiv                 |
| TABLolar/ÇİZELGELER DİZİNİ                                             | xv                  |
| <br>                                                                   |                     |
| 1. GİRİŞ                                                               | 1                   |
| 1.1. Literatür Özeti, Tezin Amacı, Katkısı ve İçeriği                  | 1                   |
| 1.2. Tezin Amacı ve Kapsamı                                            | 2                   |
| 1.2.1. Amaç                                                            | 2                   |
| 1.2.2. Tezin Kapsamı                                                   | 3                   |
| 1.2.3. Tezin Önemi                                                     | 3                   |
| 2. LİTERATÜR                                                           | 5                   |
| 2.1. Kamuda Dijital Doğrulama                                          | 5                   |
| 2.1.1. Dijital Devlet Kavramı                                          | 5                   |
| 2.1.2. Dijital Doğrulama Teknolojilerinin AB Ülkelerinde Kullanımı     | 6                   |
| 2.1.3. Dijital Kimlik ve Kimlik Doğrulamanın Kabul Edilmesi Neden Zor? | 7                   |
| 2.1.4. Dijital Doğrulama Vatandaşa ve Devlete Ne Sağlar?               | 7                   |
| 2.1.5. Dijital Kimlik Cüzdanı ve Faydaları                             | 8                   |
| 2.1.6. Pratikte AB Dijital Kimlik Cüzdanı: Vatandaşlar                 | 8                   |
| 2.1.7. Dijital Kimliklerin Güven Sorunu                                | 9                   |
| 2.2. Literatür Araştırması                                             | 9                   |
| 2.2.1. E-Vatandaşlık (Estonya Örneği)                                  | 9                   |
| 2.2.2. E-Belediyecilik                                                 | 10                  |
| 2.2.3. Dijital Doğrulama ile Ödeme Sistemleri                          | 11                  |
| 2.2.4. Dijital Cüzdan                                                  | 11                  |
| 2.2.5. Vatandaşlar Gözünden Doğrulama Teknolojileri                    | 12                  |
| 3. METOT                                                               | 13                  |
| 3.1. Tez Yazımında Kullanılan Metodoloji                               | 13                  |
| 3.2. Katılımcıların Belirlenmesi                                       | 13                  |
| 3.3. Verilerin Toplanması                                              | 14                  |
| 3.4. Verilerin Analizi                                                 | 14                  |
| 3.5. Araştırmada Kullanılan Ölçek Referansları                         | 14                  |
| 4. HİPOTEZLER                                                          | 17                  |
| 4.1. Teknoloji Kabul Modeli                                            | 17                  |
| 4.2. Teknoloji Kabul Modeli Girdileri                                  | 18                  |
| 4.2.1. Algılanan Fayda                                                 | 18                  |

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| 4.2.2. Kullanım Kolaylığı                                                               | 18 |
| 4.2.3. Güvenlik ve Gizlilik                                                             | 19 |
| 4.2.4. Kullanıcı Güveni                                                                 | 19 |
| 4.2.5. Teknoloji Yetkinliği                                                             | 20 |
| 5. BULGULAR                                                                             | 21 |
| 5.1. Demografik Veriler                                                                 | 21 |
| 5.1.1. Yaşa Göre Dijital Doğrulama Teknolojileri Kullanımı                              | 21 |
| 5.1.2. Cinsiyete Göre Dijital Doğrulama Teknolojileri Kullanımı                         | 21 |
| 5.1.3. Eğitim Durumuna Göre Dijital Doğrulama Teknolojileri Kullanımı                   | 22 |
| 5.1.4. Çalışma Durumuna Göre Dijital Doğrulama Teknolojileri Kullanımı                  | 22 |
| 5.2. Doğrulayıcı Faktör Analizi (CFA)                                                   | 23 |
| 5.2.1. Verilerin Normallik Testi                                                        | 25 |
| 5.2.2. Verilerin Güvenilirlik Analizi                                                   | 27 |
| 5.2.3. Dijital Doğrulama Teknolojilerini Kullanma Niyetini Etkileyen Faktörlerin Ölçümü | 28 |
| 6. SONUÇ                                                                                | 31 |
| 6.1. Akademik Çıktılar                                                                  | 32 |
| 6.2. Uygulamaya Yönelik Çıktılar                                                        | 32 |
| 6.3. Gelecek Çalışmalar İçin Öneriler                                                   | 34 |
| KAYNAKLAR                                                                               | 35 |
| ÖZGEÇMİŞ                                                                                | 38 |
| TEZ ÇALIŞMASI KAPSAMINDA YAPILAN YAYINLAR                                               | 39 |
| EKLER                                                                                   | 40 |

## SİMGELER ve KISALTMALAR DİZİNİ

|        |                                                         |
|--------|---------------------------------------------------------|
| UTAUT  | : Birleştirilmiş Kabul ve Teknoloji Kullanımı Teorisi   |
| UTAUT2 | : Birleştirilmiş Kabul ve Teknoloji Kullanımı Teorisi 2 |
| NFC    | : Near Field Communication / Yakın Alan İletişimi       |
| SMS    | : Kısa Mesaj                                            |



## ŞEKİLLER DİZİNİ

|                                                                                        | <b><u>Sayfa</u></b> |
|----------------------------------------------------------------------------------------|---------------------|
| <b>Şekil 3.1:</b> İzlenen yol.                                                         | 26                  |
| <b>Şekil 4.1:</b> UTAUT2 model dijital doğrulama teknolojileri kullanımı değişkenleri. | 30                  |
| <b>Şekil 5.1:</b> Ölçüm (CFA) modeli.                                                  | 36                  |
| <b>Şekil 5.2:</b> Yol analizi.                                                         | 41                  |



## TABLolar/ÇİZELGELER DİZİNİ

|                                                                      | <b><u>Sayfa</u></b> |
|----------------------------------------------------------------------|---------------------|
| <b>Tablo 3.1:</b> Ölçek referansları.                                | 28                  |
| <b>Tablo 5.1:</b> Yaş gruplarındaki kişi sayısı dağılımı.            | 33                  |
| <b>Tablo 5.2:</b> Cinsiyet gruplarındaki kişi sayısı dağılımı.       | 33                  |
| <b>Tablo 5.3:</b> Eğitim durumu gruplarındaki kişi sayısı dağılımı.  | 34                  |
| <b>Tablo 5.4:</b> Çalışma durumu gruplarındaki kişi sayısı dağılımı. | 34                  |
| <b>Tablo 5.5:</b> Standartlaştırılmış regresyon ağırlıkları.         | 36                  |
| <b>Tablo 5.6:</b> Model uyum metrikleri.                             | 37                  |
| <b>Tablo 5.7:</b> Verilerin normallik testi.                         | 39                  |
| <b>Tablo 5.8:</b> Geçerlilik ve güvenilirlik değerlendirmesi.        | 39                  |
| <b>Tablo 5.9:</b> Regresyon ağırlıkları.                             | 41                  |
| <b>Tablo 5.10:</b> Kare çoklu korelasyonlar.                         | 41                  |

# 1. GİRİŞ

## 1.1. Literatür Özeti, Tezin Amacı, Katkısı ve İçeriği

Endüstri 4.0 ve dijital dönüşüm tanımlarının hayatımıza girmesi ile birçok işlem artık dijital olarak yürütülmektedir. Dijitalleşmenin bir parçası olarak; yüz tanıma, biyometrik doğrulama, elektronik imza ve kimlik belgesi doğrulama gibi dijital doğrulama sistemleri de daha sık görülmeye başlanmıştır.

Bankadan yeni bir hesap açmak, e-devlet üzerinden tapu bilgilerini kontrol etmek gibi kişisel verilerin olduğu farklı işlemleri yapabilir hale gelinmiştir. Bu doğrultuda hem kişisel verilerimizin korunması hem de işlem yapan kişinin gerçek ve doğru kişi olduğunun ispatı için doğrulama teknolojileri devreye girmektedir. Parmak izi, yüz biyometrisi, göz retinası ve elle atılan imzanın biyometrik verileri gibi kişiye özel olan veriler sayesinde kimliği tespit etmek mümkündür.

Dijital doğrulamada; issuer, holder, verifier tipinde 3 grup vardır: Değiştirilemeyen belgeleri (bordro, adli kayıt, kimlik vs.) veren kurumlara issuer denir. Bu belgelerin sahipleri, yani doğrulananlara holder denir. Issuerların holderları doğruladığı cihaz vb. araçlara verifier denir. Issuer ve holder arasında politikalar, kanun ve yönetmelikler; diğerleri arasında prosedürler bulunmaktadır.

Dijital kimlikler, kamu başta olmak üzere yakın zamanda pek çok alanda kullanılacaktır. Notere gitmeden işlem yapmak ve tapu dairesine gitmeden mülk alıp satmak mümkün olabileceği; gibi dijital kimlik altında diploma, öğrenci belgesi gibi belgeler de saklanabilir hale gelecektir.

Sahtecilik riski, hep belgelerin fizikselinde ve fiziksel doğrulamalarda oluşmaktadır. Çünkü bir belgenin değiştirilebilen kısmı fiziksel kısımdır. Bunun önlenmesi için değiştirilemeyen belgelerin, değiştirilemeyen kısımlarının doğrulanması önemlidir. Değiştirilemeyen bu kısımlar, blok zincir teknolojisi ile çalışmaktadır. Her ülkenin blok zinciri farklı (ethereum, bitcoin vb.) olabilir. Ancak ilerleyen zamanlarda globalde ortak bir yapı olmalı ve blok zincirler birbiri ile konuşmalıdır.

Toplumda yaşanan hızlı değişime kamu kesiminin ayak uyduramadığı ve bunun sonucunda da kamu tarafından sunulan hizmetlerin kalitesinin toplumsal talepleri karşılayacak düzeyden uzak kaldığı görüşü, özellikle son yıllarda genellikle kabul

görmektedir (Gül, 2002). Bu tez çalışmasına; dijital doğrulama teknolojilerinin yaygınlaşmasına, dijital devlet kavramının gelişmesine, bu sektörde rol alan veya alacak kurumların bu ürünlerin kullanıcılarını artırmaya yönelik çalışmalarında kullanmak üzere çalışmadan yararlanmasına yönelik faydalı olacağı düşünülerek ihtiyaç duyulmuştur.

Bu çalışmada; dijital doğrulama teknolojilerinin kullanımını etkileyen faktörlerin belirlenmesi amacıyla bir model oluşturulmuştur. Teknoloji kabul modeliyle oluşturulan bu modele göre internet ortamında bir anket yapılmıştır. Bu anket sonuçlarının analizinde elde edilen bulgular şöyledir; Veriler, yapılan analizlerde güvenilir ve geçerli bulunmuştur. Kullanım kolaylığı, kullanıcı güveni, gizlilik ve güvenlik, algılanan fayda, kullanıcı güveni, teknoloji yetkinliği faktörlerinin incelendiği bu analizde; kullanıcı güveni ve teknoloji yetkinliğinin niyet üzerinde anlamlı bir etkisi olduğu görülmüştür. Diğer faktörlerin ise niyet üzerinde anlamlı bir etkisi bulunmamıştır.

## **1.2. Tezin Amacı ve Kapsamı**

### **1.2.1. Amaç**

Dijital doğrulama teknolojileri son yıllarda sıklıkla kullanılmaya başlanmıştır. Bununla beraber vatandaşlar tarafından kullanımı etkileyen (güvenlik endişesi, teknoloji yetkinliği vb.) bazı faktörler de ortaya çıkmıştır. Bu tez, dijital doğrulama teknolojilerinin vatandaşlar tarafından kamu hizmetlerinden kullanımını etkileyen faktörleri incelemek ve analiz etmektedir. Araştırma, bu teknolojilerin kabul edilme sürecini, yaygınlaşma seviyelerini ve vatandaşların bu teknolojileri kullanmalarını teşvik eden veya engelleyen unsurları ortaya koymayı hedeflemektedir. Bu doğrultuda, UTAUT2 teknoloji kabul modeli girdileri ile bir anket çalışması yapılarak, vatandaşların dijital doğrulama teknolojilerini benimsemelerinde etkili olan sosyal, kültürel, teknik ve güvenlik odaklı faktörler incelenmiştir. Anket sonuçlarına göre vatandaşların dijital doğrulama teknolojilerini kullanma niyetinde ne gibi etkenlerin var olduğu görülecektir.

### 1.2.2. Tezin Kapsamı

Bu tezde, dijital doğrulama teknolojileri tüm kullanım alanlarıyla ele alınmıştır. Türkiye ve dünyada dijital doğrulama teknolojilerinin kullanım durumları ve kullanıcıyı etkileyen faktörleri UTAUT2 yöntemiyle belirlenen ölçekler ile anket yapılarak ölçümlenecektir. Aynı zamanda kullanıcıların demografik yapısı da ölçümlenecektir. Araştırma kapsamında, vatandaşların bu teknolojileri benimseme ve kullanma niyetlerini belirleyen unsurlar üzerinde durulacaktır. Tez, dijital doğrulama teknolojilerinin kullanımını etkileyen faktörlerin çeşitliliğini ve etkilerini anlamak için literatür taraması, anket çalışmaları ve olası vaka analizleri gibi metodolojileri içermektedir.

