NESNELERİN İNTERNETİ (IoT)'NİN ASKERİ ALANDA KULLANILABİLİRLİĞİ VE KABUL MODELİ ÖNERİSİ

Rabia SAYLAM

Doktora Tezi
Yönetim Bilişim Sistemleri Anabilim Dalı
Doç. Dr. Abdulkadir ÖZDEMİR
2020

T.C.
ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

Rabia SAYLAM

NESNELERİN İNTERNETİ (IoT)'NİN ASKERİ ALANDA KULLANILABİLİRLİĞİ VE KABUL MODELİ ÖNERİSİ

DOKTORA TEZİ

TEZ YÖNETİCİSİ
Doç. Dr. Abdulkadir ÖZDEMİR

ERZURUM - 2020

SOSYAL BİLİMLER ENSTİTÜSÜ
Graduate School of Social Sciences

TEZ BEYAN FORMU

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

BİLDİRİM

Atatürk Üniversitesi Lisansüstü Eğitim ve Öğretim Uygulama Esaslarının ilgili maddelerine göre hazırlamış olduğum "Nesnelerin İnterneti (IoT)'nin Askeri Alanda Kullanılabilirliği ve Kabul Modeli Önerisi" adlı tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kâğıt ve elektronik kopyalarının aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım.

Gereğinibilgilerinizearz ederim *.

☐ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☒ Tezimin/Raporumun makale için **altı ay,** patent için **ikiyıl** süreyle erişiminin ertelenmesini istiyorum.

02.07.2020
Rabia SAYLAM
Aslı Islak İmzalıdır

***LİSANSÜSTÜ TEZLERİN ELEKTRONİK ORTAMDA TOPLANMASI, DÜZENLENMESİ VE ERİŞİME AÇILMASINA İLİŞKİN YÖNERGE**

.....

ÜÇÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Lisansüstü tezlerin erişime açılmasının ertelenmesiMADDE 6– (1) Lisansüstü tezle ilgili **patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda**, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu **iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.**

(2) Yeni teknik, materyal ve metotların kullanıldığı, henüz **makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış** ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile **altı ayı aşmamak üzere tezin erişime açılması engellenebilir**.

Gizlilik dereceli tezler MADDE 7– (1) Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.

(2) Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

SOSYAL BİLİMLER ENSTİTÜSÜ
Graduate School of Social Sciences

TEZ KABUL TUTANAĞI

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Doç. Dr. Abdulkadir ÖZDEMİR danışmanlığında, Rabia SAYLAM tarafından hazırlanan bu çalışma 02/07/2020 tarihinde aşağıda isimleri yazılı jüri tarafından Yönetim Bilişim Sistemleri Anabilim Dalı'nda Doktora Tezi olarak kabul edilmiştir.

Başkan	:Prof. Dr. Sibkat KAÇTIOĞLU	İmza: Aslı Islak İmzalıdır
Jüri Üyesi	: Prof. Dr. Abdullah NARALAN	İmza: Aslı Islak İmzalıdır
Jüri Üyesi	: Doç. Dr. Abdulkadir ÖZDEMİR	İmza: Aslı Islak İmzalıdır
Jüri Üyesi	: Dr. Öğr. Üyesi Bilal USANMAZ	İmza: Aslı Islak İmzalıdır
Jüri Üyesi	: Dr. Öğr. Üyesi Serdar AYDIN	İmza: Aslı Islak İmzalıdır

Prof. Dr. Sait UYLAŞ
Enstitü Müdürü

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM
ASKERİ ALANDA NESNELERİN İNTERNETİNİN KULLANIMI VE KABUL MODELİ

ÖZET

DOKTORA TEZİ

NESNELERİN İNTERNETİ (IoT)'NİN ASKERİ ALANDA KULLANILABİLİRLİĞİ VE KABUL MODELİ ÖNERİSİ

Rabia SAYLAM

Tez Danışmanı: Doç. Dr. Abdulkadir ÖZDEMİR

2020, 128 Sayfa

Jüri: Prof. Dr. Sibkat KAÇTIOĞLU
Prof. Dr. Abdullah NARALAN
Doç. Dr. Abdulkadir ÖZDEMİR
Dr. Öğr. Üyesi Serdar AYDIN
Dr. Öğr. Üyesi Bilal USANMAZ

Bu tez çalışmasında, önümüzdeki yıllar içinde savaşta baskın bir varlık haline gelmesi muhtemel görünen Nesnelerin İnterneti (IoT)'nin kaynağı olduğu büyük veriden başlayarak; teknolojileri, askeri alan içinde getirileri, alanın doğası gereği ortaya çıkan gereksinimleri incelenmiştir. Çalışma bu anlamda askeri IoT alanıyla ilgilenen araştırmacılara, bilim insanlarına ve karar verici komutanlara kapsamlı bir bilgi sağlamaktadır.

Öte yandan her yeni teknolojide olduğu gibi bu teknolojiyi kullanacak ya da bir parçası olacak personel tarafından IoT'ye yönelik tutumun belirlenmesinin önemli olduğu değerlendirilmiş ve askeri koşullar göz önüne alınarak bir kabul modeli geliştirilmiştir. Yapılan anket uygulamasında açık uçlu sorularla personelin görüşleri alınırken, likert tipi ölçekler ile bu teknolojinin kullanımını etkilediği savunulan ve kabul modelinde yer alan faktörlerin incelenmesi amaçlanmıştır.

Analiz sonuçları personelin en büyük çekincelerinin güvenlik, gizlilik ve siber tehditler üzerine yoğunlaştığını ancak yine de kullanıma yönelik olumlu yönde görüş ortaya koyduklarını göstermektedir. Bu çalışmanın sonuçları IoT teknolojisinin askeri alanda uygulanabilirliğini etkileyen faktörleri ortaya koyarak, önümüzdeki yıllarda bu kapsamda yapılacak konsept, planlama ve ihtiyaç duyulacak yeni yönetim anlayışına yön verebilecektir.

Anahtar Kelimeler: Nesnelerin İnterneti, IoT, Askeri IoT, Teknoloji Kabul Modeli

ABSTRACT

Ph. D. DISSERTATION

APPLICABILITY OF THE INTERNET OF THINGS (IoT) IN MILITARY ENVIRONMENT AND A PROPOSED ACCEPTANCE MODEL

Rabia SAYLAM

Advisor: Assoc. Prof. Dr. Abdulkadir ÖZDEMİR

2020, 128 Pages

Jury: Prof. Dr. Sibkat KAÇTIOĞLU
Prof. Dr. Abdullah NARALAN
Assoc. Prof. Dr. Abdulkadir ÖZDEMİR
Asst. Prof. Dr. Serdar AYDIN
Asst. Prof. Dr. Bilal USANMAZ

The subject of the thesis is firstly to examine the Internet of Things (IoT), which seems likely to become a dominant presence in the battlespace over the next few decades, starting examining the big data from which it is originated, and then scrutinizing relative technologies, the benefits within the military field and the requirements arising due to the nature of the field. In this sense, the study provides comprehensive information to researchers, scientists interested in the military IoT field and to the decision maker commanders.

In addition, like any other new technology, it is considered important to determine the attitude towards IoT by the personnel who will use or will be a part of this technology and an acceptance model is proposed considering its unique military conditions. In the survey, the opinions are collected via open-ended questions and also it is aimed to examine the factors included in the acceptance model, which is hypothesized to be associated with the use of this technology using likert-scale questions.

The results of the analysis show that the biggest concerns of the personnel are pointed on security, privacy, and cyber threat while, at the same time, they have positive opinions about attitude towards its usage. The results of this study would identify the factors affecting the applicability of IoT in military battlespace, that, it may help to draw a roadmap for future concept, plans, and required new management approach.

Keywords: Internet of Things, IoT, Military IoT, Technology Acceptance Model

KISALTMALAR DİZİNİ

ABD : Amerika Birleşik Devletleri
AFA : Açıklayıcı Faktör Analizi
AMQP : Gelişmiş Mesaj Kuyruğu Protokolü
ANT : Uyarlanabilir Ağ Topolojisi
BLE : Bluetooth Düşük Enerji
BT : Bilgi Teknolojileri
CFI : Karşılaştırmalı Uyum İndeksi
CoAP : Kısıtlı Uygulama Protokolü
C2 : Komuta ve Kontrol
C4ISR : Komuta, Kontrol, İletişim, Bilgisayar, İstihbarat, Gözetleme ve Keşif Konsepti
df : Serbestlik Derecesi
DFA : Doğrulayıcı Faktör Analizi
DLA : Savunma Lojistik Ajansı
DoD : ABD Savunma Bakanlığı
GFI : Uyum İyiliği İndeksi
GFS : Google Dosya Sistemi
GSM : Mobil İletişim İçin Küresel Sistem
HDFS : Hadoop Dağıtılmış Dosya Sistemi
HTTP : Hiper Metin Aktarım Protokolü
IDC : Uluslararası Veri Şirketi
IEEE : Elektrik ve Elektronik Mühendisleri Enstitüsü
İHA : İnsansız Hava Aracı
IoT : Nesnelerin İnterneti
IoV : Araçların İnterneti
LTE : Uzun Dönem Evrim
LTE-A : Gelişmiş Uzun Dönem Evrim
NATO : Kuzey Atlantik Antlaşması Örgütü
NFC : Yakın Alan İletişimi
NFI : Normlandırılmış Uyum İndeksi
NoSQL : SQL ve Daha Fazlası

OAA	: Açık Oto İttifakı
QoS	: Servis Kalitesi
RFID	: Radyo Frekans Tanımlama
RMSEA	: Tahminlemenin Ortalama Karesel Hatasının Karekökü
SIG	: Özel İlgi Grubu
SOA	: Servis Odaklı Mimari
SPSS	: Sosyal Bilimler İçin İstatistik Paketi
SQL	: Yapılandırılmış Sorgu Dili
STO	: Science and Technology Organization
TCP	: İletim Kontrol Protokolü
TKKBM	: Teknoloji Kabul ve Kullanım Birleştirilmiş Modeli
TKM	: Teknoloji Kabul Modeli
UCI	: Evrensel Komuta ve Kontrol Arayüzü
UDP	: Kullanıcı Datagram Protokolü
UMTS	: Evrensel Mobil Telekomünikasyon Sistemi
USTRANSCOM	: ABD Ulaştırma Komutanlığı
UWB	: Ultra Geniş Bant
WSN	: Kablosuz Sensör Ağı
XML	: Genişletilebilir İşaretleme Dili
YEM	: Yapısal Eşitlik Modeli
YYT	: Yeniliklerin Yayılması Teorisi

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

ÖNSÖZ

Doktora ve tez çalışmamın her aşamasında yapıcı ve yönlendirici kişiliği ile yardımlarını hiçbir zaman esirgemeyen danışman hocam Doç. Dr. Abdulkadir Özdemir'e, Yönetim Bilişim Sistemleri Bölüm Başkanı Prof. Dr. Üstün ÖZEN başta olmak üzere, bölüm öğretim üyelerine, tez izleme komitesinde yer alan ve değerli girdileri ile tezime yön veren Dr. Öğr. Üyesi Serdar AYDIN ve Dr. Öğr. Üyesi Bilal USANMAZ'a teşekkürü bir borç bilirim.

Doktora çalışmam boyunca desteğe ihtiyacımız olan her an koşulsuz yanımızda olan anneme, babama, kayınvalideme ve kardeşime, anlayışı ve desteği ile hayatımı kolaylaştıran yol arkadaşım, eşim Serhat'a minnettarım. Onlar olmasaydı bu çalışmayı tamamlayamazdım.

Son olarak doktora ve tez çalışmamla beraber büyüyen, yaşam kaynağım, canım oğullarım Mustafa Mert ve Kemal Yiğit'e bir gün gurur duyacakları ve örnek alacakları bir çalışma yapabilmiş olma umuduyla…

Erzurum-2020 **Rabia SAYLAM**

GİRİŞ

Teknolojinin zaman içinde ilerlemesiyle meydana gelen veri miktarındaki olağanüstü artış büyük veri kavramını literatüre ve hayatımıza katmıştır. Aslında bu teknoloji, sadece artan veri boyutunu değil, boyutla beraber çeşitlilik, gerçeklik ve değer gibi kavramları da içermektedir. Büyük veri, çeşitli veri paketlerinden yüksek hızda veri yakalama, keşfetme, analiz etme ve ekonomik olarak değer elde etme amacıyla tasarlanmış yeni nesil teknoloji ve mimariyi de kapsamaktadır.

Büyük miktarda depolama, işleme gerektiren bu verinin nereden geldiği ise önemli sorulardan biridir. Hiç kuşkusuz ilk aklan gelen örnekler; kitaplar, fotoğraflar, ses ve videolar ve bunların yanında insanların son derece öznel kayıtları olan sosyal medya verileridir. Daha çok iş insanlarının içerisinde olduğu iş süreçleri, ürün imal etme, sipariş alma vb. alanlarından elde edilen iş sistemleri verileri ve son olarak bu verilerin önemli kaynaklarından biri olan makinaların ürettiği verilerdir. Nesnelerin İnterneti (IoT), sıcaklık, ağırlık, ses gibi değerleri ölçen basit sensörlerden, karmaşık bilgisayar kayıtlarına kadar büyüdükçe büyüyen veri kapasitesine sahiptir.