### 1.2.3. Tezin Önemi

Günümüzde dijital dönüşüm, kamu hizmetlerinin sunumu ve erişimi açısından önemli bir evrime işaret etmektedir. Dijital doğrulama teknolojileri, bireylerin kimliklerini ve yetkilendirmelerini dijital platformlarda sağlamalarına imkan vermektedir. Bu tez, dijital doğrulama teknolojilerinin vatandaşlar tarafından kamu hizmetlerinde kullanımını etkileyen faktörleri incelemeyi amaçlamaktadır.

Bu tez, çeşitli boyutlardan dijital doğrulama teknolojilerinin vatandaşlar açısından önemini vurgular:

**Güvenlik:** Dijital kimlik doğrulama teknolojileri, kullanıcıların çevrimiçi platformlarda kimliklerini güvende tutmalarına ve kişisel bilgilerini korumalarına yardımcı olur. Bu, siber suçlarla mücadelede ve veri güvenliğinde önemli bir adımdır.

**Erişim Kolaylığı:** Dijital doğrulama teknolojileri, kamu hizmetlerine daha hızlı ve kolay bir erişim sağlar. Vatandaşlar, evlerinden veya mobil cihazlarından hizmetlere erişebilirler, bu da zaman ve kaynak tasarrufu sağlar.

**Verimlilik:** Dijital doğrulama teknolojileri, kamu hizmetlerinin verimliliğini artırabilir. Kimlik doğrulama süreçlerinin basitleştirilmesi, kamu kurumlarının iş yükünü azaltabilir ve hizmet sunumunu hızlandırabilir.

**Katılımın Artırılması:** Dijital doğrulama, çevrimiçi katılımı teşvik edebilir. Vatandaşlar, çeşitli hizmetlere daha rahat bir şekilde erişebildikleri için daha fazla katılım gösterebilirler.

Teknolojik Gelişme: Dijital doğrulama teknolojileri, teknoloji alanındaki ilerlemeleri teşvik eder. Bu tez, teknolojik gelişmelerin vatandaşların yaşam kalitesini nasıl iyileştirebileceğini araştırmaktadır.

Bu tez, dijital doğrulama teknolojilerinin vatandaşlar ve kamusal hizmet sağlayıcıları üzerindeki etkilerini anlamak için bir temel sağlamayı amaçlamaktadır. Bu anlayış, dijital kimlik doğrulamanın daha yaygın ve verimli bir şekilde kullanılması için stratejiler geliştirmek ve kamu hizmetlerini iyileştirmek için önemli bir adım olabilir.



## 2. LİTERATÜR

### 2.1. Kamuda Dijital Doğrulama

#### 2.1.1. Dijital Devlet Kavramı

Bilgiyi yönetme kabiliyetinin, otorite yapılarını güçlendirerek, modern devletlerin oluşumunda ve dönüşümünde önemli bir yeri olduğu bilinmektedir (Black, 2014). Aynı zamanda bilginin güvenliği sağlamak da olmazsa olmaz gereksinimlerdenidir. Sokağa çıktığında güvenliğinin polis tarafından sağlandığını düşünen vatandaşa, aynı şekilde siber güvenliğinin sağlandığını güvence altına almak gerekmektedir.

Kullanıcılar artık sadece dijital kanallardan hizmet almakla yetinmiyor; tüm kanallarda dijital hizmet talep ediyorlar. Alışkanlıklar henüz tam anlamıyla değişmemekle beraber, kullanıcılar (örneğin; banka işlemleri için) dijital kanaldan hizmet alabilir ancak bir insan ile görüşmesi gerekiyorsa onunla da görüşebilmelidir. 2000 kişinin katıldığı bir ankete göre kullanıcılar dijital devletten beklentilerini şöyle açıklıyor; %75 ‘i devlet ve finansal işlemlerine güvenli erişmek istiyor ama güvensiz hissediyor, %65 ‘i kişisel bilgilerinin saklanması ve güvenliğinden endişe duyuyor, %70 ‘i daha dijital, daha güvenli istiyor ama paylaşıırken ben de işin içinde olayım bunu başkası yapmasın diyor (Baheer vd., 2020).

Tüm bilgileri, kişinin kendisi tarafından yönetilebiliyor ve istediği her yerde kullanılabilir olmalıdır. Fiziksel kimlik, genellikle yüz yüze işlemleri desteklemek üzere tasarlanırken, dijital kimlik, kullanıcılar için gelişmiş fonksiyonlar sunmak ve dijital ortamlardaki işlemler için optimize edilmiştir (Web 4, 2016). Böyle bir durumda kimliği; seyahatlerde, aşı kartı, vatandaşlık hizmeti vs. işlemlerde kullanabiliriz.

Doğrulanabilir veriyi bir cüzdanda taşıyabilir, o cüzdanı veri sahibi olarak yine sadece biz açabiliriz. Yalnızca doktorun kişinin belirlediği kadar bir sürede sağlık verilerine ulaşabilmesi, eğitim ve diploma verileri, eğitim sertifika doğrulamaları, vize başvurusunda evrak doğrulamaları gibi kısa süreli işlemleri yalnızca belirli kişilerin görebileceği düzeyde açılabilmesi bu konuda örnek çalışmalar olabilir.

### 2.1.2. Dijital Doğrulama Teknolojilerinin AB Ülkelerinde Kullanımı

Covid-19 salgınıyla birlikte, kamu hizmetlerinde dijitalleşme eğilimi hızlanarak devam etmiş olup, Türkiye ve diğer ülkelerde, mevcut sağlık acil durumlarına yanıt olarak özel Covid-19 bilgi portalları, tıbbi ürünlerin tedariki için e-hizmetler, sanal tıbbi randevular, kendi kendine teşhis uygulamaları ve sokağa çıkma yasakları için e-izinler gibi yeni araçlar uygulanmıştır (Çaptuğ, 2021).

2021 yılı raporu, dijital çağda Üye Devletlerin temel hakların korunmasıyla ilgili karşılaştıkları zorluklara ve en iyi uygulamalara odaklanmıştır (Web 2, 2021). İnsanlara tanıdığı en büyük hak sınır özgürlüğü olan Avrupa Birliği, kuruluşu itibarıyla sınırsız olmalı. Ancak sınırdan geçerken ki özgürlük bankada hesap açarken doğrulama işlemleri esnasında bu şekilde özgür olmayacaktır. Polonya ‘da aldığınız üniversite diplomasını Almanya ‘da beyan etmeniz gerektiğinde bu tek cüzdanda çözülebilir. Amaç kişilerin farklı farklı yerlerde birden fazla doğrulama işini yapabilmesidir.

İngiltere’de 2016’da kamu sektöründe özel kimlik tanımlayıcılarına başlanmış ve aynı zamanda özel sektör kuruluşlarına da uzanan online kayıtlar yoluyla kimlik doğrulama sistemlerine imkan sağlanmıştır (Web 3, 2019).

Avrupa Komisyonu, tüm Avrupalılar için güvenilir ve güvenli bir Dijital Kimlik önermektedir (Web 1, 2021). Bu kimlik bilgilerine dijital cüzdanlardan erişilebilir ve herkes mobil cihazlarından erişebilir. Bu da herhangi bir AB vatandaşına veya işletmesine kimliklerini veya haklarını hızlı ve güvenilir bir şekilde kanıtlama yeteneği verecektir. Bu, kamu ve özel sektör hizmetlerine çevrimiçi olarak erişmeyi veya basitçe işlem yapmayı çok daha kolay hale getirecektir. Daha önce karmaşık ve zaman alıcı süreçler basit ve hızlı hale gelecektir.

Kullanım durumları şunları içerebilir:

- Doğum belgesi, tıbbi kayıt veya tapu kaydı gibi kamuya açık bir kayda erişim talep etme
- Bir müşteriyi dijital bir hizmete alma
- Bir iş sözleşmesi imzalama
- Banka hesabı açma
- Vergi beyannamesi verme

- Türkiye'nin herhangi bir yerindeki bir üniversiteye başvurmak AB
- Tıbbi reçete talep etmek
- Yaşı kanıtlamak
- Araba kiralamak veya şirket arabası filo sözleşmesine kaydolmak
- Otele giriş yapmak.

### **2.1.3. Dijital Kimlik ve Kimlik Doğrulamanın Kabul Edilmesi Neden Zor?**

Kimsiniz ve bunu nasıl kanıtlayabilirsiniz? Bunlar basit sorular. Ancak iki taraf birbiriyle işlem yaparken son derece önemli hale gelirler.

Fiziksel dünyada belirli kimlik belgeleri bulunurken, dijital varlıkların güvenli kimliği için benzer bir sistem yoktur (Shrier, Wu, ve Pentland, 2016, s. 5).

Paylaşım ekonomisi geliştikçe dijital işlemlerin sayısı da arttı. Bununla birlikte, paydaşlar, sahte bir belgeden orijinali tanımak için eğitilmemiştir. Sağlam ve kullanımı kolay bir dijital kimlik çözümüne ihtiyaçları var.

Peki dijital 'kimlik doğrulama' süreci şimdi nasıl görünüyor? Şu anda, çoğu yöntem üç faktörün bir kombinasyonunu kullanır:

- Müşterinin bildiği bir şey (PIN veya şifre)
- Müşterinin sahip olduğu bir şey (telefon, dongle)
- Müşterinin olan bir şey (parmak izi, retina, yüz)
- Bunlar iyi yöntemler, ancak ilk iki kategoriye duyulan bir güven sarsıcı olabilir. Ne yazık ki, suçluların şifreleri çalması oldukça kolaydır.

### **2.1.4. Dijital Doğrulama Vatandaşa ve Devlete Ne Sağlar?**

McKinsey (2014) 'e göre devletlerin dijitalleşmesi küresel ekonomiye yıllık 1 trilyon dolar civarında tasarruf sağlayacaktır.

Dijitalleşmenin devlete de birçok fayda getireceği tartışılmaz bir gerçektir. Bu yüzden bu dönüşüm süreci çok köklü bir değişikliği beraberinde getirmektedir. Dijital devlet uygulamaları her düzeyden vatandaşın yönetim süreçlerine katılımını sağlar. İşlem süreleri kısalmış, yolsuzluk azalmış. Vatandaşın yönetim süreçlerinde yer alması vatandaş

ve devlet arasındaki etkileşimi güçlendirir (Yıldırım ve Öner, 2004). Bilgiye ulaşmanın kolaylaşmasıyla vatandaşın özgüveni de artacak, yönetim sürecine daha aktif katılımı sağlanabilecek, etkin bireylerin oluşmasında ve süreçte daha fazla rol almasını sağlayacaktır (Çetinkaya, 2017).

### **2.1.5. Dijital Kimlik Cüzdanı ve Faydaları**

Cüzdan, işletmelerin kendi işyerlerindeki günlük aktivitelerini iyileştirmelerine yardımcı olacaktır. Örneğin; İK departmanları, bir iş adayının kimliğini hızlı bir şekilde doğrulayabilecek ve başvurularını desteklemek için gönderdikleri tüm belgeleri doğrulayabilecektir. Ayrıca cüzdan uygulamasına maaş bordrosu da ekleyebileceklerdir.

ID2020'de, dijital kimliklerin insan haklarına, temel hizmetlere, ekonomik fırsatlara, ihtiyaç sahiplerine destek ve cinsiyet eşitliği gibi konularda kritik olduğu vurgulanmıştır (Web 4, 2016).

Dijital kimliğin yalnızca öznitelik paylaşımını etkinleştirmez. Ayrıca dijital imzaları da destekler. Cüzdan, iş sözleşmelerini ve yasal izinleri dijital olarak imzalamak için kullanılabilir. Bu, satın alma ve tedarik ekiplerinin işini çok daha kolay hale getirecektir.

### **2.1.6. Pratikte AB Dijital Kimlik Cüzdanı: Vatandaşlar**

2021 yılının Haziran ayında Avrupa Birliği, Avrupa çapında bir Dijital Kimlik için bir çerçeve önerdiğinde, şimdiye kadarki en büyük dijital kimlik projelerinden birine doğru bir adım attı. Vatandaşlar, ilk kez telefonlarından Avrupa'nın herhangi bir bölgesindeki hizmetlere erişmelerini sağlayacak bir Avrupa Dijital Kimlik cüzdanı kullanabilecekler.

Estonya, kamu ve özel ağların verimliliğini artırmanın yanı sıra, "konumdan bağımsız olarak işletme yönetmeyi hedefleyen herkes için kullanılabilir uluslararası dijital kimlik" sunmayı amaçlamaktadır (Sullivan ve Burger 2017, s.470).

### **2.1.7. Dijital Kimliklerin Güven Sorunu**

Vatandaşın kullanımını artırmak için, kamu veya özel sektördeki güvenilir aktörler, kimliklerimizin yeterli ve güvenli bir şekilde ele alınmasını sağlamalıdır. Kimlik geliştiriciler, kişisel verilerin KVKK ve GDPR ile korunmasını sağlamak, vatandaşlarının her birinin dijital kimliğini korumayı ve güvenceye almayı amaçlamalıdır.

Kimlik doğrulama sistemleri, güvenliğini artırarak dijital ortamda güvenilir bir deneyim sunar ve kullanıcıların çevrimiçi etkinliklerini daha güvenli hale getirir. Kimlik doğrulama faktörleri, güvenliğini artırarak siber saldırıları azaltmayı ve veri kaybını en aza indirmeyi hedefler (Gündüz ve Yazıcı, 2020).

## **2.2. Literatür Araştırması**

### **2.2.1. E-Vatandaşlık (Estonya Örneği)**

Dünyada, dijital devlet ve e-vatandaşlık hizmetleri denildiğinde akla ilk gelen örneklerden biri Estonya 'dır. 1990 yılında Sovyetler Birliği döneminden bu yana, dünya ekonomisinde önemli bir rolü vardır.