Büyük veri ve IoT, günlük rutinlerimizden eğitim, iş ve bilim dünyasına kadar geniş yaşam çerçevemizi değiştirmektedir. Hayatımıza kolaylık katan akıllı ev uygulamaları, zamanı göstermenin çok ötesine geçmiş akıllı saatler, sağlık uygulamaları yaygın olarak bilinirken; değişime uğrayan önemli alanlardan biri de askeri alan uygulamalarıdır. Gelecekteki savaş alanı yoğun olarak çeşitli nesnelerle dolu olacaktır. Nesneleri ve personeli iş birliği içinde, senkronize bir şekilde çalışabilen sistemlere dönüşüm kaçınılmazdır. Nesneler arasında sensörler, mühimmat, silahlar, robotlar ile insanlı-insansız araç ve cihazlar bulunacaktır. Seçici bir şekilde veri toplama, işleme, koordineli savunma eylemleri gerçekleştirme, rakipler üzerinde çeşitli etkiler yaratma ve müttefikler ile ortak harekât icra edebilme yeteneği kazanma gelecekteki orduları farklı kılacaktır.

Askeri alan içinde bu teknolojinin avantajları olduğu gibi, birçok kısıtlama ve gereksinimi bulunmaktadır. İhtiyaç ve kısıtlamaların bazıları teknik altyapının geliştirilmesini gerektirirken, bazı ihtiyaçlar yönetimsel çerçevede ele alınmalıdır. Geleceğin orduları geleneksel yöntemlerin aksine, süreçleri gözlemleyecek, insan ve nesnelerin ordusunu yönetecek yeni bir komuta kontrol yönetim sistemine ihtiyaç duyacaktır.

Literatür ve açık kaynaklı haberler incelendiğinde özellikle Amerika Birleşik Devletleri destekli enstitüler ve araştırmacıların bu alana öncülük ettiği gözlemlenmektedir. Elektrik ve Elektronik Mühendisleri Enstitüsü Dünya IoT Forumunda (IEEE World Forum on IoT) IoT Askeri Uygulamalarına yönelik özel oturum açılması bu alana olan yönelimi göstermektedir.

Bunun yanında, NATO Bilim ve Teknoloji Organizasyonu (Science and Technology Organization-STO) IoT Askeri Uygulamaları Araştırma Çalışma Grubu (IST-147 (COM)) 2016-2019 yılları arasında, Askeri Komuta Kontrol ve IoT Sistemlerinin Federasyonla Birlikte Çalışabilirliği Çalışma Grubu (IST-176 (COM)) 2019-2022 yılları arasında çalışmalarını sürdürmektedir.

IoT teknolojisi veya herhangi bir yeni teknolojiye adapte olurken; bunları kullanacak ya da bir parçası olacak kişilerin teknoloji tercihlerini belirlemek, değişikliklere nasıl tepki verebileceklerini, uyum sağlayıp sağlayamayacaklarını tahmin etmeye çalışmak çok önemlidir. Her geçen gün yeni bir teknoloji ile karşı karşıyayız. Bazı teknolojiler hızlıca kabul görürken bazıları beklenmedik bir şekilde reddediliyor.

Bu çalışmanın amacı, akıllı nesnelerle donatılmış (zaten kısmen donanımlı) geleceğin ordularında IoT'nin kullanılabilirliğini, bu teknolojiyi kullanacak veya bir parçası olacak personel açısından değerlendirmek ve bu teknolojinin kişiler üzerinde etkisini incelemektir. Uzun yıllar içinde askeri uygulamalar bilinen pek çok teknolojinin çıkış noktası olurken, rekabetçi piyasa ekonomisi içinde firmalar bu geleneği değiştirerek yeni teknoloji alanlarına öncülük etmeye başladılar. Komutanlar alan içinde her yeni teknolojinin erken kullanıcılarından olmayabiliyorlar. Bu maksatla personelin görüşleri, hazırlanan anket (EK 1-2) içinde hem açık uçlu sorular vasıtasıyla hem de likert tipi sorular ile alınmıştır. Sonuçlar, öneri ve çekinceleri gözler önüne sererken, geliştirilen kabul modelinin değerlendirilmesini ele almıştır.

Tez üç bölümden oluşmaktadır. Tezin birinci bölümünün ilk kısmında büyük veri, literatürde yer alan V'ler aracılığıyla tanımlanmakta, başarıya götüren faydalarının yanı sıra kısıtlarına yer verilmekte, büyük veriyi oluşturan ve uygulanmasını sağlayan teknolojiler açıklanmaktadır. Teknolojinin daha iyi açıklanması maksadıyla çeşitli sınıflandırmaları yapılmakta ve büyük veri kaynakları sosyal ağlar, geleneksel iş sistemleri ve IoT olmak üzere sınıflandırılarak tanımlanmaktadır. Büyük veri

kaynaklarından biri olan IoT birinci bölümün ikinci kısmıdır. IoT altında sensör, iletişim kanalları ve hesaplama ana unsurları ile bu teknolojiyi mümkün kılan mimari ve protokollere ayrı alt başlıklarda yer verilmektedir. Sonrasında ise kullanılan ya da kullanımı öngörülen alanlar listelenmektedir. Bu alanlardan biri de bu çalışmanın ana konusu olan askeri alandır. Birinci bölümün son kısmında askeri IoT uygulamalarına derinlemesine yer verilmiş, alana özgü teknolojik ve yönetimsel gereksinim ve kısıtlar ayrı başlıklar altında sunulmuştur.

İkinci bölümde, tüketicilerin yeni teknolojileri kabullerini ve kullanım niyetlerini açıklamak için tasarlanan model ve teoriler yer almaktadır. Çalışmamıza temel olan, Teknoloji Kabul Modeli (TKM) en yaygın ve bilinen model olarak çeşitli uyarlamaları ile açıklanırken, geliştirilen modelimizde kullanılan bir diğer teori olan Yeniliklerin Yayılması Teorisi (YYT) de detaylı olarak açıklanmıştır. Çalışmamızın konusu kapsamında ikinci bölümün son kısmında geçmiş çalışmalar iki alt başlık altında incelenmiştir. Bunlar, IoT alanında kabul çalışmaları ve askeri alanda farklı teknolojilere ilişkin kabul çalışmalarıdır.

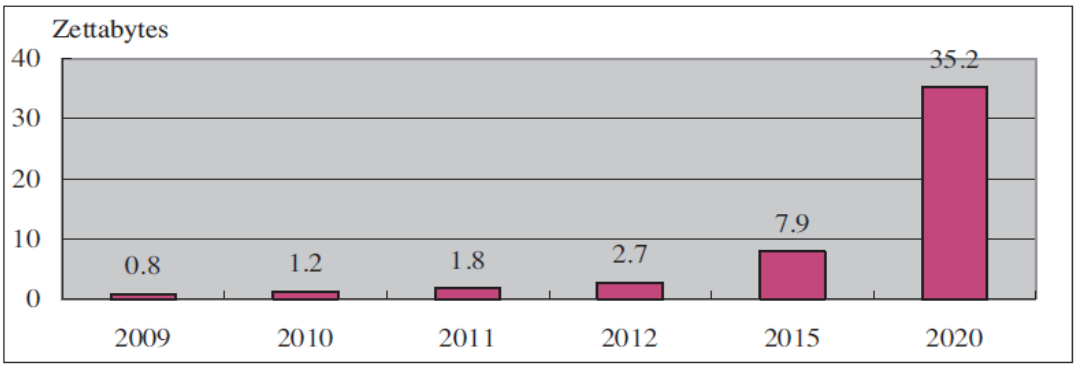
Üçüncü bölüm, araştırmanın amacının, alana katkısının yer aldığı, literatür ve alan tecrübesi göz önüne alınarak önerilen model ve hipotezlerin açıklandığı bölümdür. Modelin ve hipotezlerin değerlendirilebilmesi için hazırlanan anket, veri toplama aşaması ve sınırlılıkları ayrı başlıklar altında sunulmuştur. Bu bölümün son kısmı olan bulgular başlığı altında anket sonuçları değerlendirilerek; demografik analizler, öneri ve çekincelerin analizi, betimsel analizler, güvenilirlik ve geçerlilik analizleri ile Yapısal Eşitlik Modeli (YEM) sonuçlarına yer verilmiştir.

Sonuç ve öneriler bölümü ile uygulanan anket sonucu elde edilen analizler özetle yorumlanmıştır. Son olarak öneriler kısmında geleceğin kaçınılmaz teknolojisi olan IoT'nin askeri alanda silah mı yoksa hedef mi olacağı tartışılmış, açıkça risk görülen alanlara yönelik çalışma alanları sunularak çalışma tamamlanmıştır.

BİRİNCİ BÖLÜM

BÜYÜK VERİ KAYNAĞI OLARAK NESNELERİN İNTERNETİ

Veri, sosyal medya ağları, sensörler ve satın alma işlemleri gibi akla gelebilecek pek çok kaynakla birlikte özellikle son yıllarda büyük artış göstermiştir. Veri artış hızı şimdiden Moore Yasasının öngörülerini geçmiştir. Uluslararası Veri Şirketi (IDC) tarafından sağlanan dünya çapında tahmini veri hacmi sonuçları Şekil 1.1'de (Wang ve diğerleri, 2016) yer almaktadır. Açıkça görülmektedir ki "Büyük Veri" (Big Data) dönemi çoktan gelmiştir. 2003'ten itibaren yavaşça büyüyen büyük verinin en az 2030'a kadar Bilgi Teknolojileri (BT) sektörlerini domine etmesi beklenmektedir.



Şekil 1.1. IDC Tarafından Tahmin Edilen Dünya Çapında Veri Hacmi

Evlerden, iş yerlerine ve okullara hayatımızın dokunmadığı alanı kalmayan bilgi teknolojileri, sensörler, gelişen depolama ve işleme yöntemleriyle hayal edilenin ötesine geçmiş durumdadır.

1.1. BÜYÜK VERİ

Verinin büyüklüğü bir başka deyişle hacmi, verinin önemli bir kısmını ifade etmekte ama tamamını ifade edememektedir (Ahmed ve Patgiri, 2016). Verilerin karmaşık yapısı, veriyi ele alma ve yönetme karmaşıklığı büyük veri kavramını bir araya getirmektedir. Tanıtıldığı günden beri, büyük veri hem bilimsel hem de mühendislik alanında en popüler konulardan biri haline gelmiştir (Wang ve diğerleri, 2016).

İnternet şirketleri, çok büyük ölçüdeki bu veriyi neredeyse gerçek zamanlı olarak kullanarak başarılı büyük veri yatırım projelerine öncülük etmektedir. Facebook her gün yaklaşık bir milyar içerik sorguyla ilgilenmekte, Netflix her gün milyonlarca öğeyi arayan

ve ekleyen üyelerle milyarlarca izleyici derecelendirmesini bir araya getirmektedir. Önce müşteri reytingi kullanarak kalabalığa dayalı bir algoritma yoluyla, daha sonra, geniş bir veri yelpazesinin püf noktalarından yeni bilgiler edinebilen makine-öğrenme tabanlı algoritmalar aracılığıyla içerik öneri motorunu geliştirmek için büyük veriyi kullanmıştır. Büyük veri üretimli öneriler kullanıldığında, Netflix filmi veya dizisi izleme sayısı dört kat artmıştır. Google, daha hızlı arama sorgusu oluşturmak için çok fazla sayıda deneme yapmaktadır. Birkaç mikro saniye, harcanan ek milyonlarca dolarlık paraya çevrilmektedir (Bughin, 2016).

Büyük verinin özellikleri ve ikilemleri, İngilizce 'V' harfleri ile başlayan terimlerle ele alınmaktadır.

1.1.1. Büyük Verinin V'leri

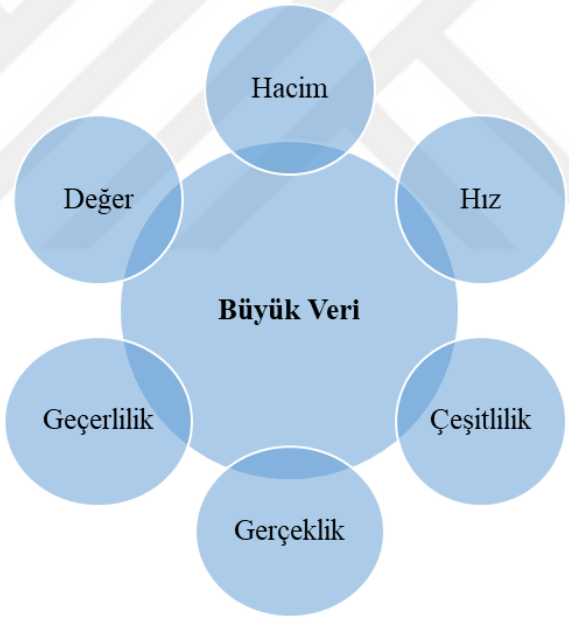
Burada büyük verinin özelliklerini açıklamada İngilizce 'V' ile başlayan tanımlamalar kullanarak hatırlamada kolaylık sağlanması amaçlanmıştır. Daha değişik sayıda 'V' ile detaylandırılan tanımlamalar mevcut olmakla birlikte, büyük verinin V'leri çalışmamızda Şekil 1.2'de yer alan başlıklar altındaki özellikleri ile açıklanmıştır.