Estonya, hem teknoloji hem de kurduğu yönetim altyapısı ile güveni kazanmıştır. Tüzel ve gerçek kişiler dahil bu hizmetleri kamuya sunmuştur.

Estonya'nın başarısı uluslararası alanda dikkat çekti ve deneyim paylaşımı için E-yönetişim akademisini kurdu (Nielsen, 2017, s.300). Estonya'da, dijital kimlik kullanarak dijital imzalama işlemleri gerçekleştirilebilir. Kimlik kartı ve özel bir yazılım sayesinde belge dijital olarak imzalanabilir. Estonya'da dijital imza, resmi ya da özel işlerde kullanılabilen ıslak imza niteliğindedir.

Kimlik doğrulama ve dijital imzanın güvenliği, Kamu Anahtar Altyapısı tarafından güvence altına alınır (Parsovs, 2020, s.1785). Estonya'da dosyaların %95'i dijital olarak imzalanırken, vergi mükelleflerinin %96'sı vergilerini elektronik olarak beyan etmekte, banka işlemlerinin %99,6'sı çevrimiçi yapılırken, 2015 parlamento seçimlerinde %33'e varan oranda e-oy kullanılmıştır (Aydın, 2021, s. 2).

Estonya, yabancılara sunduğu e-Kimlikle dünyanın herhangi bir yerinden Estonya vatandaşı gibi e-hizmetlerden faydalanma olanağı sağlar. Bu hizmetler arasında şirket

kurma ve yönetme, anlaşma imzalama, ödeme yapma, bankacılık gibi işlemlerin yasal çerçevesini güvence altına alır. E-vatandaşlık politikası, yabancı uzmanların Estonya'da çalışabilmesi için ikamet zorunluluğunu ortadan kaldırmakla kalmaz, aynı zamanda iş kurma olanağını da içerir.

Estonya sadece kendi vatandaşlarına değil, dünyadaki herkese dijital kimlik uygulamasında hak tanımaktadır. Dijital vatandaşlık web sitesinden belirttiği üzere bilişim teknolojilerini konum sınırını ortadan kaldırma vizyonu ile yola çıkmıştır (Koç, 2021).

### **2.2.2. E-Belediyecilik**

Birleşmiş milletlere göre devlet yönetimine dair 8 ‘doğru’ ilke: Hukukun egemenliği, şeffaflık, cevaplanabilirlik, fikir birliğine dayanma, eşitlikçilik ve kapsayıcılık, etkililik, verimlilik ve güvenilebilirlik şeklindedir.

Devletlerin sağladığı, sunduğu ve işlerliğini sağladığı dijital kimlik yapısı, otoritelerin gücünü bireylere eşit sunması ile ilkelerin varlığını ortaya koymaktadır.

Kamuda bürokrasinin beraberinde getirdiği süreç yavaşlığını ve kağıtsızlaşmayı en aza indirmeyi amaçlayan dijital bir belediyecilik sistemi oluşturulmaktadır.

Bireysel tabanda dijital ID, dünyadaki ekonomik ikili ilişkiden dışlanan 1.7 milyar kişiyi potansiyel olarak ekonomiye katabilir. Kurumsal tabanda, dijital ID, mesafeli satış ilişkisi tabanında güvenlik sunar. Ticaret faaliyetlerindeki insan hatalarını süreçlerden arındırarak kayıpları azaltmaya yardımcı olur. Verimlilik artışı, zaman kayıplarında azalma ve hızlı teslimat gibi faydaları mevcut ekonomik akışlara ekleyebilir ve faydaları her bir süreç içinde sinerji yaratır.

Dijital belediyeciliğe geçişte birimlerin dönüşümü, hedeflerin belirlenmesi ve uygulanacak politikaların planlanması, dijital belediyecilik hedeflerine ulaşmayı kolaylaştırır (Şahin, 2007). Devletler, artan bir şekilde vatandaşların işlemlerini online olarak tamamlayacakları bir sisteme doğru yol almaktadırlar. Örnek olarak, en gelişmiş kamu internet sitelerinden birisine sahip olan Washington eyaletinde web kullanıcıları, gelir ve kurumlar vergilerini (dijital doğrulama teknolojilerini kullanarak) ödeyebilmekte; iş, işsizlik sigortası veya okul başvurusu yapabilmekte; doğum, ölüm, boşanma belgeleri isteyebilmekte; sabıka kaydı elde edebilmektedirler (Gül, 2002).

### 2.2.3. Dijital Doğrulama ile Ödeme Sistemleri

Mobil ödemenin kullanılan 2 farklı formu vardır; Yakından mobil ödeme, uzaktan mobil ödeme. Yakından mobil ödeme, tüketicilerin cep telefonlarını kullanarak satış noktasında doğrudan mal ve hizmet satın almasını sağlayan temassız, yakın alan iletişimine (NFC) dayanır. Tüketiciler cep telefonlarını okuyucularına yakın tutarak ödeme yapabilirler ve ön ödemeli hesapları, mobil hesapları veya banka hesapları buna göre düşülecektir. Doğrudan mobil hesaptan kesinti yapar veya diğer uygulamaları veya İnternet'i kullanarak banka kartları, kredi kartları veya Alipay veya PayPal gibi üçüncü taraf ödemeleri yoluyla ödeme yapar (Liu, 2015).

Yakın alan iletişimi (NFC) mobil ödeme sistemleri müşterilerin akıllı telefonlarını nakit veya manyetik şeritli kartlar yerine fiziksel noktadaki ödemeler için kullanmalarını sağlar. İşlem değeri ülkeye özgü bir eşiğin altında olduğu sürece, NFC özellikli bir cihazı bir satış noktasında (POS) bir satıcının NFC terminaline 10 cm veya daha az bir mesafeye yerleştirerek ödemeleri tetikler (Gerpott ve Meinert, 2017). NFC ile bu özelliği taşıyan telefonlardan ödeme yapılabileceği gibi yüzük ve bileklik gibi cihazlara da bu özellik yüklenerek ödeme yapılabilmektedir. Telefondaki dijital cüzdan bu cihaz ile eşleştirilmektedir. NFC cihazları daha yüksek bir güvenlik düzeyine sahiptir çünkü hem haberleşmeleri sağlamak hem de ortadaki adam saldırılarını gerçekleştirmek imkansız olmasa da daha zordur. Son yıllarda, NFC teknolojisi, temassız mobil ödeme hizmetleri için giderek daha fazla bir çözüm olarak kabul edilmektedir (Luo vd., 2016).

### 2.2.4. Dijital Cüzdan

Dijital cüzdan; kullanıcısının, doğrulayabileceği her türlü belgeyi (kredi kartı, banka kartı, kimlik kartı, diploma vb.) ve bilgilerini güvenli bir şekilde saklama ve kullanabilme özelliğine sahip elektronik bir cüzdandır. Dijital Cüzdan ile para yüklenebilir, ödemeler online ve QR kod ile yapılabilir. Doğrulayıcı nitelikli cihazlar ve uygulamalar ile de ödeme yapılabilir.

Kişilerin bilgi güvenliğini sağlamak ve çeşitli cihazlara veya platformlara güvenli erişimini sağlamak için geliştirilmiş bazı kimlik doğrulama sistemleri, kullanıcıların kişisel verilerini veya diğer önemli verileri yetkisiz erişimlerden korur (Kayrancıoğlu, 2019). Kayrancıoğlu'nun (2019) belirttiği gibi, bilgi güvenliğini sağlamak amacıyla

geliştirilen kimlik doğrulama sistemleri, kullanıcıların çeşitli cihazlara veya platformlara güvenli bir şekilde erişmelerine izin verir. Bu sistemler aynı zamanda kullanıcıların kişisel verilerini ve diğer önemli bilgilerini yetkisiz erişimlerden korur. Bu, dijital ortamdaki güvenlik açıklarını minimize etmek ve kullanıcıların dijital varlıklarını korumak için önemli bir adımdır.

### **2.2.5. Vatandaşlar Gözünden Doğrulama Teknolojileri**

Dijital vatandaşlık, dijital teknolojilerle kendinden emin ve olumlu bir etkileşimi ifade eder. Dijital vatandaşlık eğitimi, öğrencilerin dijital okuryazarlığı elde etmelerine ve anlamalarına yardımcı olmanın yanı sıra çevrimiçi güvenlik, siber güvenlik, dijital sorumluluk ve dijital sağlık ve esenliği sağlamak için gereklidir.

Dijital vatandaşlığın 9 boyutu şöyle tanımlanmaktadır:

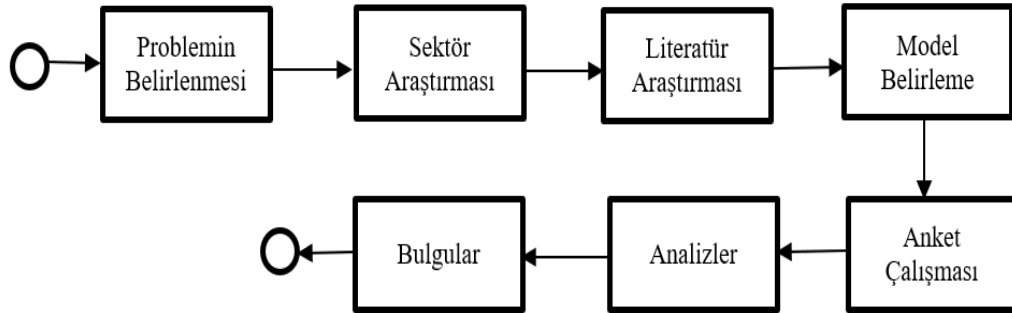
1. Dijital erişim.
2. Dijital ticaret.
3. Dijital iletişim.
4. Dijital okuryazarlık.
5. Dijital etik.
6. Dijital kanun.
7. Dijital hak ve sorumluluklar.
8. Dijital sağlık
9. Dijital güvenlik

Dünyanın birçok noktasından dijital teknolojilerin kullanılabilirliği olması, bütün dünya vatandaşlarının eşit hak ve sorumluluklara sahip birer dijital vatandaş olabileceğini göstermektedir. Coğrafi sınırlara bağlı bir vatandaşlık algısının küreselleşmeyle ortadan kalkması, aynı dijital platformların tüm dünya vatandaşları tarafından kullanılabilir hale gelmesi gibi sebepler, dijital vatandaşlık kavramının ortaya çıkmasını neden olmuştur (Çubukçu ve Bayzan 2013).

### 3. METOT

#### 3.1. Tez Yazımında Kullanılan Metodoloji

Bu çalışmada, problem belirlendikten sonra ilk olarak dijital doğrulama teknolojilerinin kamudaki konumu incelenmiştir. Sonrasında literatür çalışması yapılmış, doğrulama teknolojilerini türleri incelenmiştir. Uygulamaların kullanıcılara etki eden yöntemlerinin araştırılmasında daha çok teknoloji kabul modeli kullanıldığı görülmüştür. Bu modelin en güncel girdileri ele alınmıştır. Farklı yaş, gelir ve çalışma durumundan 208 kişilik katılımcı grubuyla anket çalışması yapılmıştır. Anket yöntemiyle toplanan verileri analiz etmek ve sonuçları ortaya çıkarmak amacıyla araştırma sorusuna dair değerlendirmeler ortaya koyulmaya çalışılmıştır. Anket yöntemi, genellikle araştırma yapmak veya belirli bir konu hakkında insanların görüşlerini, tercihlerini veya deneyimlerini ölçmek için kullanılan bir veri toplama yöntemidir. Anket çalışmasının sonuçları istatistiki programlarla incelenmiş ve doğrulama teknolojilerini kullanımı etkileyen faktörler ve aralarındaki ilişki tespit edilmiştir.



Şekil 3.1: İzlenen yol.

### **3.2. Katılımcıların Belirlenmesi**

Dijital doğrulama teknolojilerinin vatandaşlar tarafından kullanımını etkileyen faktörler konusunda yapılan anket çalışmasında katılımcıları belirlerken, öncelikle hedef kitlenin belirlenmesi kritiktir. Bu kitle, farklı yaş grupları, eğitim seviyeleri, gelir düzeyleri ve dijital beceri düzeyleri gibi faktörlere göre segmentlere ayrılabilir. Ardından, örnekleme yöntemleriyle bu segmentlerden temsilci bir örneklem seçilir. Anket katılımcılarının belirlenmesinde, teknolojiye olan ilgi düzeyi, güvenlik endişeleri, dijital yaşam alışkanlıkları gibi faktörler dikkate alınmıştır. Anketin doğru hedef kitleye ulaşması, elde edilen verilerin güvenilirliği ve sonuçların geçerliliği açısından son derece önemlidir.

### **3.3. Verilerin Toplanması**

Anketler, veri toplamının etkili ve yaygın bir yöntemidir çünkü birçok farklı alanda kullanılabilirler ve çeşitli bilgi türlerini elde etmek için esnek bir araç sağlar. Birçok farklı anket yöntemi bulunmaktadır. Bu çalışmada internet üzerinden anket yöntemiyle veri toplanmıştır. Toplam 38 soruluk 6 faktörden oluşan bir anket oluşturulmuş, dijital form şeklinde toplanmıştır. 208 kişinin doldurduğu bu anketler SPSS istatistik programları kullanılarak analiz edilmiştir.

### **3.4. Verilerin Analizi**

İlk adım olarak veri setinin yapısını ve temel özelliklerini anlamak için tanımlayıcı istatistikler uygulanmıştır. Bu, veri setindeki değişkenlerin merkezi eğilim (ortalama, medyan), dağılım (standart sapma, varyans) ve diğer özelliklerini incelemeyi içermektedir. Araştırma hipotezleri Yapısal Eşitlik Modeli tekniği aracılığıyla AMOS uygulaması kullanılarak test edilmiştir. Analizler sonucunda elde edilen bulguların anlamlılığı ve önemi değerlendirilmiştir.

### 3.5. Araştırmada Kullanılan Ölçek Referansları

**Tablo 3.1:** Ölçek referansları.

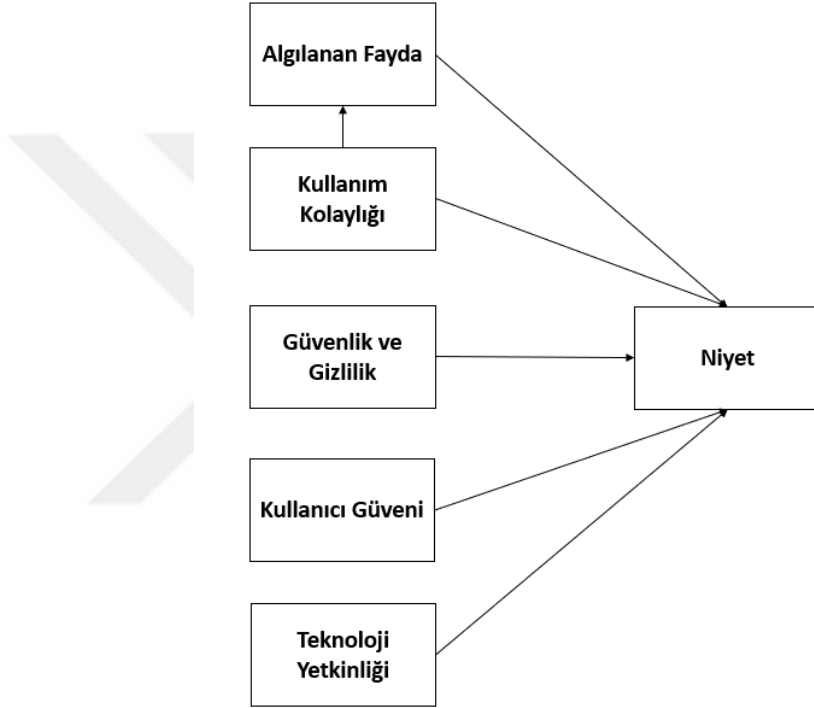
| Değişkenler                      | Ölçek Referansları      | İfadeler                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Niyet (N)</b>                 | Yılmaz ve Kavanoz, 2017 | 1.Dijital doğrulama teknolojisi araç ve ortamlarını bol bol değerlendirmeye devam etmeyi planlıyorum.<br>2.Gelecekteki dijital doğrulama teknolojileri gereksinimleri için başka doğrulama teknolojisi araç ve ortamlarını araştıracağım.<br>3.İleride başka doğrulama teknolojisi araç ve ortamlarını kullanmaya devam etmek niyetindeyim.                                                                                                                                                                                                                     |
|                                  | Can, 2019               | 4.Hayatımda dijital doğrulama teknolojilerini sürekli kullanmayı düşünüyorum.<br>5.Başkalarına da dijital doğrulama teknolojilerini kullanmalarını tavsiye edeceğim.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Kullanım Kolaylığı (KK)</b>   | Ursavaş, vd., 2014      | 1.Kamu hizmetlerinde dijital doğrulama teknolojilerini kullanmak benim için kolaydır.<br>2.Dijital doğrulama teknolojileri kullanımı benim için kolaydır.<br>3.Kamu hizmetlerinde dijital doğrulama teknolojilerini kullanabilecek beceriye sahip olmak benim için kolaydır.                                                                                                                                                                                                                                                                                    |
|                                  | Can, 2019               | 4.Dijital doğrulama teknolojilerinin kullanımını öğrenmek benim için kolaydır.<br>5.Dijital doğrulama teknolojilerini kullanmak zihinsel çaba gerektirmez.<br>6.Dijital doğrulama teknolojileri açık ve anlaşılırdır.                                                                                                                                                                                                                                                                                                                                           |
| <b>Güvenlik ve Gizlilik (GG)</b> | Sevinç, 2021            | 1.Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.<br>2.Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.<br>3.Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.                                                                                                                                                                                                                                                                                  |
|                                  | Aka, 2023               | 4.Dijital doğrulama teknolojileri, çevrimiçi faaliyetlerim hakkındaki bilgilerin diğer taraflarla (3.shahıslarla) paylaşılmayacağına dair bana güvence verir.<br>5.Dijital doğrulama teknolojileri, hakkımdaki bilgileri korur.<br>6.Dijital doğrulama teknolojileri, kişisel bilgilerimi başka sitelerle paylaşmaz.                                                                                                                                                                                                                                            |
| <b>Algılanan Fayda (AF)</b>      | Alkan, 2020             | 1.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanarak işlemlerimi daha hızlı gerçekleştirebilirim.<br>2.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmam işlem performansımı artırır.<br>3.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmam işlemlerdeki etkinliğimi artırır.<br>4.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmak işlemleri daha kolay gerçekleştirmemi sağlar.<br>5.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmak faydalıdır. |

**Tablo 3.1:** devam.

|                                          |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kullanıcı<br/>Güveni<br/>(KG)</b>     | Alkan,<br>2020 | 1.Dijital doğrulama teknolojileri kullanılarak kamu hizmetleri işlemleri yapmak güvenli olacaktır.<br>2.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmada kişisel bilgilerin saklanması önemlidir.<br>3.Dijital doğrulama teknolojileri kullanarak kamu hizmetleri işlemleri yapmada güvenlik önemlidir.<br>4.Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri verilerine hiç kimsenin izinsiz erişim sağlamaması benim için önemlidir.                                                                                                                                                                                                             |
| <b>Teknoloji<br/>Yetkinliği<br/>(TY)</b> | Ünsal,<br>2021 | 1.Yeni bilgi-iletişim teknolojilerini olumlu buluyorum.<br>2.Teknolojik yenilikleri kolay benimserim.<br>3.Yeni teknolojilere kolaylıkla uyum sağlarım.<br>4.Teknolojiye anadilim gibi hakimim.<br>5.Son çıkan teknolojik cihazlara sahip olmak benim için önemlidir.<br>6.Çevrimiçi olarak paylaştıklarım yaşamımın önemli bir kısmını yansıttıyor.<br>7.Bence çevrimiçi iletişim yüz yüze iletişimin yerini tutar.<br>8.Günün her anında çevrimiçi olmaktan memnunum.<br>9.Not alırken el yazısıyla yazmaktansa bilgisayara ya da telefona not almayı tercih ederim.<br>10.Bir şeyi İnternet üzerinden satın aldıysam mutlaka çıktısını da saklarım.<br>(Örneğin fatura, bilet vb.) |

## 4. HİPOTEZLER

Aşağıdaki Şekil 4.1.'de dijital doğrulama teknolojilerinin vatandaşlar tarafından kullanımını etkileyen model girdileri gösterilmektedir. Modelde 2 bağımlı ve 3 bağımsız olmak üzere 5 faktör bulunmaktadır. Bağımlı değişkenler: algılanan fayda ve niyettir. Bağımsız değişkenler ise: kullanım kolaylığı, gizlilik ve güvenlik, kullanıcı güveni, teknoloji yetkinliğidir.



**Şekil 4.1:** UTAUT2 model dijital doğrulama teknolojileri kullanımı değişkenleri.

### 4.1. Teknoloji Kabul Modeli

UTAUT birleşik kabul ve teknoloji kullanımı teorisidir. Bir bilgi teknolojisinin kullanıcı benimseme davranışı üzerindeki etkisini ölçmek için kullanılır (Venkatesh vd., 2003). Günümüzün dijital dünyasında, vatandaşlar ve kamu hizmeti sağlayıcıları arasındaki etkileşimlerde teknolojik yeniliklerin benimsenmesi ve kullanılması giderek daha büyük bir önem kazanmaktadır. Bu bağlamda, dijital doğrulama teknolojileri, vatandaşların kamu hizmetlerine erişimlerini ve kullanımlarını kolaylaştırmak, veri güvenliğini sağlamak ve etkili bir şekilde kimlik doğrulamak

amacıyla yaygın olarak kullanılmaktadır. Ancak, bu teknolojilerin vatandaşlar tarafından kabul edilmesi ve kullanılması, bir dizi karmaşık faktörden etkilenebilir. Bu çalışma, bu faktörleri incelemek ve dijital doğrulama teknolojilerinin vatandaşlar tarafından kamu hizmetlerinde kullanımını etkileyen etmenleri anlamak amacıyla Teknoloji Kabul Modeli' ni (Technology Acceptance Model - TAM) temel alır. Bu çalışma, TAM' ı temel alarak, vatandaşların dijital doğrulama teknolojilerini kabul etme niyetlerini etkileyen faktörleri analiz ederek, kamu hizmetlerinde bu teknolojilerin daha geniş kullanımını teşvik etme hedefini taşımaktadır. Bu nedenle, teknoloji kabulünün ölçülmesi ve faktörlerin etkilerinin anlaşılması, daha etkili kamusal hizmet sunumunu destekleyebilir ve vatandaşların daha iyi hizmetlere erişimini kolaylaştırabilir.

## **4.2. Teknoloji Kabul Modeli Girdileri**

### **4.2.1. Algılanan Fayda**

Algılanan fayda kavramı, ürün veya hizmetin sağladığı belirli işlevlerin veya özelliklerin kullanımı sonucunda, tüketicinin elde etmiş olduğu algılanan kazanç olarak belirtilmektedir (Park vd., 2011).

Algılanan kullanım kolaylığı ve algılanan fayda niyet üzerinde; niyet ise gerçekleşen davranış (İKBS kullanımı) üzerinde pozitif etkiye sahiptir (Aras vd.,2015).

Yukarıdaki tartışmaya dayanarak aşağıdaki hipotez ileri sürülmektedir:

H1: Vatandaşın dijital doğrulama teknolojilerinin kullanımına yönelik davranışının oluşmasında algılanan fayda, niyeti olumlu yönde etkilemektedir.

### **4.2.2. Kullanım Kolaylığı**

Teknoloji Kabul Modeli (TKM); Davis tarafından geliştirilen, kullanıcıların davranışlarını tahmin yoluyla bilgi sistemleri kabulünü etkileyen faktörleri açıklayan bir modeldir. Bu modelde algılanan fayda ve kullanım kolaylığının bilgi sistemleri kabul davranışı ile ilişkili olduğu varsayılmaktadır (Davis vd., 1989).

Algılanılan kullanılışlılık ve algılanan kullanım kolaylığı, bilgi teknolojilerinin kullanımı ve kabulünün açıklanmasında çok önemli bir rol oynamaktadır. Bu faktörler, bilgi sistemlerini kullanma açısından bireylerin niyetlerini oluşturan önemli faktörler olarak bilinmektedir. (Çelik vd., 2010: 36).

Yukarıdaki tartışmaya dayanarak aşağıdaki hipotez ileri sürülmektedir:

H2: Vatandaşın dijital doğrulama teknolojilerinin kullanımına yönelik davranışın oluşumunda kullanım kolaylığı, algılanan faydayı olumlu yönde etkilemektedir.

#### **4.2.3. Güvenlik ve Gizlilik**

Gizlilik veya mahremiyet, bir işlem sırasında müdahil olan taraflara ait bilgilerin, işlem verilerinin ya da yazışmaların konu dışındaki kişi veya kurumlardan saklı tutulması durumu olarak tanımlanabilir. Şahsi verilerin sağlandığı elektronik ve internet gibi sanal ortamlarda bulunan verilerin korunup korunmadığı inancını ifade etmektedir (Karakaya, 2014).

Tüketiciler, kredi kartı bilgisi ve diğer kişisel bilgilerin korunduğu güvenlik sistemlerine sahip işletmelerden daha çok alışveriş yapmak niyetinde olacaklardır (Kaplan ve Nieschwietz, 2003).

Yukarıdaki tartışmaya dayanarak aşağıdaki hipotez ileri sürülmektedir:

H3: Dijital doğrulama teknolojilerinin güvenliği ve gizliliği, kullanıcıların bu teknolojilere olan niyetini olumlu yönde etkilemektedir.

#### **4.2.4. Kullanıcı Güveni**

Tüketici güveni, “kişinin güvendiği bir değişim ortağına güvenme isteği” olarak tanımlanır. Bir teknolojiye, sisteme veya markaya tüketici güveni, etkili çalışma ilişkilerinin temel unsurlarından biri olarak kabul edilir (Cabrera-Sánchez vd., 2021). Mobil ödeme bağlamında, algılanan güven, mobil ödeme kullanıcılarının hizmetin güvenilir ve onu benimsemenin güvenli olduğuna ne ölçüde inandıkları anlamına gelir (Al-Saedi vd., 2020).

Min'nin (2003) araştırmasına göre İnternet şirketinde güvenliğin az olmasının müşterilerin satın alma niyetini olumsuz etkileyebileceği yönünde sonuçlanmıştır.