Hacim (Volume)

Veri hacmi bilim, eğitim, iş ve insan etkileşimi gibi pek çok alanda oluşan, saklanacak ve işlenecek büyük veri kümesini ifade eder. Hacim depolama ve işlemede önemli bir rol oynar. Veriler, veri tabanlarında ve veri ambarında manuel olarak veya otomatik olarak toplanır. Depolama kapasitesi, bir yandan hızla gelişen depolama teknolojileri ve diğer yandan depolama fiyatlarının düşmesi ile işlemeye oranla daha kolay yönetilebilmektedir. Uygun maliyetli depolama çözümleri ve bulut teknolojileri organizasyonlara veri depolama fırsatı sunar. Bununla birlikte, veri hacminin veri işleme, veri yönetimi ve karar verme üzerinde temel bir etkisi vardır (Khan ve diğerleri, 2018). Çünkü veri boyutu, işleme sisteminin hesaplama gücüne kıyasla daha hızlı büyümektedir. Hacim gelecekte Zettabayt (10^{21}bayt), Yottabayt (10^{24}bayt) veya ötesine yayılabilir (Ahmed ve Patgiri, 2016). Teknoloji, artan veri büyüklüğü ile başa çıkmayı sağlayabilmelidir. Bu verilerin yönetimi büyük önem arz etmektedir. Uygun ortamlarda saklanmalı, işlenmeli ve ihtiyaca uygun olarak organizasyon ve kişilere sunulmalıdır.

Hız (Velocity)

Hız, veri işleme hızını ifade eder. Temel olarak iki öğe ile, yani büyüme hızı ve transfer hızı ile ilgilidir (Ahmed ve Patgiri, 2016). Verinin işlenme hızının, verilerin üretilme hızını karşılaması gerekmektedir. Örneğin; IoT cihazları sürekli olarak büyük miktarda sensör verisi üretir. Veri başka veriyi doğurur. Sağlık alanında kullanılan doktora veya bir tesise acil durum bildiren kalp pilleri düşünüldüğüne, verilerin işlenmesinde ve sonuçların ilgili birimlere gönderilmesinde gecikmeler olduğunda hastanın ciddi zarar görmesine hatta ölümüne neden olabilir. Benzer şekilde, siber-fiziksel alandaki cihazlar genellikle yürütme konusunda katı zamanlama standartları uygulayan gerçek zamanlı işletim sistemlerine dayanır ve bu nedenle büyük bir veri uygulamasından sağlanan veriler zamanında teslim edilemediğinde sorunlarla karşılaşabilir (Hariri ve diğerleri, 2019).



Şekil 1.2. Büyük Verinin V'leri

Çeşitlilik (Variety)

Çeşitlilik, çeşitli veri formlarıdır. Bunlar yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış verileri içerir. Yapılandırılmış veriler bir veri formu, yarı yapılandırılmış veriler, log verisini, Genişletilebilir İşaretleme Dili (Extensible Markup Language-XML) verilerini ve yapılandırılmamış veriler videolar, görüntüler, bilimsel bilgiler gibi verileri içerir (Ahmed ve Patgiri, 2016). İnternet ve sosyal medya çağında veriler çoğunlukla video, ses klipleri, görüntüler ve metinler biçimindedir. Örneğin

YouTube kullanıcılar tarafından her dakika 400 saatlik video yüklendiğini bildiriyor ve bu oran sürekli olarak artıyor. Benzer oranlar Facebook, Twitter, Instagram ve diğer sosyal medya ağları için de geçerlidir. Çeşitliliğe katkıda bulunan bir başka faktör de çok sayıda satıcının ve tedarikçinin varlığı ile birçok alanda standardizasyon eksikliğidir (örneğin, farklı sensör cihazları genellikle uyumsuz veri formatları kullanır). Basit metinsel bilgileri ifade etmek için kullanılan insan dilindeki fark bile, farklı veri kümeleri arasında heterojenlik yaratır. (Dautov ve Distefano, 2017) Veri kümeleri boyut olarak büyüdükçe, ilişkisel veri biçimi birincil veri depolama biçimi olmayı bırakmaktadır. Geleneksel yöntemler ile bu verileri saklamak, işlemek ve yönetmek mümkün olmayacaktır.

Gerçeklik (Veracity)

Gerçeklik doğruluk, tutarlılık ve güvenilirlik gibi verilerin kalitesini ifade eder. Veriler doğru ve tutarlı olduğu gibi güvenilir bir sistem tarafından oluşturulmalıdır. Büyük hacimli veriler üzerinde bir miktar işlem yapmak istediğimizde veri sorunlu hale gelebilmektedir. Yapılan operasyonların başarılı olduğu hangi verilerle kanıtlanabilir? Tehlikeli olan yanlış veriler yanlış kararlar alınmasına yol açabilir (Ahmed ve Patgiri, 2016).

Geçerlilik (Validity)

Verilerin geçerliliği, verilerin gerçekliği ile aynı fikirlere sahip olabilir, ancak aslında aynı kavramlara ve teorilere sahip değildirler. Verilerin durumu keşiften eyleme geçer hale geldiğinde, veriler geçerli olmalıdır. Bir veri kümesinde herhangi bir doğruluk problemi olmayabilir, görev doğru gerçekleşmiş olabilir ancak geçerliliğini yitirmiş veriler sonucunda yapılan analizler doğru sonuçları vermeyecektir. Geçerlilik zamana göre farklılık gösterebilir. Benzer şekilde, belirli bir uygulama veya kullanım için bir veri kümesi doğrulanabilir ancak başka bir uygulama veya kullanım için geçersiz olabilir (Khan ve diğerleri, 2018). Örneğin barfiks kol gücünü ölçmekte çok doğru ve gerçek bir yöntemdir ama bacak gücünü ölçme için geçerli değildir. Büyük Veri üreten kaynakların geçerliliği ve sonuçta yapılan analizler tam olarak doğru olmalıdır.

Değer (Value)

Daha önce açıklanan V'ler daha çok büyük verilerdeki zorlukları temsil etmeye odaklanırken; Değer, karar verme için verilerin bağlamını ve kullanışlılığını temsil eder.

Örneğin, Facebook, Google ve Amazon, ilgili ürünlerindeki analizler yoluyla büyük verilerin değerini kullandılar. Amazon, ürün önerileri sağlamak için büyük kullanıcı veri kümelerini ve satın alımlarını analiz eder, böylece satış ve kullanıcı katılımını artırır. Google, Google Haritalar'daki konum hizmetlerini iyileştirmek için Android kullanıcılarından konum verileri toplar. Facebook, hedefli reklamcılık ve arkadaş önerileri sağlamak için kullanıcıların etkinliklerini izler (Hariri ve diğerleri, 2019). Bu verinin değerini anlayabilen şirketler ve organizasyonlar, büyük ham veri kümelerini inceleyerek ve daha iyi iş kararları almak için faydalı bilgiler elde ederek büyük kitleler haline geldiler.

1.1.2. Büyük Verinin Faydaları

Büyük veri artan 'değeri' sayesinde, yaşadığımız ve çalıştığımız dünyayı, düşünme şeklimizi değiştirmekte ve dönüştürmektedir. Büyük verinin farklı perspektiflerde getirileri vardır.

Ulusal kalkınma

Ulusal düzeyde, büyük miktarda veri biriktirme, işleme ve kullanma kapasitesi, ülkenin gücünün yeni bir simgesi haline gelecektir. Bir ülkenin siber uzayda veri egemenliği; kara, deniz, hava ve uzay ortamlarının (domain) yanı sıra bir başka büyük güç ortamı olmaya başlamıştır. Amerika Birleşik Devletleri'nin (ABD) Mart 2012'de açıkladığı Büyük Veri Araştırma ve Geliştirme Girişimi, ABD'yi yalnızca yüksek teknoloji alanlarında öncülük etmeye teşvik eden bir stratejik plan değil, aynı zamanda ulusal güvenliğini ve sosyo-ekonomik gelişimini koruma amaçlı bir plandır. Gelecekte, ülkeler arasındaki ekonomik ve politik yarışların, diğer geleneksel unsurların yanı sıra, büyük verilerin potansiyelini kullanma temeline dayanacağı öngörülmektedir. Kısacası, büyük verilerin araştırılması ve uygulamaları, herhangi bir ülkenin rekabet gücünü artırmak için stratejik öneme sahiptir (Jin ve diğerleri, 2015).

Endüstriyel iyileştirme

Büyük veri ihtiyacına dayalı olarak, birikmiş veriden bilgi elde etmek ve sonuçta büyük verinin büyük değerinden tam olarak yararlanmak beklentisi vardır. Yani bu verinin sanayi sektörünün bir yan ürünü değil, tüm yönleriyle sanayinin kilit bir öğesi haline geldiği anlamına gelmektedir (Jin ve diğerleri, 2015).

Bilimsel araştırma

Büyük veri, bilimsel topluluğun bilimsel araştırma metodolojisini yeniden incelemesine, bilimsel düşünce ve yöntemlerde bir devrimi tetiklemesine neden olmuştur. İnsanlık tarihindeki en eski bilimsel araştırmasının deneylere dayandığı bilinmektedir. Daha sonra, çeşitli yasa ve teoremlerin incelenmesiyle karakterize edilen teoriye dayalı bilim ortaya çıkmıştır. Ancak, teoriye dayalı analiz çok karmaşık ve pratik problemleri çözmede uygun olmadığı için, insanlar hesaplama bilimlerine yol açan simülasyon temelli yöntemleri aramaya başlamışlardır. Büyük verilerin ortaya çıkması yeni bir araştırma paradigması doğurmuştur. Araştırmacılar çalışılacak nesneye doğrudan erişmek yerine, gerekli veri ve bilgiye erişmeyi benimsemeye başlamışlardır (Jin ve diğerleri, 2015).

Disiplinler arası araştırma

Son yıllarda disiplinler arası çalışmaları kapsayan veri bilimi literatürde yerini almıştır. Araştırma nesnesi olarak veri bilimi, büyük veri ve veriden anlamlı bilgi elde etmeyi amaçlamaktadır. Bu alan, bilgi bilimi, matematik, sosyal bilimler, ağ bilimleri, sistem bilimi, psikiyatri ve ekonomi gibi birçok disiplini kanatları altına almaktadır.

Sinyal işleme, olasılık teorisi, makine öğrenimi, istatistiksel öğrenme, bilgisayar programlaması, veri mühendisliği, örüntü tanıma, görselleştirme, belirsizlik modelleme, veri ambarı ve yüksek performanslı bilgi işlem gibi birçok alandan çeşitli teknikler ve teoriler kullanır.

Dünyadaki farklı üniversitelerde (California Üniversitesi, Columbia Üniversitesi, New York Üniversitesi, Tsinghua Üniversitesi, Eindhoven Teknoloji Üniversitesi ve Hong Kong Üniversitesi gibi) son yıllarda büyük veri üzerine birçok araştırma merkezi / enstitüsü kurulmuştur (Jin ve diğerleri, 2015).

İnsanların şimdiki zamanı daha iyi algılamasına yardımcı olmak

Büyük veri, özellikle büyük ağ bağlantılı veriler, zengin bir toplumsal bilgi içerir ve bu toplumu haritalayan bir ağ olarak görülebilir. Bu amaçla, büyük verileri analiz etmek, dolaylı olarak içerdiği ipuçlarını özetlemek ve bulmak, şimdiki zamanı daha iyi anlamamıza yardımcı olabilir (Jin ve diğerleri, 2015).

İnsanlara geleceği daha iyi tahmin etmelerine yardımcı olmak

Çok kaynaklı heterojen büyük veriler üzerinde etkili entegrasyon ve doğru analiz sayesinde, gelecekteki olayların daha iyi tahminleri elde edilebilir. Büyük veri analizinin, toplumun ve ekonominin sürdürülebilir gelişimini teşvik etmesinin yanı sıra veri hizmetleriyle ilgili yeni endüstrileri doğurması da mümkündür (Jin ve diğerleri, 2015).

1.1.3. Büyük Verinin Kısıtları

Bir dizi başarı öyküsüne rağmen, büyük veri ile ilgilenen kuruluşların çoğunun karşılaştığı kısıtlar ve zorluklar bulunmaktadır. Bu zorlukların kapsamlı bir şekilde anlaşılması, organizasyonların, büyük verilerle ilgili karar vermelerine, karar olumlu ise; zorlukların sorunsuz bir şekilde üstesinden gelmelerine olanak sağlar.