İnternet’te tüketicilerin davranışını ve satın alma niyetini 2 kategori: teknoloji ve güven etkilemektedir. Teknoloji; kolay kullanma, faydalılık ve sitenin ilgi çekici olması gibi parametrelerden oluşmaktadır. Güven; şirketin büyüklüğü, ünü, şirketin bilinirliği gibi parametrelerden oluşmaktadır. Heijden, Verhagen ve Creemers’in (2003) araştırmasında ilk olarak şirketin büyüklüğünden bahsetmektedir.

Yukarıdaki tartışmaya dayanarak aşağıdaki hipotez ileri sürülmektedir:

H4: Dijital doğrulama teknolojilerine olan kullanıcı güveni, onların bu teknolojilere olan niyetini olumlu yönde etkilemektedir.

#### **4.2.5. Teknoloji Yetkinliği**

Teknoloji yetkinliği, bireyin teknolojik araçları etkili bir şekilde kullanabilme ve bu araçları anlayabilme kabiliyetidir. Bu yetkinlik, dijital aletleri kullanarak bilgiye erişim, verimli iletişim kurma, sorunları çözme ve yaratıcı düşünme gibi becerileri içerir. Teknoloji yetkinliği, hızla değişen teknolojik ortamlarda adaptasyon ve öğrenme esnekliği gerektirir.

Yetkinlik, ilgi, bilinçli kullanım ve teknolojiye yaklaşım ile girişimcilik niyeti arasındaki ilişkinin olumlu çıkması, Z kuşağı bireylerinin girişimcilik açısından desteklenmesi gerektiğini gösteriyor (Cesur ve Köse, 2021).

Temel psikolojik ihtiyaçlardan yetkinlik, bireyin bir etkinliği gerçekleştirirken yetkinlik duygusunu hissetmek için çevresiyle etkili bir şekilde etkileşime girme niyeti ve uzmanlık hissi olarak ifade edilmektedir (Deci ve Ryan, 2000).

Yukarıdaki tartışmaya dayanarak aşağıdaki hipotez ileri sürülmektedir:

H5: Dijital doğrulama teknolojilerinde kullanıcıların teknoloji yetkinliği, bu teknolojilere olan niyetini olumlu yönde etkilemektedir.

## 5. BULGULAR

### 5.1. Demografik Veriler

#### 5.1.1. Yaş Göre Dijital Doğrulama Teknolojileri Kullanımı

Katılımcılar arasında 6 farklı yaş dağılım grubu oluşturuldu ve bu gruplardaki katılımcı sayıları Tablo 5.1 'de gösterilmiştir. Burada, yaşın dijital doğrulama teknolojileri kullanma niyetine etkisi gözlemlenmek istenmiştir. Tablo 5.1 'de görüldüğü gibi, yaş grupları arasında adetsel farklar olduğu fark edilmiştir.

**Tablo 5.1:** Yaş gruplarındaki kişi sayısı dağılımları.

| Yaş Grupları    | Kişi Sayısı | %  |
|-----------------|-------------|----|
| 18 yaş ve altı  | 7           | 3  |
| 18-25 yaş       | 33          | 16 |
| 26-34 yaş       | 45          | 22 |
| 35-44 yaş       | 29          | 14 |
| 45-54 yaş       | 19          | 9  |
| 55 yaş ve üzeri | 75          | 36 |

#### 5.1.2. Cinsiyete Göre Dijital Doğrulama Teknolojileri Kullanımı

Katılımcılar arasında 3 farklı cinsiyet grubu oluşturulmuş ve bu gruplardaki katılımcı sayıları Tablo 5.2 'de gösterilmiştir. Burada, cinsiyetin dijital doğrulama teknolojileri kullanma niyetine etkisi gözlemlenmek istenmiştir.

**Tablo 5.2:** Cinsiyet gruplarındaki kişi sayısı dağılımları.

| Cinsiyet      | Kişi Sayısı | %  |
|---------------|-------------|----|
| Kadın         | 74          | 36 |
| Erkek         | 130         | 62 |
| Belirtilmemiş | 4           | 2  |

### 5.1.3. Eğitim Durumuna Göre Dijital Doğrulama Teknolojileri Kullanımı

Katılımcılar arasında 5 farklı eğitim durumu grubu oluşturuldu ve bu gruptaki katılımcı sayıları Tablo 5.3 'te gösterildi. Burada, eğitimin durumunun dijital doğrulama teknolojileri kullanma niyetine etkisi gözlemlenmek istenmiştir.

**Tablo 5.3:** Eğitim durumu gruplarındaki kişi sayısı dağılımları.

| Eğitim Durumu                      | Kişi Sayısı | %  |
|------------------------------------|-------------|----|
| İlköğretim                         | 0           | 0  |
| Ortaöğretim                        | 0           | 0  |
| Lise                               | 13          | 6  |
| Üniversite (Önlisans-Lisans)       | 131         | 63 |
| Lisansüstü (Yüksek Lisans-Doktora) | 64          | 31 |

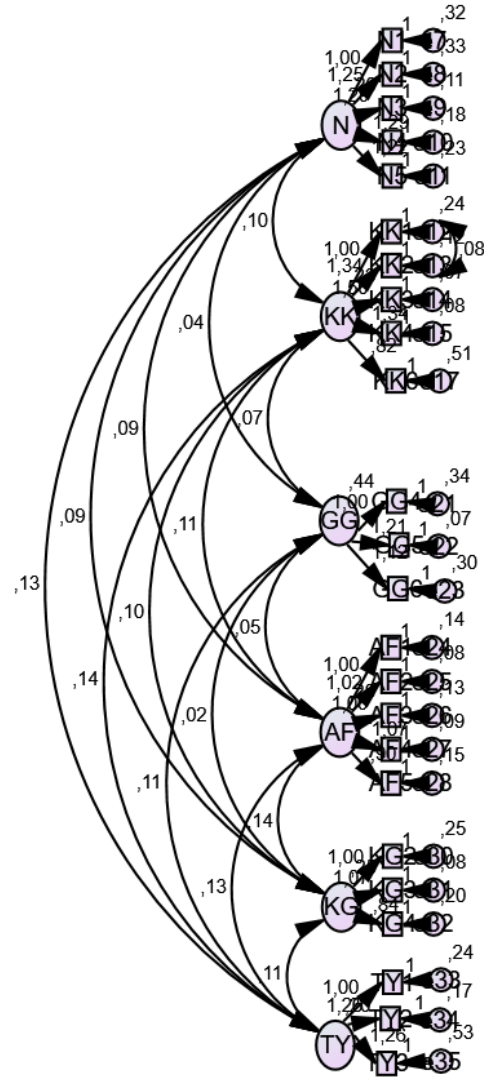
### 5.1.4. Çalışma Durumuna Göre Dijital Doğrulama Teknolojileri Kullanımı

Katılımcılar arasında 3 farklı çalışma durumu grubu oluşturuldu ve bu gruptaki katılımcı sayıları Tablo 5.4 'te gösterildi. Burada, çalışma durumunun dijital doğrulama teknolojileri kullanma niyetine etkisi gözlemlenmek istenmiştir.

**Tablo 5.4:** Çalışma durumu gruplarındaki kişi sayısı dağılımları.

| Çalışma Durumu | Kişi Sayısı | %  |
|----------------|-------------|----|
| Çalışan        | 58          | 38 |
| Çalışmayan     | 94          | 61 |
| Belirtilmemiş  | 1           | 1  |

## 5.2. Doğrulayıcı Faktör Analizi (CFA)



Şekil 5.1: Ölçüm (CFA) modeli.

Doğrulayıcı faktör analizi (CFA), ölçüm modeli olarak da bilinen, gizil değişkenler ile onlara bağlı ölçümler arasındaki ilişkiyi analiz eder. Diğer taraftan, yol analizi, yapısal model olarak da bilinen, belirtilen gizil değişkenler arasındaki ilişkiyi analiz eder. Şekil 5.1, çalışmanın yapısal modelini göstermektedir. Gizil yapılar arasındaki regresyon çizgilerindeki metrikler beta katsayılarıdır. Regresyon ağırlıklarının standartlaştırılmış formu olan beta katsayıları, sonuçları tartışmak için kullanılmıştır. Standartlaştırılmış katsayılar, tahmin edilen bir değişkenin, tahmin eden değişkenin bir standart sapma artışıyla ne kadar standart sapma değişeceğini gösterir.

CFA analizi sırasında, gizil yapıların ilgili gözlemlenen değişkenlere olan regresyon yollarının güçleri değerlendirildi. Tüm regresyon ağırlıkları  $p < 0.001$  düzeyinde istatistiksel olarak anlamlı bulundu.

**Tablo 5.5:** Standartlaştırılmış regresyon ağırlıkları.

|     |      |    | Tahmin |
|-----|------|----|--------|
| N1  | <--- | N  | ,622   |
| N2  | <--- | N  | ,703   |
| N3  | <--- | N  | ,869   |
| N4  | <--- | N  | ,806   |
| N5  | <--- | N  | ,757   |
| KK1 | <--- | KK | ,694   |
| KK2 | <--- | KK | ,879   |
| KK3 | <--- | KK | ,940   |
| KK4 | <--- | KK | ,913   |
| KK6 | <--- | KK | ,482   |
| GG4 | <--- | GG | ,753   |
| GG5 | <--- | GG | ,950   |
| GG6 | <--- | GG | ,808   |
| AF1 | <--- | AF | ,815   |
| AF2 | <--- | AF | ,884   |
| AF3 | <--- | AF | ,828   |
| AF4 | <--- | AF | ,881   |
| AF5 | <--- | AF | ,773   |
| KG2 | <--- | KG | ,708   |
| KG3 | <--- | KG | ,888   |
| KG4 | <--- | KG | ,682   |
| TY1 | <--- | TY | ,679   |
| TY2 | <--- | TY | ,807   |
| TY3 | <--- | TY | ,613   |

**Tablo 5.6:** Model uyum metrikleri.

| Ölçüm | Tahmin  | Eşik | Tercüme |
|-------|---------|------|---------|
| CMIN  | 492,050 | --   | --      |
| DF    | 236     | --   | --      |

**Tablo 5.6:** devam.

|         |       |                 |                  |
|---------|-------|-----------------|------------------|
| CMIN/DF | 2,085 | 1 ve 3 arasında | Harika           |
| CFI     | 0,920 | >0.95           | Kabul Edilebilir |
| SRMR    | 0,068 | <0.08           | Harika           |
| RMSEA   | 0,072 | <0.06           | Kabul Edilebilir |

CFA modelin uygunluğunu belirlemek için kullanılabilecek birkaç model uyum ölçütü bulunmaktadır. Yaygın olarak kullanılan ölçütler CMIN/DF, Karşılaştırmalı Uyum İndeksi (CFI) ve ortalama kare kök hatası (RMSEA) gibi metriklerdir. Tablo 5.6, bu metrikler için önerilen eşik değerleri (Hu ve Bentler, 1999; Hair vd., 2010) ve önerilen modelin uygunluk istatistiklerini sağlamaktadır. CMIN/DF, CFI ve RMSEA metrikleri göz önüne alındığında, önerilen modelin iyi bir uyum sağlayan bir model olduğu sonucuna varılabilir.

Girdilerin birbiri ile uyumları Tablo 5.6 'da verilmiştir. CMIN/DF değeri 5'in altında 2,08 olarak gerçekleşmiş, e RMSEA değeri ise 0,08'e yakın olarak gerçekleşmiştir. P değerlerinin anlamsız olması ve uyum indekslerinin kabul edilebilir düzeyde olması durumunda, anket çalışmanızın model kurmaya uygun olduğunu söyleyebiliriz.

Yapısal model için model uyum ölçütleri Tablo 5.6 'da verilmiştir. CMIN/DF, CFI ve RMSEA metriklerinin değerleri, önerilen yapısal modelin iyi uyum sağlayan bir model olduğunu göstermiştir.

### **5.2.1. Verilerin Normallik Testi**

Toplanan anket sonuçlarının analizi için, ölçütlerin normal dağılıma uyup uymadığının kontrol edilmesi gerekmektedir. Normal dağılıma uymayan, anketteki bazı girdiler çıkartılarak normalleşmesi sağlanarak veya yapılacak istatistiki analizler verilerin normal dağılmadığı varsayılarak yapılır. Yapısal Eşitlik Modellemesinin temel varsayımlarından biri çok değişkenli normalitedir. Normalite varsayımını değerlendirmek için her bir öge için yeniden ölçeklendirilmiş standartlaştırılmış basıklık değerleri incelendi. Verilerimiz bir anket çalışması sonucu elde edilmiş olup,

SPPS istatistik yazılımı ile normallik analizini yaptığımızda en önemli bölüm basıklık ve çarpıklık değerlerinin kontrol edilmesidir. Yeniden ölçeklendirilmiş çarpıklık değerleri için önerilen eşik değer  $\pm 2$ 'dir. Tablo 5.7, tüm ögelerin yeniden ölçeklendirilmiş basıklık değerlerinin 2'den küçük olduğunu göstermektedir. Basıklık değerlerine dayanarak, çalışma verilerinin normalite ihlali göstermediği sonucuna varılabilir. Bu değerlerin  $+2.0-2.0$  aralığında olması normal dağılıma uyduğunu göstermektedir.