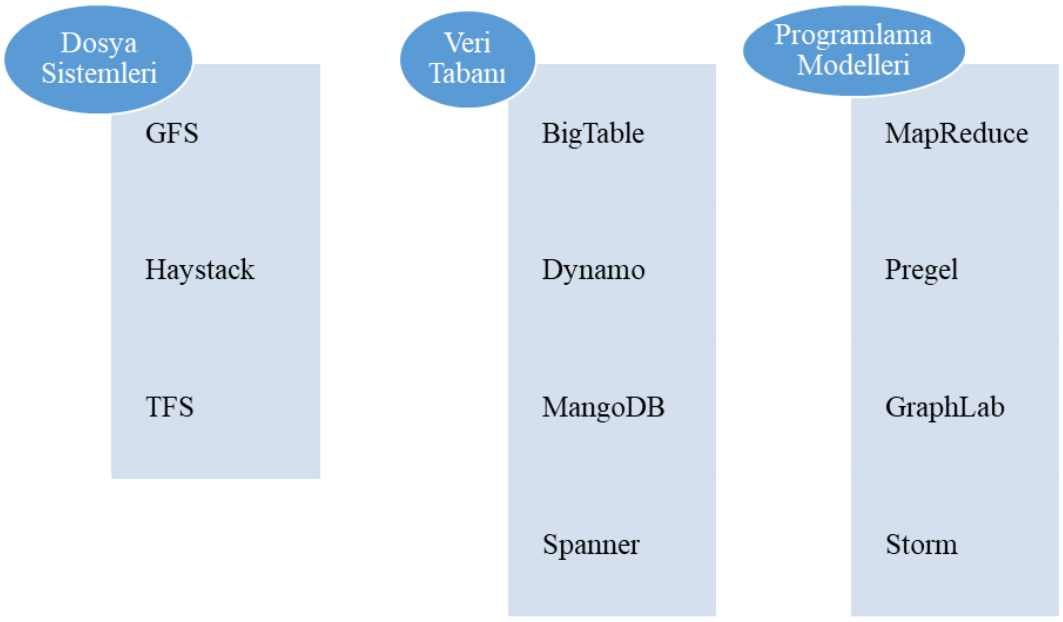
Bachlechner ve Leimbach (2016)'ın çalışmalarına göre bu kısıtlar Şekil 1.3'te yer alan üç temel kategoriye ayrılmıştır. Düşünülenin aksine kısıtlar sadece teknolojik değil, organizasyon ve insan faktörlerini, bunun yanında temel kategorilerin ilişkilerinden doğan kombinasyonları da içerir.

Şekil 1.3. Büyük Verinin Kısıtları

Kullanım durumlarının tanımlanması bir organizasyonel meseledir, öte yandan gelişmiş analitiği yürütmek ise teknolojiktir. Yetkin uzmanları işe almak insanlarla ilgili bir konudur. Kombinasyonları ele alınacak olursa; teknik bir mimarinin kurulması için, organizasyonel ve teknolojik faktörlerin kesişimi dikkate alınması gerekir. Teknik bir mimarinin kurulması hem örgütsel hem de teknolojik açıdan önemlidir. Bu mimarinin, kuruluşun belirli büyük veri kullanım durumlarından kaynaklanan gereksinimlerini karşılaması ve teknolojik fizibiliteye saygı göstermesi gerekir. Organizasyon departmanları arasındaki iş birliğinin teşvik edilmesi ise hem organizasyonel hem de insanlarla ilgili konuları dikkate almayı gerektirir. Kullanılır çözümler üretilmesi hem teknolojik fizibilite hem de bireysel kullanıcı gereksinimlerinin göz önünde bulundurulmasını gerektirir. Hepsinin kesiştiği, her üç kavramla ilgili olan ise merkezde yer alan güven'dir. İnsanların hem teknolojiye hem de meslektaşlarına güvenmeleri gerekmektedir. Büyük veri bağlamında bir güven kültürü oluşturmak bir organizasyon meselesidir (Bachlechner ve Leimbach, 2016).

1.1.4. Büyük Veri Teknolojileri

Büyük veri teknolojileri, veri yönetimi çerçevesinde Şekil 1.4'te gösterildiği gibi dosya sistemleri, veri tabanı teknolojisi ve programlama modellerinden oluşan üç katmanda bazı örneklerle detaylandırılmıştır.



Şekil 1.4. Büyük Veri Teknolojileri

1.1.4.1. Dosya Sistemleri

Dosya sistemi büyük veri depolamasının temelidir ve bu nedenle hem endüstriden hem de akademiden büyük ilgi görmektedir. Örneğin;

- Google, büyük dağıtılmış veri uygulamaları için ölçeklenebilir dağıtılmış bir dosya sistemi olarak Google Dosya Sistemini (GFS- Google File System) tasarladı. GFS, çok sayıda müşteriye hata toleransı ve yüksek performans sağlamak için ucuz emtia sunucularında çalışır. Google, milyarlarca internet sayfasına ev sahipliği yapmaktadır. Bu sayfaların analizlerini bu sistem üzerinde tutmaktadır (Karabay ve Ulaş, 2017).
- Facebook, büyük miktarda küçük dosya içeren fotoğrafları depolamak için Haystack'ı geliştirdi. Küçük dosyalar için benzer dağıtılmış dosya sistemi, Tao Dosya Sistemi (TFS) Taobao tarafından önerilmiştir. Dosya sistemleri, uzun süren büyük ölçekli ticari girişimlerin ardından nispeten olgunlaşmıştır (Hu ve diğerleri, 2014).

1.1.4.2. Veri Tabanı Teknolojileri

Veri tabanı teknolojileri, otuz yıldan uzun bir süredir gelişim sürecinden geçmektedir. Farklı veri kümeleri ölçekleri ve uygulamalar için çeşitli veri tabanı sistemleri önerilmiştir. Geleneksel ilişkisel veri tabanı sistemleri açıkça büyük verilerin gerektirdiği çeşitlilik ve ölçek zorluklarını ele alamaz. Kolay çoğaltmayı destekleme, basit bir API'ye sahip olma, nihai tutarlılık ve büyük miktarda veriyi destekleme dahil olmak üzere bazı temel özellikleri nedeniyle, “SQL ve daha fazlası” anlamına gelen NoSQL (Not Only SQL) veri tabanı büyük veri problemleriyle başa çıkmak için standart hale gelmektedir (Karabay ve Ulaş, 2017).

- BigTable sütun yönelimli veri tabanlarının ilham kaynağıdır. Verileri satır yerine sütunlara göre depolar ve işler. Ölçeklenebilirliği sağlamak için hem satırlar hem de sütunlar birden fazla düğüme bölünür. Google uydu görüntüleri, web sayfaları, finans verileri ve haberleri bu veri tabanlarında tutmaktadır. BigTable, tüm bu verileri gerçek zamanlı, esnek ve yüksek performanslı bir şekilde kontrol etmektedir (Karabay ve Ulaş, 2017).

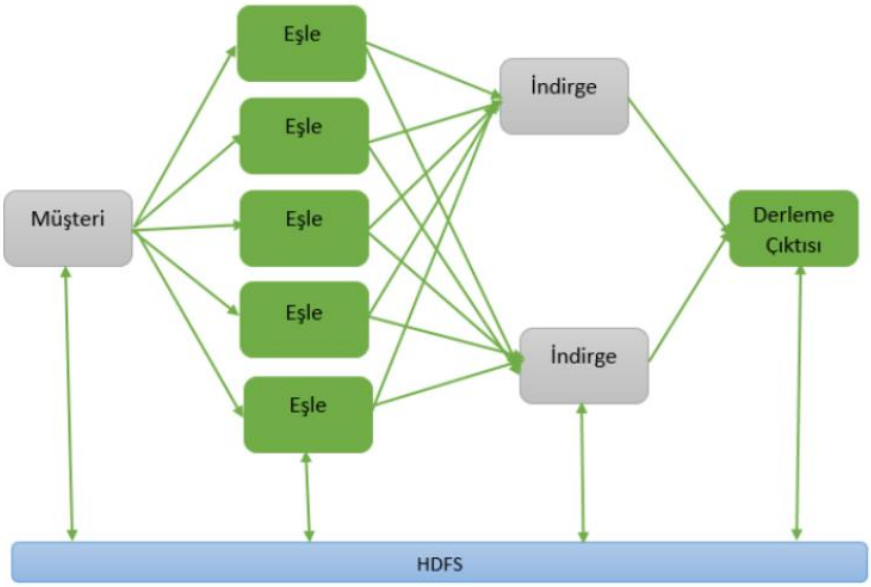
- Amazon Dynamo anahtar-değer (key-valued) veri tabanlarının büyük ölçüde etkilendiği; verilerin bir anahtar-değer çifti olarak saklandığı basit bir veri modeline sahiptir. Anahtarların her biri benzersizdir ve istemciler her anahtar için bir değer koyar veya ister (Hu ve diğerleri, 2014).
- Belge depoları, anahtar-değer depolarından daha karmaşık veri yapılarını destekler. Şema geçiş çabalarının gerekliliğini ortadan kaldırır. Hangi belgelere uyulması gerektiğine dair kesin bir şema yoktur. MangoDB bu veri tabanlarından biridir (Hu ve diğerleri, 2014).
- Spanner, anahtar verileri küresel ölçekte dağıtan ve harici olarak tutarlı dağıtılmış işlemleri destekleyen ilk sistemdir. Bigtable'daki sürümlü anahtar-değer deposu modelinin aksine, Spanner geçici bir çoklu sürüm veri tabanına dönüşmüştür. Spanner'ın göze çarpan özellikleri, harici olarak tutarlı olan okuma, yazma ve küresel olarak tutarlı bir zaman damgasıyla veri tabanı boyunca okumalarıdır (Hu ve diğerleri, 2014).

1.1.4.3. Programlama Modelleri

NoSQL veri tabanları birçok nedenden dolayı çekici olsa da ilişkisel veri tabanı sistemlerinin aksine, birleştirme işleminin ifadesini desteklemez ve sorgulama ve analiz işlemlerinde sınırlı destek sunar. Programlama modeli, uygulama mantığını sağlamak ve veri analizi uygulamalarını kolaylaştırmak için kritik öneme sahiptir (Hu ve diğerleri, 2014).

- MapReduce genel işleme modeli, büyük verileri işlemeyi hedef alan dağıtık bir programlama modelidir. Temel olarak MapReduce ile analiz işleminde iki fonksiyon kullanılır. Bunlardan birincisi map (eşle) fonksiyonu, diğeri ise reduce (indirge) fonksiyonudur. Map adımında elamanlar bir anahtar ile eşleştirilip diğer adıma iletilir. Reduce adımında aynı anahtar için değerler listesi alınır ve bunlar filtrelenip, örneklenip azaltılır (Gürbüz ve Aydın, 2017). Çelik (2017) çalışmasında, MapReduce çalışma mantığını Hadoop Dağıtılmış Dosya Sistemi (Hadoop Distributed File System- HDFS) depolama katmanı üzerinde Şekil 1.5’te görüldüğü gibi anlatmıştır.

- Hadoop: Ciddi bir destek topluluğuna sahip ve bilinen bir büyük veri teknolojisidir. Büyük veriyi geleneksel teknolojiler kullanarak işlerken ve analiz ederken karşılaşılan düşük performans ve karmaşıklığı önleyecek şekilde tasarlanmıştır. Hadoop'un ana avantajlarından biri, paralel kümeleri ve dağıtılmış dosya sistemi sayesinde büyük veri kümelerini hızlı bir şekilde işleme kapasitesidir. Geleneksel teknolojilerin aksine, Hadoop hesaplamaları yürütmek için tüm uzak verileri belleğe kopyalamaz. Bunun yerine Hadoop, verilerin depolandığı yerde görevleri yürütür. Böylece, Hadoop ağı ve sunucuları önemli bir iletişim yükünden kurtarır. Örneğin, klasik yöntemde 20 dakika veya daha fazla zamanda sorgulanan büyük miktarda veri, Hadoop'ta sadece birkaç saniyede yürütülebilir. Hadoop'un bir diğer avantajı da genellikle dağıtılmış ortamda karşılaşılan hata durumlarına dayanıklılık sağlarken, programları çalıştırabilmesidir. Bunu garanti etmek için, sunuculardaki verileri çoğaltarak veri kaybını önler. Hadoop platformunun gücü iki ana alt bileşene dayanır: HDFS ve MapReduce çerçevesi ile kümelenmiş bilgisayarlar arasında büyük çaplı verileri işlemeyi amaçlayan açık kaynaklı bir ekosistemdir. Ekosistem bir düzeni, bir sistemin çevresinde oluşan varlıkları temsil eder. Ayrıca kullanıcılar Hadoop'un üzerine, hedeflerine ve uygulama gereksinimlerine (kapasite, performanslar, güvenilirlik, ölçeklenebilirlik ve güvenlik gibi) göre gerektiğinde modüller ekleyebilirler. Böylece Hadoop topluluğu ekosistemini çeşitli açık kaynaklı modüllerle zenginleştirmeye katkıda bulundu (Karabay ve Ulaş, 2017, Oussous ve diğerleri, 2017).



Şekil 1.5. MapReduce Çalışma Mantığı

- HDFS donanım üzerinde güvenilir, ölçeklenebilir ve hataya dayanıklı veri depolaması sağlayan kendi kendini onaran, dağıtılmış bir dosya sistemidir. HDFS, mimariden bağımsız olarak metin, resim, video ve benzeri formattaki verileri kabul eder ve yüksek bant genişliği akışı için otomatik olarak optimize eder (Ghazi ve Gangodkar, 2015).
- Hadoop MapReduce, büyük miktarda veri düğümünü paralel olarak büyük miktarlarda veriyi hızla işleyen uygulamalar yazmak için kullanılan bir programlama modeli ve yazılım çerçevesidir. MapReduce, dosya bölümlerine erişmek ve düşük sonuçları depolamak için HDFS'yi kullanır (Padhy,2012).

- Google’s Pregel ve GraphLab ise grafik modeller kategorisinde yer alan iki diğer modeldir. Bu modeller büyüyen uygulama sınıfı (sosyal ağ analizi gibi) ile, birbirleriyle ilişkili varlıkları grafik modeller kullanarak yakalayabilir. Akış tipi modellerin aksine, grafik işlemenin doğası gereği yinelemeli ve aynı veri kümesi üzerini birden çok kez ziyaret etmeli olduğu söylenebilir (Hu ve diğerleri, 2014).
- Storm, dağıtık ve akan veri işleme platformudur. Java sanal makinası üzerinden çalışır (Çelik, 2017). Storm ve Hadoop kümeleri birbirine benzerdir ancak, Storm'da farklı storm görevleri için farklı topolojiler çalıştırmak mümkündür. Bunun yerine, Hadoop platformunda tek seçenek, ilgili uygulamalar için

MapReduce uygulamaktan ibarettir. MapReduce ve farklı topolojiler arasındaki temel farklardan biri şudur; MapReduce işi durdurabilir, ancak bir topoloji iletileri her zaman veya kullanıcı sonlandırıncaya kadar işlemeye devam eder. Storm, kullanımı kolay, hızlı, ölçeklenebilir ve hataya dayanıklı bir sistemdir. Bir veya daha fazla işlem başarısız olursa, Storm otomatik olarak yeniden başlatır. İşlem tekrar tekrar başarısız olursa, Storm başka bir makineye yönlendirecek ve orada yeniden başlatacaktır. Gerçek zamanlı analitik, çevrimiçi makine öğrenimi ve sürekli hesaplama gerektiren birçok durum için kullanılabilir (Oussous ve diğerleri, 2017).

- Apache Spark: Netflix, Yahoo ve eBay gibi büyük şirketler de dahil olmak üzere çok sayıda şirketin veri alanındaki en büyük açık kaynak topluluğu haline gelmiş bir işleme çerçevesidir. Hadoop ve MapReduce'u temel alır ve genişletir. Spark, Hadoop kümesinde bir uygulamayı çalıştırmaya yardımcı olur. Hadoop Mapreduce işleminden bellekte 100, disk üzerinde 10 kat daha hızlıdır. Java, Scala ve Python gibi birden fazla dili destekler. Bu özelliği ile uygulamalar farklı dillerde yazılabilir. Gelişmiş Analiz sağlar. 'Map' ve 'Reduce' fonksiyonları yanında SQL sorguları, akış verileri, makine öğrenme ve grafik algoritmalarını destekler (Çelik, 2017, Wakde ve diğerleri, 2018).

Yukarıda bahsi geçen ekosistemler yanında pek çok gelişme bulunmaktadır. Aşağıda bu alanda bilinen bazı sistem/platformlar sıralanmıştır.

- Talend Open Studio for Big Data
- SAP HANA
- KNIME Big Data Connector
- Amazon EMR
- QlickView
- IBM BigInsights
- Apache Impala
- MapR Converged Data Platform

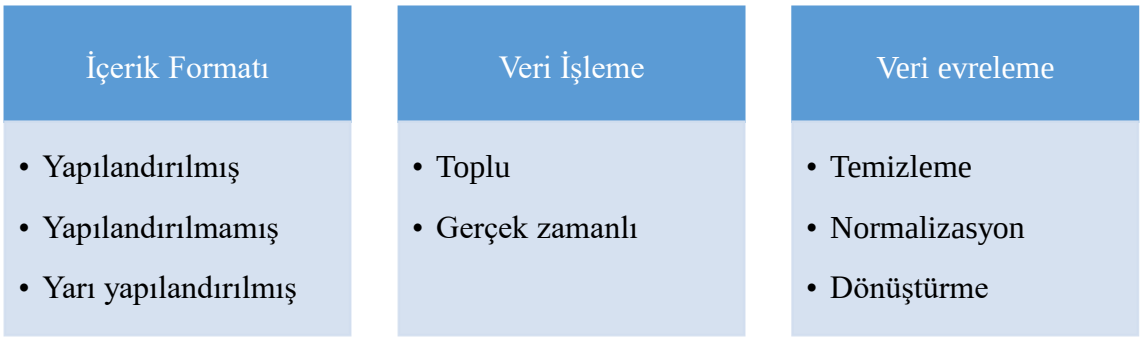
Milyonlarca dağıtık ve yapılandırılmamış verinin etkin bir şekilde işlenmesi ve zamanında bilgi sağlaması için kapsamlı paralel işleme ve sınıflandırma ya da kümeleme yanında yeni analitik algoritmalar gerekmektedir. Tüm bunlar yanında görselleştirme

nihai kullanıcıya bilgi sunma bakımından büyük önem teşkil etmektedir. Görselleştirme, sayısal verilerin anlamlı 3 boyutlu görüntülere dönüştürüldüğü bir işlemdir. Dygraphs, ZingChart, Polymaps, Timeline, Exhibit, Modest Maps, Leaflet, Visual.ly, Visualize Free, jQuery Visualize, JqPlot, Many Eyes, JavaScript InfoVis, JpGraph, Highcharts, R, WEKA, Flot, RAPHAEL ve Crossfilter bu amaçla kullanılabilecek araçlardır (Vijayarani ve Sharmila, 2016).

1.1.5. Büyük Veri Sınıflandırılması

Büyük veri, Vijayarani ve Sharmila (2016)'nin çalışmalarından faydalanılarak aşağıdaki Şekil 1.6'da görülen başlıklar altında sınıflandırılmıştır.

İçerik formatı yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış olmak üzere üçe ayrılır. Yapısal format, çoğunlukla SQL tarafından yönetilir ve veriler, bir kayıt veya dosya içindeki belirlenmiş alanda bulunur. Yapılandırılmamış format genellikle metin ve multimedya içeriğini içerir, yapılandırılmış verinin zıddıdır. Yarı yapı formatı ilişkisel bir veri tabanında bulunmaz; XML belgeleri içerebilir ve NoSQL veri tabanında yönetilebilir (Vijayarani ve Sharmila, 2016).



Şekil 1.6. Büyük Veri Sınıflandırması

Veri işleme, toplu ve gerçek zamanlı olarak iki türe dayanır. Toplu olarak bir zaman sonra yapılırken gerçek zaman akan veri dahilinde işleme gerektirir.

Veri evrelemesi üç şekilde sınıflandırılmıştır; bunlar temizlik, dönüştürme ve normalleştirmedir. Temizlik tamamlanmamış verileri tanımlar. Normalleştirme, fazlalığı en aza indiren yöntemdir. Dönüştürme ise verileri uygun forma aktaran sınıf olarak tanımlanabilir (Vijayarani ve Sharmila, 2016).

1.1.6. Büyük Veri Kaynakları

Yukarıda yer alan sınıflandırmaya ek olarak bir sınıflandırma da büyük veri kaynakları ele alınarak yapılabilir. Genellikle büyük veri kaynağı sınıflandırılması, Sosyal Ağlar, Geleneksel İş Sistemleri ve IoT olmak üzere üç kategoriye ayrılır.

- Sosyal Ağlar (insan kaynaklı bilgi)

Bu tür veriler, daha önce kitaplarda ve sanat eserlerinde ve daha sonra fotoğraf, ses ve videoda kaydedilen insan deneyimlerinin kaydı olan bilgileri içerir. İnsan kaynaklı bilgi artık neredeyse tamamen dijital hale getirilmiş ve kişisel bilgisayarlardan sosyal ağlara kadar her yerde saklanmaktadır. Veriler gevşek bir şekilde yapılandırılmıştır (loosely structured) ve genellikle sosyal ağlar (Facebook, Twitter vb.), bloglar ve yorumlar, kişisel belgeler, resimler (instagram vb.), videolar (YouTube vb.), internet arama motoru, mobil veri içeriği, metin mesajları, kullanıcı tarafından oluşturulan rotalar ve e-postalardan oluşur (Vijayarani ve Sharmila, 2016, Vaccari, 2014).

- Geleneksel İş Sistemleri (süreç aracılı veri)

Geleneksel iş sistemleri, süreç aracılı veridir. Bu süreçler, bir müşteriyi kaydetme, bir ürünü üretme, sipariş alma, vb. gibi, ilgilendikleri iş olaylarını izler ve kaydeder. Bu şekilde toplanan süreç aracılı veriler, son derece yapılandırılmıştır ve işlemler, referans tabloları ve ilişki içeriğini belirleyen meta verileri içerir.

Geleneksel iş verileri, Bilgi Teknolojilerinin hem operasyonel hem de İş Zekâsı sistemlerinde işlediği ve yönettiği verilerin büyük çoğunluğudur. Genellikle yapılandırılmış veriler ilişkisel veri tabanı sistemlerinde saklanır (Vijayarani ve Sharmila, 2016, Vaccari, 2014). Bu sınıfa ait "İdari veriler" kategorisine, Kamu Kurumları bağlantılı süreçlerden üretilen veriler (sağlık kayıtları gibi) girebilir. “İşletmeler tarafından üretilen veriler” kategorisinde ticari kayıtlar, bankacılık, lojistik takibi gibi süreçlerden üretilen veriler bulunur (Vijayarani ve Sharmila, 2016, Vaccari, 2014).

- IoT (makine tarafından üretilen veriler)

Fiziksel dünyadaki olayları ya da durumları ölçmek, onları kaydetmek için kullanılan sensörlerin ve makinelerin sayısındaki olağanüstü büyümeden elde edilen verilerdir. Sensörlerin çıkışı makine tarafından üretilen verilerdir ve basit sensör kayıtlarından karmaşık bilgisayar kayıtlarına kadar, iyi yapılandırılmıştır. Sensörler

çoğaldıkça ve veri hacimleri büyüdükçe, birçok işletme tarafından saklanan ve işlenen bilgiler giderek daha önemli bir bileşen haline gelmektedir. İyi yapılandırılmış doğası, bilgisayar işlemeye uygun, ancak büyüklüğü ve hızı geleneksel yaklaşımların ötesindedir. Sensörlerden elde edilen veriler; sabit sensörler, ev otomasyonu sensörleri, hava sensörleri, trafik sensörleri / kameraları, bilimsel sensörler, videolar, cep telefonu konumları gibi mobil sensörler, uydu görüntüleri ve bilgisayar sistem kayıtları ve web günlüklerinden alınan veriler gibi çeşitlere ayrılır (Vijayarani ve Sharmila, 2016, Vaccari, 2014).

1.2. NESNELERİN İNTERNETİ

IoT, fiziksel nesnelerin bir işi/görevi gerçekleştirmek için "konuşarak" bilgi paylaşmalarını ve kararlarını koordine etmelerini sağlar. IoT, bu fiziksel nesneleri; yaygın bilgisayar kullanımı, gömülü cihazlar, iletişim teknolojileri, sensör ağları, internet protokolleri ve uygulamaları gibi temel teknolojileri kullanarak geleneksel olmaktan çıkarmakta ve akıllı hale getirmektedir (Al-Fuqaha ve diğerleri, 2015).

1.2.1. Ana Unsurlar

IoT'nin evrensel olarak kabul edilmiş ve eyleme geçirilebilir bir tanımı olmasa da IoT tabanlı sistemleri inşa etmek için kullanılan "Lego" ya da büyük bloglar benzeri yapı taşlarının ana unsurları aşağıdaki gibi tanımlanabilir.

1.2.1.1. Sensör

Sensör, sıcaklık, ağırlık, ses, konum, hızlanma ve kimlik gibi fiziksel özellikleri ölçen elektronik araçtır. Tüm sensörler işlemlerinde mekanik, elektriksel, kimyasal, optik ve benzeri efektler kullanır. Sensörler, kimlik (veya bağlı olduğu "şeyin" kimliği) gibi belirli fiziksel özelliklere sahiptir. Farklı üreticilerden gelebilir, raftan alınabilir veya belli özelliklere göre üretilebilirler. Sabit coğrafi konumlar veya mobil cihazlarla ilişkilendirilebilirler. Sensörün, toplanan verilerini kontrol eden, ne zaman ve nasıl erişileceğine izin veren yani onu kontrol eden bir sahibi bulunabilir. Sensörler, alternatif akım, güneş, rüzgâr, pil veya radyo dalgaları gibi çeşitli güçlerle çalıştırılabilirler. Sensörler uzun süre kullanmadan hazır olarak bekleyebilir (Voas ve diğerleri, 2018).