**Tablo 5.7:** Verilerin normallik testi.

| Değişken | Min   | Maks  | Eğrilik | C.R.   | Basıklık | C.R.   |
|----------|-------|-------|---------|--------|----------|--------|
| TY3      | 1,000 | 5,000 | ,002    | ,010   | -,365    | -1,076 |
| TY2      | 2,000 | 5,000 | -,764   | -4,497 | 1,067    | 3,141  |
| TY1      | 1,000 | 5,000 | -,797   | -4,695 | 2,010    | 5,918  |
| KG4      | 1,000 | 5,000 | -1,525  | -8,980 | 4,116    | 12,116 |
| KG3      | 2,000 | 5,000 | -,734   | -4,320 | ,218     | ,643   |
| KG2      | 2,000 | 5,000 | -,877   | -5,164 | ,593     | 1,744  |
| AF5      | 1,000 | 5,000 | -,722   | -4,250 | 2,998    | 8,826  |
| AF4      | 1,000 | 5,000 | -,875   | -5,150 | 2,984    | 8,785  |
| AF3      | 2,000 | 5,000 | -,491   | -2,889 | ,958     | 2,820  |
| AF2      | 1,000 | 5,000 | -1,212  | -7,138 | 5,932    | 17,463 |
| AF1      | 1,000 | 5,000 | -1,354  | -7,971 | 5,230    | 15,396 |
| GG6      | 1,000 | 5,000 | -,290   | -1,708 | -,359    | -1,057 |
| GG5      | 1,000 | 5,000 | -,298   | -1,755 | ,146     | ,431   |
| GG4      | 1,000 | 5,000 | -,331   | -1,949 | -,149    | -,438  |
| KK6      | 1,000 | 5,000 | -,423   | -2,488 | -,101    | -,298  |
| KK4      | 2,000 | 5,000 | -,673   | -3,962 | ,951     | 2,800  |
| KK3      | 1,000 | 5,000 | -1,024  | -6,031 | 2,149    | 6,326  |
| KK2      | 1,000 | 5,000 | -1,005  | -5,920 | 2,094    | 6,165  |
| KK1      | 2,000 | 5,000 | -,766   | -4,510 | 1,381    | 4,066  |

**Tablo 5.7:** devam.

| Değişken | Min   | Maks  | Eğrilik | C.R.   | Basıklık | C.R.  |
|----------|-------|-------|---------|--------|----------|-------|
| N5       | 2,000 | 5,000 | -,435   | -2,560 | ,198     | ,584  |
| N4       | 1,000 | 5,000 | -,594   | -3,496 | ,943     | 2,776 |
| N3       | 2,000 | 5,000 | -,613   | -3,610 | ,912     | 2,686 |
| N2       | 1,000 | 5,000 | -,495   | -2,913 | ,214     | ,629  |
| N1       | 1,000 | 5,000 | -,648   | -3,813 | 1,288    | 3,792 |

### 5.2.2. Verilerin Güvenilirlik Analizi

Anketimizdeki diğer analizleri yapmak için öncelikle verilerimizin güvenilirliğini ölçümlememiz gerekmektedir. Anket yapılırken ölçekler; teknoloji yetkinliği: 3, niyet: 5, kullanım kolaylığı: 6, gizlilik ve güvenlik: 6, algılanan fayda: 5 ve kullanıcı güveni: 3 farklı ifade kullanılarak ölçülmüştür. Ölçeklerin güvenilirlik testi değerleri Tablo 5.8’ de görülmektedir. Güvenirlik, ölçek maddelerinin iç tutarlılığının bir ölçüsüdür. Bu çalışmada yapı güvenilirliğini değerlendirmek için bileşik güvenilirlik (CR) kullanıldı. Herhangi bir faktör için güvenilirliğin sağlanması için CR değeri değerinin 0.70 'den büyük olması önerilir. Bu çalışmada CR değerleri (Tablo 5.8), önerilen 0.70 eşik değerinin üzerinde bulunmuştur. Yapı geçerliliği, ölçülenler arasında gerçekte ilişki olup olmadığını değerlendiren yapı geçerliliğinin bir alt türüdür. Yapı geçerliliğinin sağlanması için AVE değerlerinin 0.50'den büyük olması gerekir. Bu çalışmada AVE değerleri (Tablo 5.8) tüm faktörler için 0.50'den büyük bulunmuştur; bu nedenle, her bir yapının yapı geçerlilik varsayımının geçerli olduğu sonucuna varılabilir.

**Tablo 5.8:** Geçerlilik ve güvenilirlik değerlendirmesi.

|    | CR    | AVE   | MSV   | Max R(H) | N            | KK           | GG | AF | KG | TY |
|----|-------|-------|-------|----------|--------------|--------------|----|----|----|----|
| N  | 0,868 | 0,572 | 0,391 | 0,888    | <b>0,756</b> |              |    |    |    |    |
| KK | 0,895 | 0,641 | 0,435 | 0,945    | 0,487<br>*** | <b>0,801</b> |    |    |    |    |

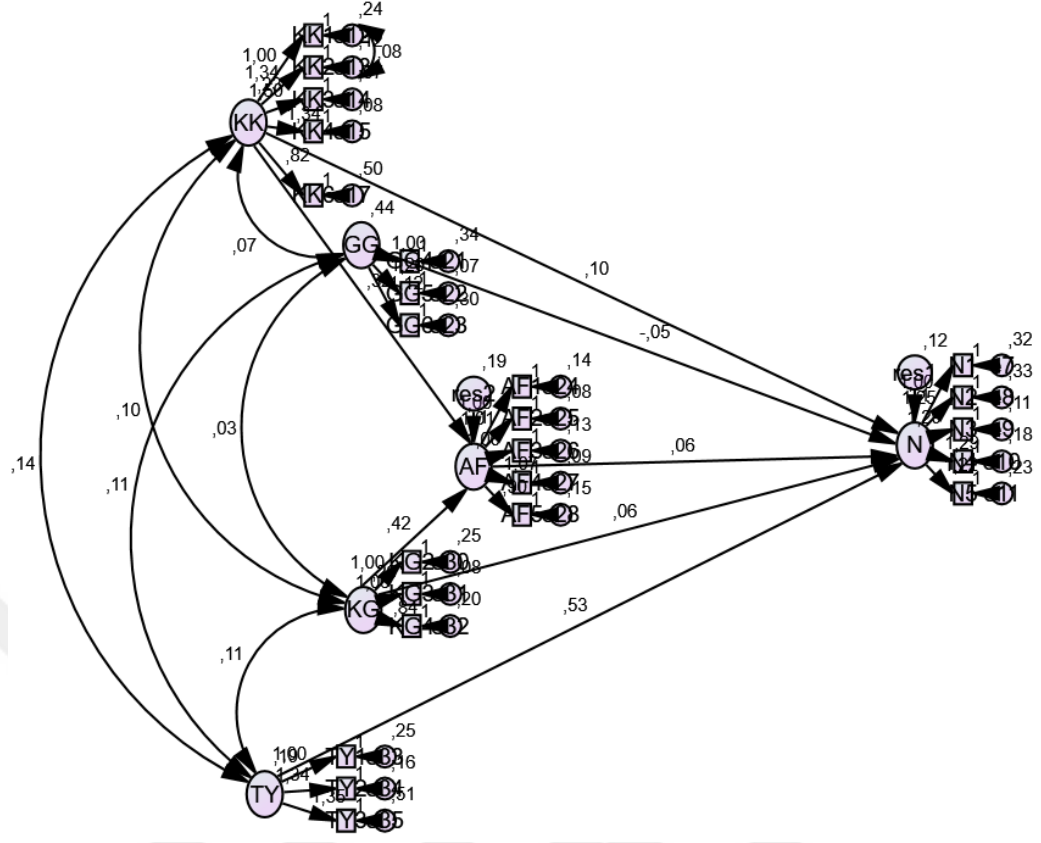
**Tablo 5.8:** devam.

|                | CR    | AVE   | MSV   | MaxR(H) | N            | KK           | GG           | AF           | KG           | TY                |
|----------------|-------|-------|-------|---------|--------------|--------------|--------------|--------------|--------------|-------------------|
| <b>G<br/>G</b> | 0,878 | 0,707 | 0,132 | 0,925   | 0,147<br>†   | 0,212*<br>*  | <b>0,841</b> |              |              |                   |
| <b>AF</b>      | 0,921 | 0,701 | 0,278 | 0,927   | 0,378<br>*** | 0,454*<br>** | 0,151*       | <b>0,837</b> |              |                   |
| <b>K<br/>G</b> | 0,806 | 0,585 | 0,263 | 0,848   | 0,388<br>*** | 0,432*<br>** | 0,071        | 0,513**<br>* | <b>0,765</b> |                   |
| <b>TY</b>      | 0,745 | 0,496 | 0,435 | 0,769   | 0,626<br>*** | 0,659*<br>** | 0,363**<br>* | 0,527**<br>* | 0,500**<br>* | <b>0,70<br/>5</b> |

### 5.2.3. Dijital Doğrulama Teknolojilerini Kullanma Niyetini Etkileyen Faktörlerin Ölçümü

Teknoloji kabul modelinin girdileri yapılan anket çalışmasıyla niyeti ölçecek sorularla ve farklı ifadelerle anket katılımcılarına sorulmuştur. Teknoloji yetkinliği, kullanıcı güveni, algılanan fayda, gizlilik ve güvenlik, kullanım kolaylığı ve niyet ile ilgili sorular literatürdeki benzer çalışmalardaki ölçeklerden yararlanılarak ankette kullanılmıştır. Anket soruları tezin ek kısmında paylaşılmıştır. Ankete 208 kişi katılım sağlamıştır. Yanıtlar analize uygun hale getirilerek, SPSS AMOS istatistik programında analiz edilmiştir.

Modelin girdileri, belirli bir anket çalışmasındaki uygunluğu değerlendirmek ve girdiler arasındaki nedensel ilişkileri belirlemek amacıyla yapısal eşitlik modellemesi ile incelenmiştir. Yapısal eşitlik modeli, kullanılan değişkenlerin büyük bir kısmını model içerisine entegre etme yeteneğine sahiptir. Bu değişkenlerin etkileri, model üzerinde dolaylı veya doğrudan gözlemlenebilir; ayrıca, bunlar örtük veya gözlemlenen değişkenler olarak tanımlanabilir.



Şekil 5.2: Yol analizi.

Tablo 5.9: Regresyon ağırlıkları.

|             |      |    | Tahmin | S.E. | C.R.   | P    |
|-------------|------|----|--------|------|--------|------|
| AF          | <--- | KK | ,319   | ,085 | 3,756  | ***  |
| AF          | <--- | KG | ,419   | ,087 | 4,800  | ***  |
| N           | <--- | KK | ,104   | ,097 | 1,077  | ,281 |
| N           | <--- | GG | -,052  | ,050 | -1,041 | ,298 |
| N           | <--- | AF | ,057   | ,070 | ,823   | ,410 |
| N           | <--- | KG | ,055   | ,084 | ,654   | ,513 |
| N           | <--- | TY | ,533   | ,147 | 3,620  | ***  |
| *** p<0,001 |      |    |        |      |        |      |

Tablo 5.9 'da regresyon ağırlıklarının standartlaştırılmış formu verilmiştir. Standartlaştırılmış regresyon ağırlıkları, bağımlı ve bağımsız değişkenlerin

varyanslarının 1 olduğu şekilde standartlaştırılmış tahminlerdir. Bu standartlaştırılmış katsayılar, bağımsız değişkenin bir standart sapma artışıyla bağımlı değişkenin ne kadar standart sapma değişeceğini gösterir.

**Tablo 5.10:** Kare çoklu korelasyonlar.

|    | Tahmin |
|----|--------|
| AF | 0,340  |
| N  | 0,403  |

Tablo 5.10’da verilen diğer önemli bir tahmin, kare çoklu korelasyonlardır. Kare çoklu korelasyon, bir gösterge değişkeni için ortaklık tahminidir. Kare çoklu korelasyon, bir veri göstergesi değişkenindeki varyansın, onun gizil değişkeni tarafından açıklandığı yüzdeyi ölçer. Ayrıca, bir gösterge değişkeninin güvenilirliği olarak da yorumlanabilir. Yani, bu gösterge ne kadar yüksekse, verilen göstergenin o kadar güvenilir olduğu anlamına gelir. Düşük kare çoklu korelasyon değerine sahip göstergelerin modelden çıkarılması gerekebilir. Tablo 5.10 ‘da, tüm göstergelerin kare çoklu korelasyonlarının 0,50’nin üzerinde olduğunu göstermektedir. Bağımlı değişkenin kare çoklu korelasyon değeri Tablo 5.10 ‘da verilmiştir.

Kare çoklu korelasyon, tahmin edilen değişkenin varyansının, tahmin edici değişkenlerden tahmin edilebilir yüzdesini gösterir. Niyetin, algılanan faydanın varyansının %34’ünü açıkladığı tahmin edilmektedir.

Şekil 5.2 ‘de verilen yapısal modelin regresyon ağırlıkları üzerine araştırma bulgularını özetleyen aşağıdaki ifadeler aşağıda verilmiştir:

- Kullanım Kolaylığı (KK) ( $\beta_{KK}=-0.319$ ,  $SE=0,085$ ,  $p<0.001$ ) ‘nın, dijital doğrulama teknolojilerinin kullanımını etkileyen algılanan fayda üzerinde anlamlı bir etkisi olduğu görülmüştür.
- Kullanıcı Güveni (KG) ( $\beta_{KG}=0.419$ ,  $SE=0,087$ ,  $p<0.001$ ) ‘nin, dijital doğrulama teknolojilerinin kullanımını etkileyen algılanan fayda üzerinde anlamlı bir etkisi olduğu görülmüştür.
- Kullanım Kolaylığı (KK) ( $\beta_{KK}=-0.104$ ,  $SE=0.097$ ,  $p=0.281$ ) ‘nın, dijital

doğrulama teknolojilerinin kullanımını etkileyen niyet üzerinde anlamlı bir etkisi bulunmamıştır.