Sensör verileri; analog, dijital olaylar (loglar), manuel girişler veya komutlarla anlık olarak ya da önceden tanımlanmış zamanlarda üretilebilir. Sensör verileri birden fazla IoT'ye gönderilebilir veya bu veriler birden fazla IoT'nin kısıtlı kullanımına sunulabilir. Bu verilerinin belirsizliği dikkate alınmalıdır. Örneğin, sensör verileri doğru ve kabul edilebilir aralıklarda ancak tamamen ya da kısmen hatalı olabilir. Sensörler, bir sistemin "sağlığı" hakkındaki veriler de dahil olmak üzere geçerli ancak eski veriler sağlayabilir. İşte bu sebeple; çalışma aralıkları ihlal edildiğinde kontrolün bir insana ya da makineye devredilmesi için kurallar gerekebilir. Sensörler belirli çalışma özelliklerine sahiptir. İnternet erişimine, yazılım işlevlerine ve bilgi işlem gücüne sahip olabilirler. Sensörlerin gerçek olarak doğrulanabilme yetenekleri olmalıdır. Sensörlerin veri yayınlama sıklığı verinin geçerliliği ve uygunluğunu etkiler. Bir sensörün hassasiyeti ne kadar bilgi sağlandığını belirleyebilir. (Voas ve diğerleri, 2018).

Sensörler belirli kalite ve güvenlik etkilerine sahiptir. Örneğin, ucuz, atılabilir veya zaman içinde yıpranabilir olabilirler. Sensör emniyeti ve güvenliği söz konusu olduğunda; tüketici sınıf, askeri sınıf ve endüstriyel sınıf arasında farklılıklar olabilir. Tamamen veya aralıklı olarak bozulabilir, hassasiyeti ya da kalibrasyonu kaybedebilirler. Karmaşık ve pahalı sensörler değiştirilmek yerine tamir edilebilir. Sensör ya da verinin karıştırılması, çalınması, silinmesi, düşürülmesi veya güvenli bir şekilde iletilememesi durumları endişe vericidir. Bazı güvenlik kaygılarını ortadan kaldırmak için verilerin şifrelenmesi sağlanabilir (Voas ve diğerleri, 2018).

1.2.1.2. İletişim Kanalları

İletişim kanalı verilerin iletildiği ortamdır. Veri, IoT'nin içinde akan "kan" olarak tanımlanırsa, iletişim kanalları da bu kanın içinde aktığı damarlar olarak tanımlanabilir. IoT iletişim teknolojileri heterojen nesneleri birbirine bağlar. IoT için kullanılan haberleşme protokollerinin örnekleri WiFi, Bluetooth, IEEE 802.15.4, Z-Wave ve Gelişmiş Uzun Dönem Evrim (LTE-A)'dır. Ayrıca bazı özel iletişim teknolojileri Radyo Frekans Tanımlama (Radio-frequency Identification- RFID), Yakın Alan İletişimi (Near Field Communication- NFC) ve Ultra Geniş Bant Genişliği (Ultra-Wide Bandwidth-UWB) gibi kullanımlardır.

- RFID, makineden makineye (M2M- Machine to Machine) kavramını gerçekleştirmek için kullanılan ilk teknolojidir (RFID etiketi ve okuyucu). RFID etiketi, nesnenin kimliğini belirlemek için ekli basit bir çipi veya etiketi temsil eder. RFID okuyucusu, etikete bir sorgu sinyali iletir ve iletilen etiketten yansıtılan sinyali alarak sırasıyla veri tabanına iletir. Veri tabanı, 10 cm ila 200 m aralığında yansıtılan sinyallere dayanarak nesneleri tanımlamak için bir işleme merkezine bağlanır. RFID etiketleri aktif, pasif veya yarı pasif/aktif olabilir. Aktif etiketler batarya ile çalıştırılırken pasif olanların bataryaya ihtiyaçları yoktur. Yarı pasif/aktif etiketler gerektiğinde panel gücünü kullanır (Al-Fuqaha ve diğerleri, 2015).
- NFC Protocol, 13.56 MHz'de yüksek frekans bandında çalışır ve 424 Kbps'ye kadar veri hızını destekler. Uygulanabilir aralık, aktif okuyucular ve pasif etiketler veya iki aktif okuyucu arasındaki iletişimin gerçekleşebileceği 10 cm'ye kadardır (Al-Fuqaha ve diğerleri, 2015). NFC, çok uzun bir el sıkışma süreci olmadan kolay ağ erişimi ve veri paylaşımı sağlar. NFC kullanıcı amacı ile yapılandırılabilir ve cihaza çok daha iyi erişilebilirlik sağlar. Ayrıca IoT için çok önemli noktalardan biri olan çoklu düzeyde veri güvenliği sağlar. En büyük dezavantajı ise mesafedir (Sain ve diğerleri, 2017).
- UWB iletişim teknolojisi, son zamanlarda sensörleri birbirine bağlayan, uygulamaları artmış olan, düşük enerji ve yüksek bant genişliği kullanan düşük menzilli kapsama alanındaki iletişimleri desteklemek için tasarlanmıştır (Al-Fuqaha ve diğerleri, 2015).
- Diğer bir iletişim teknolojisi, 20 metreden 100 metre aralığa kadar nesneler arasında veri alışverişinde bulunmak için radyo dalgalarını kullanan Wi-Fi'dir. Wi-Fi, bazı özel yapılandırmalarda yönlendirici kullanmadan akıllı cihazların iletişim kurmasına ve bilgi alışverişine olanak tanır (Al-Fuqaha ve diğerleri, 2015, Sain ve diğerleri, 2017).
- Bluetooth, güç tüketimini en aza indirmek için kısa dalga boylu radyo kullanarak 8-10 metre cihazlar arasında veri alışverişinde kullanılan bir iletişim teknolojisi sunar. Son zamanlarda, Bluetooth Özel İlgi Grubu (Special Interest Group- SIG), IoT'yi desteklemek için Bluetooth Düşük Enerji (BLE) 'nin yanı sıra yüksek hızlı

ve IP bağlantısı sağlayan Bluetooth 4.1'i üretti (Al-Fuqaha ve diğerleri, 2015, Sain ve diğerleri, 2017).

- IEEE 802.15.4 kablosuz kişisel alan ağları protokolü, güvenilir ve ölçeklenebilir iletişimi hedefleyen düşük güçlü kablosuz ağlar için hem fiziksel bir katmanı hem de orta erişim kontrolünü içerir (Al-Fuqaha ve diğerleri, 2015).
- LTE (Uzun Dönem Evrim); GSM ve UMTS (Evrensel Mobil Telekomünikasyon Sistemi) şebeke teknolojilerine dayalı cep telefonları arasında yüksek hızlı veri aktarımı için standart bir kablosuz iletişimdir. Hızlı hareket eden cihazları kapsayabilir ve çok noktaya yayın hizmetleri sağlayabilir. LTE-A, 100 MHz'e kadar aşağı ve yukarı bağlantı ve genişletilmiş kapsama, daha yüksek çıkış ve daha düşük gecikmeler içeren bant genişliği uzantısı da dahil olmak üzere geliştirilmiş bir LTE sürümüdür (Al-Fuqaha ve diğerleri, 2015).

1.2.1.3. Hesaplama

İşleme birimleri (örneğin, mikro denetleyiciler, mikroişlemciler) ve yazılım uygulamaları IoT'nin hesaplama yeteneğini yani "beynini" temsil eder. IoT uygulamalarını çalıştırmak için Arduino, UDOO, FriendlyARM, Intel Galileo, Ahududu Pi, Gadgeter, BeagleBone, Cubieboard, Z1, WiSense, Mulle ve T-Mote Sky gibi çeşitli donanım platformları geliştirilmiştir (Al-Fuqaha ve diğerleri, 2015).

IoT işlevselliklerini sağlamak için birçok yazılım platformu kullanılmaktadır. Bu platformlar arasında, İşletim Sistemleri bir cihazın tüm aktivasyon süresi boyunca çalıştığı için hayati öneme sahiptir. Gerçek Zamanlı İşletim Sistemi (RTOS) gerçek zamanlı IoT uygulamalarının geliştirilmesi için iyi bir aday olarak görülmektedir. Örneğin, Contiki RTOS IoT senaryolarında yaygın olarak kullanılmıştır. Contiki, araştırmacı ve geliştiricilerin IoT ve kablosuz sensör ağı (Wireless Sensor Network-WSN) uygulamalarını taklit etmelerini sağlayan Cooja adlı bir simülatöre sahiptir. Ayrıca TinyOS, LiteOS ve Riot OS, IoT ortamları için tasarlanmış yükte hafif işletim sistemleri sunar. Bunların yanında, bazı otomobil endüstrisi liderleri Google ile birlikte Açık Oto İttifakı (Open Automotive Alliance- OAA) kurmuş ve Araçların İnterneti (Internet of

Vehicles- IoV) paradigmasının benimsenmesini hızlandırmak için Android platformuna yeni özellikler getirmeyi planlamaktadır (Al-Fuqaha ve diğerleri, 2015).

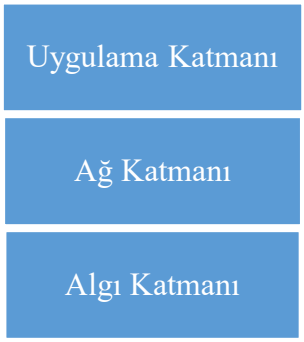
Bulut Platformları, IoT'nin bir başka önemli hesaplama bölümünü oluşturur. Bu platformlar, akıllı nesnelere verilerini buluta göndermeleri, büyük verilerin gerçek zamanlı olarak işlenmesi ve sonunda son kullanıcıların toplanan büyük verilerden elde edilen bilgilerden yararlanmaları için olanaklar sağlar. IoT hizmetlerine ev sahipliği yapacak birçok ücretsiz ve ticari bulut platformu ve çerçevesi vardır. Bugünün IoT platformları genellikle bulut tabanlıdır. Bu bileşen, IoT entegrasyon ara yazılımı olarak adlandırılabilir, çünkü bu bileşen işleme ünitesini temsil eder ve IoT'nin farklı sensör tipleri, aktüatörler, cihazlar ve uygulamalar için kombinasyon katmanı olarak görev yaptığı hesaplama kabiliyetini sağlar. Uygun iletişim teknolojilerini destekler, cihazlar arasında iletişim kurmak için WebSockets gibi protokolleri kullanır ve platformlar arasındaki iletişimi sağlar (Hejazi ve diğerleri, 2018).

1.2.2. Katmanlar Mimarisi

IoT için farklı katmanlı mimariler bulunmaktadır. Bunlardan bazılarına aşağıda yer verilmektedir (Lin ve diğerleri, 2017 ve Al-Fuqaha ve diğerleri, 2015).

1.2.2.1. Üç Katmanlı Mimari

Tipik olarak IoT mimarisi Şekil 1.7'de görüldüğü gibi üçe ayrılır.



Şekil 1.7. Üç Katmanlı Mimari

- Algı Katmanı: Bu katman sensör katmanı olarak da bilinir. IoT mimarisinde alt katman olarak uygulanır. Algılama katmanı, fiziksel aygıtlarla ve bileşenlerle akıllı aygıtlarla (RFID, sensörler, aktüatörler vb.) etkileşime girer. Temel

hedefleri, nesneleri IoT ağına bağlayarak; bu nesnelerle ilgili durum bilgilerini konuşlandırılmış akıllı cihazlar aracılığıyla ölçmek, toplamak, işlemek ve işlenen bilgileri katman ara yüzleri aracılığıyla üst katmana iletmektir (Lin ve diğerleri, 2017).