- Gizlilik ve Güvenlik (GG) ( $\beta_{GG}=-0.052$ ,  $SE=0.050$ ,  $p=0.298$ ) 'in, dijital doğrulama teknolojilerinin kullanımını etkileyen niyet üzerinde anlamlı bir etkisi bulunmamıştır.
- Algılanan Fayda (AF) ( $\beta_{AF}=-0.057$ ,  $SE=0.070$ ,  $p=0.410$ ) 'nın, dijital doğrulama teknolojilerinin kullanımını etkileyen niyet üzerinde anlamlı bir etkisi bulunmamıştır.
- Kullanıcı Güveni (KG) ( $\beta_{KG}=0.055$ ,  $SE=0.084$ ,  $p=0.513$ ) 'nin, dijital doğrulama teknolojilerinin kullanımını etkileyen niyet üzerinde anlamlı bir etkisi bulunmamıştır.
- Teknoloji Yetkinliği (TY) ( $\beta_{TY}=0.533$ ,  $SE=0.147$ ,  $p<0.001$ ), dijital doğrulama teknolojilerinin kullanımını etkileyen niyet üzerinde anlamlı bir etkisi olduğu görülmüştür.

## 6. SONUÇ

Dijital doğrulama teknolojilerinin vatandaşlar tarafından kullanımını etkileyen faktörler çok yönlü bir yaklaşım gerektirmektedir. Gizlilik ve güvenlik, kullanım kolaylığı, algılanan fayda, niyet, teknoloji yetkinliği ve kullanıcı güveni faktörlerinin birlikte ele alınması, bu teknolojilerin toplumda daha geniş bir kabul görmesine katkı sağlayacaktır.

Dijital doğrulama teknolojileri, kullanıcıların kimliklerini çevrimiçi ortamlarda güvenli bir şekilde doğrulamalarına yardımcı olan sistemlerdir. Bu teknolojilerin ortaya çıkışı ve yaygınlaşması birkaç faktöre dayanmaktadır. Artan Çevrimiçi Etkileşimler: İnternetin yaygınlaşması ve çevrimiçi etkileşimlerin artmasıyla birlikte, kullanıcıların dijital kimliklerini güvenli bir şekilde doğrulama ihtiyacı ortaya çıktı. Özellikle e-ticaret, bankacılık, sağlık hizmetleri gibi alanlarda güvenli kimlik doğrulama gereksinimi arttı. Kimlik Hırsızlığı ve Dolandırıcılık: Kimlik hırsızlığı ve çevrimiçi dolandırıcılık vakalarının artması, dijital ortamlarda güvenli kimlik doğrulama sistemlerine olan talebi artırdı. Klasik kimlik doğrulama yöntemleri (kullanıcı adı ve şifre) bu tür tehditlere karşı yeterli koruma sağlamadığından, daha güvenli yöntemlere duyulan ihtiyaç ortaya çıktı. Gelişen Teknolojiler: Biyometrik verilerin kullanımı, akıllı kartlar, iki faktörlü kimlik doğrulama gibi gelişen teknolojiler, dijital doğrulama sistemlerini daha güvenli ve etkili hale getirdi. Parmak izi tarayıcıları, yüz tanıma sistemleri, retina tarayıcıları gibi biyometrik teknolojiler, kullanıcıların kimliklerini daha güvenli bir şekilde doğrulamalarına olanak tanıdı.

Yasal Düzenlemeler: Birçok ülke ve bölgede, çevrimiçi hizmet sağlayıcılarının kullanıcı kimliklerini doğrulamalarını ve güvenlik önlemleri almalarını sağlayan yasal düzenlemelerin oluşturulması, dijital doğrulama teknolojilerinin yaygınlaşmasına katkıda bulundu. Bu düzenlemeler, çevrimiçi hizmet sağlayıcılarını daha güvenli hale getirmeye teşvik etmiştir.

Bu çalışma, sınırlı sayıda örneklemle yapılmış olup; emekli ve orta yaş üstü gruptan oluşmaktadır. Analiz bulgularının bu durum dikkate alınarak değerlendirilmesi gerekmektedir.

## 6.1. Akademik Çıktılar

Dijital doğrulama teknolojileri günümüzde birçok alanda yaygın olarak kullanılmaktadır. Kullanıcıların kimliklerini doğrulamak için biyometrik verileri, mobil cihazları veya özel anahtarları kullanarak güvenli bir şekilde erişim sağlamak, çevrimiçi platformlar ve hizmet sağlayıcıları için standart bir uygulama haline gelmiştir. Dijital doğrulama teknolojilerinin, vatandaşlar tarafından kullanımını etkileyen faktörleri incelemek amacıyla, literatürdeki teknoloji kabul modelleri üzerine birçok çalışma yapılmıştır. Teknolojik ilerlemelerin sürekli olarak devam etmesi, bu modellerin değiştiği ve evrim geçirdiği gerçeği nedeniyle, dijital doğrulama teknolojileri değerlendirirken en güncel modellerden biri tercih edilmiştir; bu bağlamda teknoloji kabul modeli kullanılmıştır. Literatürdeki araştırmalardan elde edilen bulgulara göre, dijital doğrulama teknolojilerinin farklı coğrafyalardaki çalışmalarında özellikle UTAUT ve UTAUT2 modelinin kullanıldığı gözlemlenmiştir. Modellerin esnekliği, farklı ülkelerde gerçekleştirilen çalışmalarda çeşitli sonuçlara yol açmıştır.

Bu araştırmada, UTAUT2 modeli ve ilgili değişkenlere dair literatürden bilgiler sunulmuş ve modelin değişkenleri detaylı bir şekilde incelenmiştir. Modelin değişkenlerine dayalı olarak hipotezler oluşturulmuştur. Bu hipotezlere dayalı olarak gerçekleştirilen anket çalışmasıyla, hipotezlerin test edilmesi amaçlanmıştır. Anket sonuçları, demografik özellikler ve model değişkenleri incelenerek, vatandaşların dijital doğrulama teknolojilerini kullanımını etkileyen faktörler ortaya konulmuştur. Yapılan anket çalışması neticesinde model değişkenleri istatistiksel olarak incelenmiş ve vatandaşların dijital doğrulama teknolojilerini kullanımını etkileyen faktörler belirlenmiştir. Elde edilen farklılıklar, gelecekteki dijital doğrulama teknolojilerinin ve mevcut olanların özelliklerinin belirlenmesi ve bu özelliklerin vurgulanması konusunda önem taşımaktadır. Bu durum, dijital doğrulama teknolojilerini kullanıcı sayısını artırma açısından önemli bir faktördür.

## 6.2. Uygulamaya Yönelik Çıktılar

Cinsiyet, yaş, çalışma durumu ve eğitim durumu gibi faktörlerin, dijital doğrulama teknolojilerini kullanma niyetinde farklılık yaratıp yaratmadığı incelenmiştir. Demografik verilerle ilgili bilgi verilmiştir.

Anket çalışmasında, ölçümlenen teknoloji kabul modeli değişkenleri SPSS istatistik programı ile analiz edilmiştir. Ankette yer alan sorular, literatürde yer alan benzer ölçeklerden alınarak doğrulama teknolojileri konumuza uyarlanmıştır. Soruların doğru sorulup sorulmadığı ise doğrulayıcı faktör analizi ile analiz edilmiştir. Analize göre, soruların doğru sorulduğu tespit edilmiştir.

Yol analizi ile; karmaşık ilişkilerin, etkileşimlerin ve model yapılarının anlaşılması ve araştırma modelinin doğrulanması, geçerliliği ve öngörme yeteneğini değerlendirmek hedeflenmiştir. Yol analizi sonucunda, modelin tüm girdilerinin dijital doğrulama teknolojileri kullanımına ne kadar etkisi olduğu ortaya çıkarılmıştır. Model çıktılarına göre gizlilik ve güvenlik, kullanım kolaylığı, algılanan fayda, teknoloji yetkinliği ve kullanıcı güveni faktörlerinin dijital doğrulama teknolojileri kullanma niyetiyle anlamlı bir ilişkisi olduğu görülmüştür. Modelde en yüksek etkiye sahip olan; kullanım kolaylığı, algılanan fayda ve gizlilik ve güvenlik koşullarıdır. Gizlilik ve güvenlik modeli negatif etkilemektedir. Buna göre vatandaşların gizlilik ve güvenlik endişesi varsa doğrulama teknolojilerini kullanma niyetinde olmayacaklardır. Vatandaşlar, özellikle kişisel ve biyometrik bilgilerini paylaşacakları platformlara güven duymak ve kolay kullanabilmek isterler. Bu nedenle vatandaşların, dijital doğrulama teknolojilerini kullanımını artırmak ve verimli hale getirmek için; kullanıcı dostu arayüzler, artırılmış siber güvenlik önlemleri etkili olacaktır. Teknoloji yetkinliği, bu teknolojileri kullanma niyetine doğrudan etki etmektedir. Kullanıcılar, teknoloji okur yazarlığına sahipse, dijital doğrulama teknolojilerini anlamada ve kullanmada daha istekli olacaklardır.

Yol analizinden sonra, güvenilirlik analizi yapılmıştır. Verilerinin güvenilirliği ölçümlemek için analiz yapılarak; anket çalışması yapılırken kullanılan her bir ölçek için birçok ifadeden yararlanıldı ve güvenilirlik analizi her bir ölçek için ayrı ayrı yapılmıştır. Faktörlerin analiz değerleri güvenilir seviyelerinde seyretmektedir.

Bu tez ile Türkiye dijital doğrulama teknolojileri pazarında rol alan veya alacak firmaların; ürünlerinde pazarlama faaliyetleri ve ürün geliştirmelerini bu sonuçları değerlendirerek, kullanıcılarını ürünlerini kullanmaya teşvik edebilirler. Vatandaşların, dijital doğrulama teknolojileri kullanırken öncelikle en yüksek etkiye sahip olan kullanım kolaylığı, gizlilik ve güvenlik etkenlerine dikkat ettiklerini değerlendirerek vurgu yapılmalıdır.

### 6.3. Gelecek Çalışmalar İçin Öneriler

Bu çalışmada küçük örneklem ve kısıtlı sayıda katılımcı ile araştırma yapılmıştır. Kısıtlarımızdan bir diğeri katılımcıların yoğunluklu olarak lise ve üzeri eğitime sahip kitle olmasıdır. Gelecek çalışmalar; daha genel kitlelerde araştırma yapabilir, farklı demografik durumları da çalışmalara dahil edebilirler.

Gelecekteki çalışmalar, dijital doğrulama teknolojilerinin kullanımını artırmak ve güveni pekiştirmek için daha fazla detaylı araştırmaya odaklanabilir. Dijital doğrulama teknolojileri, kullanıcı niyetleri çeşitlenerek pazarın dinamiklerine bağlı olarak değişecektir. Yapılan çalışmanın, belirlenen zamanın koşullarını temel aldığı değerlendirilmelidir.

Dönüşen ve dijitalleşen dünyada, kamu kurumları doğrulama teknolojilerinin kullanımını sağlamakla beraber suç ve sahtecilik durumlarının hızlı tespitini, vatandaşlarının güvenliğine verdiği önemi göstermiş olacaktır. Bu durum; bankacılık, sağlık sektörü vb. birçok sektörde de izlenilebilirliği kolaylaştıracaktır. Ayrıca, firmalar da müşterilerini uzaktan edinebilecek ve doğrulama aşamalarından geçirmiş olacaktır.

Dijital doğrulama teknolojilerinin gelişmesi, güvenlik alanında önemli katkılar sağlar. Biyometrik veriler, şifreleme ve diğer güvenlik önlemleri aracılığıyla kullanıcı kimlik doğrulamasını güçlendirerek kimlik hırsızlığını azaltır. Bu teknolojiler, çevrimiçi hizmetlere hızlı ve güvenli erişimi destekler, finansal işlemlerde güvenliği artırır, sağlık sektöründe hasta kimlik doğrulamasını güçlendirir ve kamu hizmetlerinde etkinliği artırır. Aynı zamanda, e-ticarete güveni artırır, vergi kaçaklarıyla mücadelede katkıda bulunur ve genel olarak dijital dünyada güvenliği ve verimliliği artırır. Bu teknolojilerin ve kullanıcı bilgi düzeylerinin değişmesiyle birlikte, demografik yapılarına bağlı olarak dijital doğrulama teknolojilerini kullanma niyetlerinin farklılık göstereceği öngörülmektedir. Farklı grupların kullanım niyetini etkileyen faktörleri belirlemek için yapılan çalışmalar, dijital doğrulama teknolojilerinin kullanımını artırmak ve kullanıcılara uygun ürünler oluşturmak adına önemlidir. Bu sayede, vatandaşların kullanımını etkileyen faktörlere uygun iletişim stratejileri oluşturularak dijital doğrulama teknolojilerinin kullanımı teşvik edilebilir.