- Ağ Katmanı: İletim katmanı olarak da bilinir. IoT mimarisinde orta katman olarak uygulanır. Ağ katmanı, algı katmanı tarafından sağlanan işlenmiş verileri almak ve bu verileri IoT hub'ına, cihazlarına ve uygulamalarına bütünleşmiş ağlar üzerinden iletmek için rotaları belirlemek için kullanılır. Ağ katmanı IoT mimarisindeki en önemli katmandır, çünkü çeşitli cihazlar (hub, anahtarlama, ağ geçidi, bulut bilgi işlem gerçekleştirme vb.) ve çeşitli iletişim teknolojileri (Bluetooth, Wi-Fi, uzun vadeli gelişim vb.) bu katmana entegredir. Ağ katmanı, heterojen ağlar arasındaki arayüzler, ağ geçitleri aracılığıyla farklı nesnelere veya uygulamalara veri göndermeli ve çeşitli iletişim teknolojileri ve protokollerini kullanmalıdır (Lin ve diğerleri, 2017).
- Uygulama Katmanı: İş katmanı olarak da bilinir. IoT mimarisinde üst katman olarak uygulanır. Uygulama katmanı ağ katmanından iletilen verileri alır ve gerekli hizmetleri veya işlemleri sağlamak için verileri kullanır. Örneğin, uygulama katmanı alınan verileri bir veri tabanına yedeklemek için depolama hizmetini sağlayabilir veya fiziksel verilerin gelecekteki durumunu tahmin etmek için alınan verileri değerlendirmek için analiz hizmetini sağlayabilir. Bu katmanda, her biri farklı gereksinimlere sahip olan birkaç uygulama vardır. Örnekler arasında akıllı şebeke, akıllı ulaşım, akıllı şehirler vb. gösterilebilir (Lin ve diğerleri, 2017).

Üç katmanlı mimari, IoT için temeldir. Birçok sistemde tasarlanmış ve uygulanmıştır. Katmanlı IoT mimarisinin sadeliğine rağmen, ağ ve uygulama katmanlarındaki işlevler ve işlemler çok çeşitli ve karmaşıktır. Örneğin, ağ katmanı yalnızca rotaları belirlemek ve veri iletmekle kalmaz, aynı zamanda veri hizmetleri de sağlar (veri toplama, hesaplama vb.). Uygulama katmanı sadece müşterilere ve cihazlara hizmet vermekle kalmaz, aynı zamanda veri hizmetleri de (veri madenciliği, veri analitiği vb.) sağlamalıdır. Bu nedenle, IoT için genel, esnek katmanlı bir mimari oluşturmak ve veri hizmetlerini sağlamak için; ağ katmanı ile uygulama katmanı arasında bir servis

katmanı geliştirilmelidir. Bu konsepte dayanarak, IoT'yi desteklemek için servis odaklı mimariler (Service-Oriented Architecture- SoA) yakın zamanda geliştirilmiştir.

1.2.2.2. Servis Odaklı Mimari

SoA, bir uygulamanın farklı fonksiyonel birimlerini (servis olarak da bilinir) arayüzler ve protokoller aracılığıyla bağlamak için tasarlanan, bileşen tabanlı bir modeldir. IoT mimarisini tasarlamada uygulanabilirliğini artırarak yazılım ve donanım bileşenlerinin yeniden kullanılmasını sağlayabilir. Geleneksel üç katmanlı mimaride veri hizmetleri ağ katmanı ve uygulama katmanı tarafından sağlanmaktadır. Bu kısım SoA'da yeni bir katman, bir servis katmanı (arayüz ya da orta katman olarak da bilinir) oluşturularak, IoT mimarisine kolayca entegre edilebilir. Özetle, servis odaklı bir IoT mimarisinde, Şekil 1.8'de yer alan dört katman vardır ve birbirleriyle etkileşim içindedirler (Lin ve diğerleri, 2017).

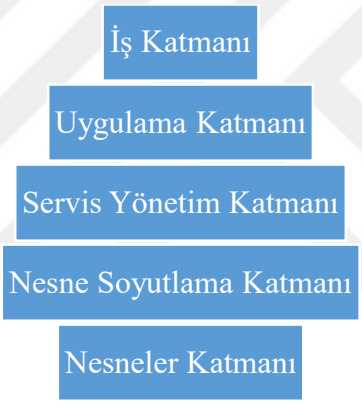
Şekil 1.8. Servis Odaklı Mimari

Dört katmanlı servis odaklı bir IoT mimarisinde, algılama katmanı mimarinin alt katmanı olarak bulunur ve fiziksel aygıtlarla ilişkili verileri ölçmek, toplamak ve çıkarmak için kullanılır. Ağ katmanı, rotaları belirlemek ve entegre heterojen ağlar üzerinden veri aktarım desteği sağlamak için kullanılır. Servis katmanı, ağ katmanı ile uygulama katmanı arasında yer almakta ve uygulama katmanını desteklemek için servisler sağlamaktadır. Servis katmanı servis keşfi, servis kompozisyonu, servis yönetimi ve servis ara yüzlerinden oluşur. Burada, servis keşfi, istenen servis taleplerini keşfetmek için kullanılır, servis kompozisyonu, bağlı nesnelerle etkileşimde bulunmak ve servis taleplerini verimli bir şekilde karşılamak için hizmetleri bölmek veya entegre etmek için kullanılır, servis yönetimi, servis taleplerini karşılamak üzere güven mekanizmalarını yönetmek ve belirlemek için kullanılır. Son olarak servis arayüzleri,

sağlanan tüm servisler arasındaki etkileşimleri desteklemek için kullanılır. Uygulama katmanı, kullanıcılardan gelen servis taleplerini desteklemek için kullanılır. Uygulama katmanı, akıllı şebeke, akıllı ulaşım, akıllı şehirler vb. dahil olmak üzere birçok uygulamayı destekleyebilir (Lin ve diğerleri, 2017).

1.2.2.3. Beş Katmanlı Mimari

İlk olarak açıklanan üç katmanlı mimari, Nesnelerin İnterneti ile ilgili ana fikri tanımlar, ancak IoT üzerinde araştırma yapmak için yeterli değildir. Araştırma genellikle Nesnelerin İnternet'inin daha ince yönlerine odaklanır. Bu kapsamda yer alan mimarilerden biri de servis yönetim ve iş katmanlarını da içeren beş katmanlı mimaridir. Beş katmanlı mimari Şekil 1.9'da yer almaktadır (Al-Fuqaha ve diğerleri, 2015).



Şekil 1.9. Beş Katmanlı Mimari

- Nesneler Katmanı: İlk katman olan nesneler (cihazlar) veya algılama katmanı, IoT'nin bilgi toplamayı ve işlemeyi amaçlayan fiziksel sensörlerini temsil eder. Bu katman, sorgulama yeri, sıcaklık, ağırlık, hareket, titreşim, hızlanma, nem vb. gibi farklı verileri gerçekleştirmek için sensörler ve aktüatörler içerir. Algılama katmanı, verileri güvenli kanallar aracılığıyla Nesne Soyutlama katmanına sayısallaştırır ve aktarır. IoT tarafından yaratılan büyük veriler bu katmanda oluşur (Al-Fuqaha ve diğerleri, 2015).
- Nesne Soyutlama Katmanı: Nesneler katmanı tarafından üretilen verileri güvenli kanallar üzerinden Servis Yönetimi katmanına aktarır. Veriler, RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth LowEnergy, kızılötesi, ZigBee, vb. teknolojiler yoluyla aktarılabilir. Ayrıca, bulut hesaplama ve veri yönetimi

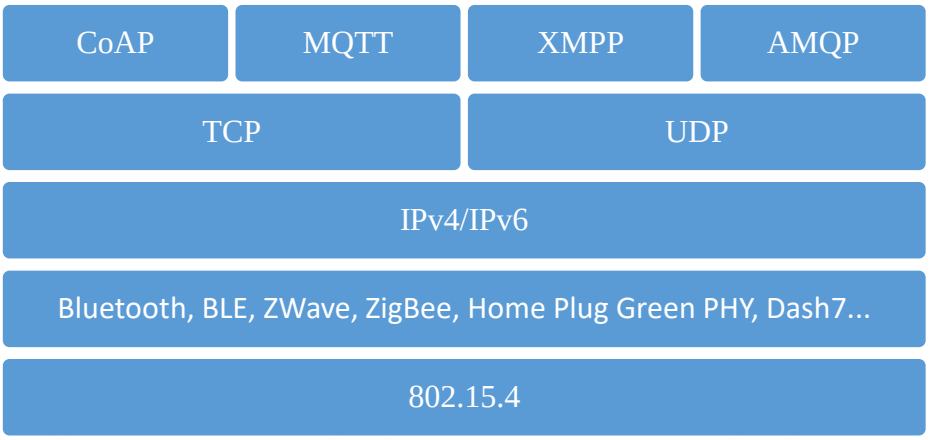
işlemleri gibi işlevler de bu katmanda ele alınmaktadır (Al-Fuqaha ve diğerleri, 2015).

- Servis Yönetim Katmanı: Servis Yönetimi veya Orta (eşleştirme) katmanı, servis isteklerini, adresleri ve isimleri temelinde eşleştirir. Bu katman, IoT uygulama programcılarının belirli bir donanım platformunu dikkate almadan heterojen nesnelerle çalışmasını sağlar. Ayrıca, bu katman alınan verileri işler, kararlar alır ve gerekli hizmetleri ağ kablo protokolleri üzerinden sunar (Al-Fuqaha ve diğerleri, 2015).
- Uygulama Katmanı: Uygulama katmanı müşterilerin talep ettiği hizmetleri sağlar. Örneğin, uygulama katmanı, bu verileri isteyen müşteriye sıcaklık ve hava nemi ölçümleri sağlayabilir. IoT için bu katmanın önemi, müşterilerin ihtiyaçlarını karşılamak için yüksek kaliteli akıllı hizmetler sağlama yeteneğine sahip olmasıdır. Uygulama katmanı, akıllı ev, akıllı bina, ulaşım, endüstriyel otomasyon ve akıllı sağlık hizmetleri gibi sayısız dikey pazarı kapsamaktadır (Al-Fuqaha ve diğerleri, 2015).
- İş Katmanı: İş (yönetim) katmanı tüm IoT sistem faaliyetlerini ve servislerini yönetir. Bu katmanın sorumlulukları, Uygulama katmanından alınan verilere dayanan bir iş modeli, grafikler, akış çizelgeleri vb. oluşturmaktır. Ayrıca, IoT sistemiyle ilgili unsurları tasarlama, analiz etme, uygulama, değerlendirme, izleme ve geliştirme gibi görevleri de gerçekleştirir. İş Katmanı, büyük veri analizine dayanan karar verme süreçlerini desteklemeyi mümkün kılar. Ek olarak, altta yatan dört katmanın izlenmesi ve yönetimi bu katmanda gerçekleştirilir. Ayrıca, bu katman hizmetleri geliştirmek ve kullanıcıların gizliliğini korumak için her katmanın çıktısını beklenen çıktıyla karşılaştırır (Al-Fuqaha ve diğerleri, 2015).

1.2.3. Protokoller

IoT'de genel olarak protokol yığınının yapısı aşağıda Şekil 1.10'da gösterilmiştir (Granjal ve diğerleri, 2015, Sharma ve Gondhi, 2018, Meera ve Rao, 2018). TCP/IP katman yapısında olduğu gibi; en altta yer alan katman Fiziksel katman, onun üzerinde

sırasıyla Veri bağı, Ağ, Taşıma ve Uygulama katmanları gösterilmekte ve bu katmanlara ait protokollerden bazılarına yer verilmektedir.



Şekil 1.10. Genel Protokol Yığını Yapısı

Aşağıdan yukarıya bu katmanlara ait karakteristikleri incelediğimizde; Fiziksel katmandaki düşük enerjili iletişim, IEEE 802.15.4 tarafından desteklenir. Bu nedenle IEEE 802.15.4, yığının alt katmanlarındaki iletişim kurallarını belirler ve daha yüksek katmanlardaki IoT iletişim protokolleri için zemin hazırlar (Granjal ve diğerleri, 2015). Bu protokol enerji verimliliği bakımından da uygun bulunmaktadır. BLE, Z-Wave, ZigBee, HomePlug GP ve Dash7 düşük güç tüketimi ile kısa menzilli kablosuz iletişim için standart beş veri bağlantı protokolüdür (Sharma ve Gondhi, 2018).

Araç içi ağ için yaygın olarak kullanılan kısa menzilli bir iletişim protokolü olan BLE, klasik Bluetooth'a göre 10 kat daha düşük enerji harcamaktadır. Z-Wave, cihazdan cihaza iletişim kurmak için düşük enerjili radyo dalgaları kullanan diğer bir kablosuz iletişim protokolüdür. Geleneksel ZigBee ise, kişisel alan ağları için kullanılan bir düşük enerjili dijital radyolar kullanılarak oluşturulan yüksek düzeyde iletişim protokollerinin özelleştirilmiş bir halidir. HomePlug GP, IoT kapsamında özellikle ev otomasyonu ve akıllı şebeke uygulamaları için tasarlanmış bir başka MAC protokolüdür. Dash7 de düşük enerjili, ZigBee'ye kıyasla daha yüksek veri hızına sahip ve IoT gereksinimlerine uygun diğer bir kablosuz iletişim protokolüdür (Salman ve Jain, 2019).

Yeni geliştirilen ve kullanılmaya başlanan IPv6, ağ yönlendirme ve tesisleri kapsülleme sağlar. Kullanıcı Datagram Protokolü (User Datagram Protocol-UDP) ve İletim Kontrol Protokolü (Transmission Control Protocol-TCP) taşıma katmanı

protokolleridir. Nesnelerin yansıra son kullanıcı uygulamalarını Internet'e bağlamak için kullanılan mevcut IoT uygulama katmanı protokolleri aşağıda sırasıyla açıklanmıştır.