## KAYNAKLAR

- Aka H. M., (2023), “Online Mağazaların Web Sitelerine Yönelik Kalite Faktörlerinin Algılanan Etkenebilirlik ve Online Satın Alma Niyeti ile İlişkisi ve Bir Araştırma”, Yüksek Lisans Tezi, Galatasaray Üniversitesi.
- Alkan A. O., (2020), “Blok Zincir Teknolojisinin Benimsenmesini Etkileyen Faktörler: Güvenlik Açısından Ampirik Bir Çalışma”, Yüksek Lisans Tezi, Başkent Üniversitesi.
- Anthes G., <https://cacm.acm.org/news/estonia/>. Erişim Tarihi: 14.11.2023.
- Aras M., Özdemir Y., Bayraktaroğlu S., (2015), “The Investigation Of Perceptions For Human Resource Information Systems Via Technology Acceptance Model”, Ege Academic Review, 15 (3), 343-352.
- Aydın, Y. A., (2021), [www.academia.edu.tr](http://www.academia.edu.tr). Erişim Tarihi: 20.01.2021.
- Baheer B.A., Lamas D., Sousa S., (2020), “A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art Challenges, and Prospects”, Administrative Sciences 10 (2), 2-28.
- Bayzan Ş., Cubukcu A., (2013), “Türkiye’de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı İle Artırma Yöntemleri”, Middle Eastern ve African Journal of Educational Research, (5), 148.
- Black J., (2014), “The Power of Knowledge How Information and Technology Made the Modern World”, New Haven/London: Yale University Press, 67 (2), 256–257.
- Can A., (2019), “Akıllı Ev Cihazları İçin Teknoloji Kabul Modeli: Kısmi En Küçük Karelerle Yapısal Eşitlik Modelleme”, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi.
- Cesur D., Köse C., (2021), “Dijital Teknolojiye Yönelik Tutumların Girişimcilik Niyetindeki Rolü: Z Kuşağında Bir Araştırma”, Biga İktisadi ve İdari Bilimler Fakültesi Dergisi, 2 (3), 252-270.
- Çaptuğ M., (2021), “Covid-19 Salgınının Kamu Hizmetlerinin Dijitalleşmesi Sürecine Etkisi ve Sonuçları”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 23, 1309-27.
- Çetinkaya N., (2017), “Türkiye’de E-devlet hizmetlerinin Eğitim ve Sosyal Hayat Üzerindeki Etkileri”, Uluslararası Sosyal Bilimler Akademik Araştırmalar Dergisi, 1 (1), 12-21.
- Davis F.D., (1989), “Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology”, MIS Quarterly, 13(3), 319-340.
- Erdoğan O., (2019), “Yerel Yönetimlerde Dijital Dönüşüm: Molenwaard Belediyesi Örneği”, Sosyal Bilimler Enstitüsü Dergisi, 7(3), 59-74.

Gerpott T.J., Meinert P., (2017), “Who signs up for NFC mobile payment services Mobile network operator subscribers in Germany”, *Electronic Commerce Research and Applications*, 23, 1-13.

Gül H., (2002), “Kamu Kuruluşlarında Elektronik Hizmetlerin Yaygınlaştırılması (E-Devlet)”, *Maliye Dergisi*, 140, 14-46.

Gündüz Ş., Yazıcı C., (2020), “Kimlik doğrulama şemalarının üniversite öğrencileri tarafından tercih edilme durumlarının incelenmesi”, *A. Keleşoğlu Eğitim Fakültesi Dergisi*, 2 (1), 1-11.

Kaplan, S. E., ve Nieschwietz, R. J. (2003). “A Web Assurance Services Model of Trust for B2C E-commerce”, *International Journal of Accounting Information Systems*, 4(2), s. 95-114.

Kaplan S. E., Nieschwietz R. J., (2003), “A Web Assurance Services Model of Trust for B2C E-commerce”, *International Journal of Accounting Information Systems*, 4 (2), 95-114.

Koç H., (2021), “Dijital dünyada yeni vatandaşlık konsepti: Estonya’da e-vatandaşlık örneği”, *Uluslararası Toplum Araştırmaları Derneği*, 17 (35), 2256-2289.

Liu Y., (2015), “Consumer protection in mobile payments in China; A critical analysis of Alipay’s service agreement”, *Computer Law ve Security Review*, 31, 679-688.

Luo J.N., Yang M. H., Huang S., (2016), “An Unlinkable Anonymous Payment Scheme based on near field communication”, *Computers and Electrical Engineering*, 49, 198-206.

Mannan M., Van Oorschot P.C., (2008), “Leveraging personal devices for stronger password authentication from untrusted computers”, *Journal of Computer Security*, 49, 703-750.

Dilmegani, vd., (2014), <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/public-sector-digitization-the-trillion-dollar-challenge>. Erişim Tarihi: 21.12.2023.

Nielsen M.M., (2017), “e-Governance and online service delivery in Estonia”, In *Proceedings of the 18th Annual International Conference on Digital Government Research*, 300-309, NY, USA, 7-9 June.

Parsovs A., (2020), “Estonian electronic identity card: security flaws in key management”, 29th Security Symposium, 1785-1802, Boston, USA, 12-14 August.

Prause G., (2016), “E-Residency: A business platform for Industry 4.0.”, *Entrepreneurship and Sustainability Issues*, 3 (3), 216-227.

Park J., Snell W., Ha S., Chung T.L., (2011), “Consumers’ Post-Adoption of M-Services: Interest in Future M-Services Based on Consumer Evaluations of Current M-Services”, *Journal of Electronic Commerce Research*, 12 (3), 165-175.

Sevinç K., (2021), “Siber Güvenlik Ölçeği Geliştirme: Geçerlik ve Güvenirlilik Çalışması”, *Yüksek Lisans Tezi, Tokat Gaziosmanpaşa Üniversitesi*.

Shrier D., Wu W., Pentland A., (2016), “Blockchain & Infrastructure (identity, data security)”, Massachusetts Institute of Technology-Connection Science, 1 (3), 1-19.

Sullivan C., Burger E., (2017), “E-residency and blockchain.”, Computer Law ve Security Review, 33 (4), 470-481.

Şahin A., (2007), “Türkiye’de e- Türkiye’de e-belediye uygulamaları ve Konya örneği”, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 29, 161-189.

Topsakal S., (2006), “İlköğretim 6.,7. ve 8. Sınıflar fen ve teknoloji öğretimi”, Ankara: Nobel Yayıncılık.

Ursavaş Ö. F., Şahin S., McILROY D., (2014), “Öğretmenler İçin Teknoloji Kabul Ölçeği (Ö-TKÖ)”, Eğitimde Kuram ve Uygulama, 10 (4), 885-917.

Ünsal P. U., (2021), “Sayısal Göçmenler ve Sayısal Yerlilerin Doğal Reklama İlişkin Tutumları Üzerinde Medya Türünün ve Marka Belirginliğinin Etkileri”, Doktora Tezi, Eskişehir Anadolu Üniversitesi.

Web 1, (2019), [http://bctr.org/dokumanlar/Dijital Kimlik](http://bctr.org/dokumanlar/Dijital%20Kimlik), (Erişim Tarihi: 22/12/2023).

Web 2, (2021), [https:// ec.europa.eu/info/sites/default/files](https://ec.europa.eu/info/sites/default/files), (Erişim Tarihi: 10/10/2023).

Web 3, (2019), <https://mckinsey.com/>, (Erişim Tarihi: 24/11/2023).

Web 4, (2016), <https://www3.weforum.org/>, (Erişim Tarihi: 05/01/2024).

Yıldırım U., Öner Ş., (2004), “Bilgi Toplumu Sürecinde Yerel Yönetimlerde Eğitim-Bilişim Teknolojisinden Yararlanma: Türkiye’de E-Belediye Uygulamaları”, The Turkish Online Journal of Educational Technology – TOJET, 3(1), 49-60.

Yıldırım U., Öner Ş., (2002), <https://www.researchgate.net/publication/228762787>. Erişim Tarihi: 14.11.2023.

Yılmaz M. B., Kavanoz S., (2017), “Teknoloji Kabul ve Kullanım Birleştirilmiş Modeli-2 Ölçeğinin Türkçe Formunun Geçerlik ve Güvenirlik Çalışması”, Turkish Studies – Bilişim Teknolojileri ve Uygulamalı Bilimler Dergisi, 12 (32), 127-146.

## ÖZGEÇMİŞ

Şeyma Nur Konyar, 2017 yılında Karabük Üniversitesi Endüstri Mühendisliği Bölümü'nden mezun olmuştur. Lisans eğitiminden sonra Gebze Teknik Üniversitesi İşletme bölümünde yüksek lisans eğitimine başlamıştır.



## TEZ ÇALIŞMASI KAPSAMINDA YAPILAN YAYINLAR

Konyar Ş., (2023), “Dijital Doğrulama Teknolojileri: Kullanım Alanlarının ve Dijital Dünyadaki Öneminin İncelenmesi”, 6. Uluslararası Antalya Bilimsel Araştırmalar ve Yenilikçi Çalışmalar Kongresi, 449-454, Antalya, Türkiye, 2-4 Aralık.



## **EKLER**

### **Ek-A: Araştırma Anketi**

Bu anket formu Gebze Teknik Üniversitesi Lisansüstü Eğitim Enstitüsünde hazırlanmakta olan yüksek lisans tezinin araştırma kısmı için tasarlanmıştır. Bu yüksek lisans çalışmasındaki amaç, dijital doğrulama teknolojilerinin vatandaşlar tarafından kamu hizmetlerinde kullanımın etkileyen faktörlere bütünsel bir model oluşturmaktır. Anket çalışması, teknoloji kullanıcısı olan vatandaşların dijital doğrulamaya olan izlenimlerini ve bakış açılarını ölçümleyebilmeyi hedeflemektedir. Her bir ifade “Kesinlikle Katılıyorum, Katılıyorum, Kararsızım, Katılmıyorum, Kesinlikle Katılmıyorum” şeklinde derecelendirilmiştir. Lütfen size en uygun olanı işaretleyiniz.

Katılımınız için teşekkür ederim.

**Şeyma Konyar Terzioğlu**

**Gebze Teknik Üniversitesi İşletme Yüksek Lisans Öğrencisi**

### **SORULAR**

#### **Niyet Ölçeği**

1. Dijital doğrulama teknolojisi araç ve ortamlarını bol bol değerlendirmeye devam etmeyi planlıyorum.
2. Gelecekteki dijital doğrulama teknolojileri gereksinimleri için başka doğrulama teknolojisi araç ve ortamlarını araştıracağım.
3. İleride başka doğrulama teknolojisi araç ve ortamlarını kullanmaya devam etmek niyetindeyim.
4. Hayatımda dijital doğrulama teknolojilerini sürekli kullanmayı düşünüyorum.
5. Başkalarına da dijital doğrulama teknolojilerini kullanmalarını tavsiye edeceğim.

#### **Kullanım Kolaylığı**

1. Kamu hizmetlerinde dijital doğrulama teknolojilerini kullanmak benim için kolaydır.
2. Dijital doğrulama teknolojileri kullanımı benim için kolaydır.

3. Kamu hizmetlerinde dijital doğrulama teknolojilerini kullanabilecek beceriye sahip olmak benim için kolaydır.
4. Dijital doğrulama teknolojilerinin kullanımını öğrenmek benim için kolaydır.
5. Dijital doğrulama teknolojilerini kullanmak zihinsel çaba gerektirmez.
6. Dijital doğrulama teknolojileri açık ve anlaşılırdır.

### **Güvenlik ve Gizlilik**

1. Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.
2. Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.
3. Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.
4. Dijital doğrulama teknolojileri, çevrimiçi faaliyetlerim hakkındaki bilgilerin diğer taraflarla (3. Şahıslarla) paylaşılmayacağına dair bana güvence verir.
5. Dijital doğrulama teknolojileri, hakkımdaki bilgileri korur.
6. Dijital doğrulama teknolojileri, kişisel bilgilerimi başka sitelerle paylaşmaz.

### **Algılanan Fayda**

1. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanarak işlemlerimi daha hızlı gerçekleştirebilirim.
2. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmam işlem performansımı artırır.
3. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmam işlemlerdeki etkinliğimi artırır.
4. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmak işlemleri daha kolay gerçekleştirmemi sağlar.
5. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmak faydalıdır.

### **Kullanıcı Güveni**

1. Dijital doğrulama teknolojileri kullanılarak kamu hizmetleri işlemleri yapmak güvenli olacaktır.
2. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri kullanmada kişisel bilgilerin saklanması önemlidir.

3. Dijital doğrulama teknolojileri kullanarak kamu hizmetleri işlemleri yapmada güvenlik önemlidir.
4. Kamu hizmetleri işlemlerinde dijital doğrulama teknolojileri verilerine hiç kimsenin izinsiz erişim sağlamaması benim için önemlidir.

### **Teknoloji Yetkinliği**

1. Yeni bilgi-iletişim teknolojilerini olumlu buluyorum.
2. Teknolojik yenilikleri kolay benimserim.
3. Yeni teknolojilere kolaylıkla uyum sağlarım.
4. Teknolojiye anadilim gibi hakimim.
5. Son çıkan teknolojik cihazlara sahip olmak benim için önemlidir.
6. Çevrimiçi olarak paylaştıklarım yaşamımın önemli bir kısmını yansıtıyor.
7. Bence çevrimiçi iletişim yüz yüze iletişimin yerini tutar.
8. Günün her anında çevrimiçi olmaktan memnunum.
9. Not alırken el yazısıyla yazmaktansa bilgisayara ya da telefona not almayı tercih ederim.
10. Bir şeyi İnternet üzerinden satın aldıysam mutlaka çıktısını da saklarım. (Örneğin fatura, bilet vb.)