- Kısıtlı Uygulama Protokolü (CoAP - Constrained Application Protocol): CoAP, Hiper Metin Aktarım Protokolü'nden (HTTP- HyperText Transfer Protocol) ilham alan ve birebir iletişim kullanan IoT donanımı için özel olarak tasarlanmış yeni bir iletişim protokolüdür. CoAP, IoT donanımı için kullanıldığından hafif, ince olmalı ve olabildiğince az trafik üretmelidir. Bu nedenle TCP/ IP iletişimini desteklemez. IP üzerinden UDP'yi kullanır. Bu protokol HTTP'den daha az kaynak kullanır ve okuma, yazma gibi özellikleri yanında gözlemleme, yürütme ve keşfetme gibi HTTP'den daha fazla özellikte barındırır. Ancak tipik bir IoT platformu, cihaz üreticisinin uygun protokolleri seçebileceği çeşitli iletişim protokolleri önerebilir (Sharma ve Gondhi, 2018).
- Mesaj Kuyruğu Telemetri Taşıma (MQTT - Message Queue Telemetry Transport): Bu protokol, hafif iletişim protokolü olan TCP/IP üzerinden uygulanan bir mesajlaşma protokolüdür. Cihazlar arasındaki iletişimin ortasında Mesaj Komisyoncu sunucusu vardır. Bu yüzden, makine-makine iletişimi değildir. Abone, yayıncı ve komisyoncu olmak üzere üç unsurdan oluşur. Müşteriler, komisyoncunun yayınlarına abone olurlar. Örneğin, müşteriler sıcaklıkla ilgili yayına abone olurlarsa, bu konu hakkında bildirim alacaklardır. Ayrıca bu protokol güvenlik ile ilgili olarak, Güvenli Soket Katmanı (SSL - Secure Sockets Layer) ve Aktarım Katmanı Güvenliğini (TLS - Transport Layer Security) destekler (Hejazi ve diğerleri, 2018).
- Genişletilebilir Mesajlaşma ve Durum Protokolü (XMPP - Extensible Messaging and Presence Protocol): Protokol telefon aracılığıyla çeşitli uygulamalara erişme mekanizması ile birlikte insanlar arasında iletişimi sağlayan cihazların daha hızlı yanıt vermesi ve daha iyi adreslemesi sayesinde tüketici odaklı IoT uygulamaları için daha iyi güvenlik ve ölçeklenebilirlik sağlar (Sharma ve Gondhi, 2018).
- Diğer bir protokol ise uygulama düzeyinde mesaj iletmek için Gelişmiş Mesaj Kuyruğu Protokolü (AMQP - Advanced Message Queuing Protocol)'dür (Sharma ve Gondhi, 2018).

Uygulama Katmanı protokolleri Tablo 1.1'de karşılaştırılmıştır (Sharma ve Gondhi, 2018).

Tablo 1.1. Uygulama Katmanı Protokolleri Karşılaştırması

Parametre	**CoAP**	**MQTT**	**AMQP**	**XMPP**
Tasarım Hedefi	Mesajı genel olarak küçük tutmak ve böylece parçalanma ihtiyacını sınırlamak	Ağ bant genişliğini azaltmak	İş mesajlarını uygulamalar arasında iletmek ve onları başka platformlarda birleştirmek	Kullanıcıların birden fazla anlık mesajlaşma sistemine bağlanmasını sağlamak
Desteklediği Uygulama Tipi	Makine-Makine	Makine-Makine ve Mobil	İş uygulamaları	Makine-Makine için pratik olmayan
Mesaj Değişim Modu	Hem senkron hem asenkron	Asenkron	Asenkron	Hem senkron hem asenkron
Gerçek Zaman Duyarlılığı	Gerçek zamanlı	Gerçek zamanlı	Gerçek zamanlı değil	Gerçek zamanlı
Güvenilirlik	Yerleşik güvenilir bir mekanizma	Farklı Servis Kalitesi seviyeleri ile Mesaj taşıma güvenliği	Sakla ve ilet özelliği güvenilirliği sağlar	TCP garantili güvenilirlik
Güvenlik	DTLS	SSL/TLS	SSL/TLS	SSL/TLS
Servis Kalitesi (QoS)	QoS sağlar	QoS sağlar	QoS sağlar	QoS opsiyonu yok
Mimari	İstek/Yanıt	Yayıncı/ Abone	Yayıncı/Abone	Yayıncı/ Abone İstek / Yanıt
Taşıma	UDP	TCP	TCP	TCP
Güç Tüketimi	Güç tüketimini azaltır	Güç tüketimini azaltır	MQTT'den daha fazla tüketim	Güç tüketimini artırır
Uygulanabilirlik	Web servisler	Küçük boy/güç mobil uygulamalar	İş ve Ticari Platformlar	Sohbet ve mesaj değişimi
Ağ Bant Genişliği	Bant genişliğini artırır	Bant genişliğini azaltır	Bant genişliğini azaltır	Bant genişliğinden yoğun kulanım

Enerji verimliliği, sensörler dahil IoT için protokolleri seçerken dikkate alınması gereken en önemli özelliklerden biridir. Bu nedenle, HTTP gibi tipik web tarayıcısı uygulama protokolleri dışındaki düşük güçlü uygulama katmanı protokollerini dikkate almak gerekir. Cihazlar ve platform arasında, platform içerisinde ve platform ile kullanıcılar arasında farklı iletişim teknolojileri kullanılır. Ayrıca, IoT modülü ve diğer platformlar arasında çok çeşitli iletişim çözümleri bulunabilir. Pille çalışan sensörlerden çok fazla güç almamak önemlidir. Sensörleri internete entegre etmek için birçok IoT uygulama katmanı protokolü mevcuttur, ancak belirli bir uygulama senaryosu için en iyi performans sonuçlarını sağlamak için en uygun uygulama

protokolünü kullanmak önemlidir. QoS (Quality of service), paket teslim oranı, gecikme süresi, güvenlik vb. gibi temel sistem gereksinimleri, seçilen uygulamaya bağlı olarak değişebilir. Bu gereksinimlerin, belirli bir uygulama için en iyi protokolü seçmek amacıyla, farklı protokollerin sunduğu özellik ve işlevlerle eşleştirilmesi gerekir. Bu nedenle, her protokolün kullanım sınıfını analiz etmek, belirli bir uygulamada kullanılmadan önce de önemlidir (Meera ve Rao, 2018).

1.2.4. Uygulama Alanları

IoT birçok farklı uygulama alanında kullanılmaktadır. Uygulama alanlarından bazıları aşağıda sıralanmıştır (Sezer ve diğerleri, 2017).

- Uzay ve havacılık (üretim: şüpheli onaylanmamış parçaların tespiti),
- Eğitim (uzaktan eğitim ve gelişmiş öğrenim),
- Enerji (akıllı ölçüm, üretim ve depolama koordinasyonu),
- Eğlence ve spor (oyun, spor, sinema, akıllı spor salonu),
- Çevre (kimyasal algılama, sıcaklık ve nem izleme),
- Finans ve bankacılık (POS terminalleri, uzak konumlandırılmış ATM'ler, çevrimiçi masaüstü ve mobil cihaz bankacılığı),
- Gıda ve çiftçilik (kontrol ve izleme tesisleri, ürün izleme, hayvancılık, arıza yönetimi, kimyasal ve çevresel koşulların korunması, sipariş hizmetinin otomasyonu, teslim sürecinin otomasyonu ve muhasebe),
- Devlet (gerçek zamanlı çevresel izleme, uzaktan hizmet sunumu, mal/varlık takibi, akıllı şehirler, şehir ve bina yönetimi ve güvenliği),
- Sağlık hizmetleri (uzaktan tedavi ve cerrahi, uzaktan teşhis ve muayeneler, uzaktan hasta gözleme ve izleme ve tıbbi varlık takibi),
- Ev otomasyonu (akıllı ev aletleri, ev güvenliği ve izleme),
- Bilgi ve iletişim teknolojileri (güvenlik ve izleme, uzaktan yönetim, cihaz takibi ve otomasyon).
- Lojistik (mobil biletleme),
- Üretim ve ağır sanayi (süreç izleme ve yönetimi, ekipman izleme, nakliye takibi, uzaktan servis, çalışanları izleme, tedarikçiler ve envanter yönetimi),
- İlaç endüstrisi (ilaç takibi, güvenlik),

- Kamu güvenliği ve askeri (gözetim ağı, uzaktan varlık kontrolü ve takibi ve afet yönetimi).
- Perakendecilik ve misafirperverlik (hırsızlık ve sahteciliğe karşılık, tesislerin izlenmesi ve yönetimi).
- Ulaşım (akıllı yollar, raylar, pistler, destekli sürüş, trafik sinyalleri, güçlendirilmiş haritalar ve akıllı ulaşım sistemleri).
- Araçlar (akıllı otobüs, uçaklar, tekneler, trenler ve otomobiller).
- Su (sistem basıncı, rezervuar seviyeleri ve su kalitesi).

1.3. ASKERİ ALANDA IoT KULLANIMI: KAVRAM, GEREKSİNİM VE KISITLAR

Nesneler akıllı olduğunda kullanıldıkları alan içinde olduğundan daha faydalı ve daha etkilidirler. Birbirleriyle konuşabilen nesneler ya da insanlar ise daha da fazla yarar sağlarlar. Bu mantık askeri savaşların dünyasını dolduran akıllı aygıtlar ve komutanlar için de geçerlidir.

Gelişmiş durumsal farkındalık, günümüz komutanlarının, insansız algılayıcılardan ve raporlardan gelen bilgilerin bütünleştirilmesiyle gerçek zamanlı analize dayalı kararlar almalarını sağlar. Komutanlar, alana yerleştirilmiş sensörler, kameralar, insanlı veya insansız hava araçları (İHA) ve askerlerin kendileri tarafından sağlanan geniş bilgi yelpazesinden yararlanırlar. Cihazlar, mevcut verilerini askeri üsse taşımakta, bazıları komuta merkezine aktarılabilmekte ve analiz edilip kapsamlı savaş alanı durum farkındalığı sağlamak için diğer kaynaklardan gelen veriler ile entegre edilebilmektedir. Elde edilen bu veriler komutanın karar vermesinde büyük rol oynar (Wind,2015).

Onlarca yıl önce, ABD Savunma Bakanlığı (DoD - Department of Defense)'nın sensör, bilgisayar ağı ve iletişim teknolojileri üzerine yaptığı çalışmalar IoT'nin temelini oluşturmada kritik rol oynadı. Bakanlık 1990'ların sonunda bilgi paylaşımını ve iş birliğini geliştirmek için "fiziksel, bilgisel ve bilişsel" üç katmanı entegre eden "ağ merkezli" (network-centric) savaş vizyonunu oluşturmuştur. Ağ merkezli savaş, son savunma dönüşümünün ardındaki itici güç olmuş ve temel alanlarda IoT ile ilgili teknolojilerin benimsenmesini sağlamıştır (Zheng ve Carter, 2015).

Askeri IoT, askeri uygulamaların doğası gereği “sıradan” IoT'den farklıdır: iletişim altyapısının olmaması, cihazların heterojenliği ve siber-fiziksel saldırılara karşı duyarlılık gibi savaş alanlarına özgü zorluklardan dolayı geleneksel IoT ağlarından önemli ölçüde farklıdır. Savaş senaryolarında muharebe verimliliği ve koordineli karar verme gerçek zamanlı veri toplamaya bağlıdır. Bu durum ağın bağlanırlığına ve düşmanların varlığında bilgi yayılmasına dayanır (Farooq ve Zhu, 2018). Bir askeri uygulama daha gelişmiş düşmanlara sahiptir, daha düşmanca ortamlarda faaliyet gösterir ve sağlam bir güvenlik mimarisine ihtiyaç duyar (Fongen ve Mancini, 2015).

Bazı yönlerden, Askeri IoT zaten bir gerçeklik haline gelmektedir ve önümüzdeki yıllar içerisinde savaşta baskın bir varlık haline gelmesi muhtemel görünmektedir.

Geleceğin savaş alanı, çeşitli nesneler tarafından yoğun olarak doldurulacaktır. Nesneler arasında sensörler, mühimmatlar, silahlar, araçlar, robotlar ve insan tarafından kullanılabilecek cihazlar yer alacaktır. Yetenekleri, bilginin seçici olarak toplanmasını, işlenmesini, anlamlandırılmasını, koordineli savunma eylemleri oluşturmasını ve muhalifler üzerindeki çeşitli etkilerini açığa çıkaracak aracılar olarak hareket etmeyi içerecektir. Tüm bunlar cihazların sürekli olarak iletişim kurması, koordine etmesi, müzakere etmesi, ortaklaşa planlaması ve faaliyetlerini yürütmesi ile iş birliği içinde yapılacaktır. (Kott ve diğerleri, 2016).

IEEE Dünya IoT Forumunda IoT Askeri Uygulamalarına yönelik özel oturum açılması bu alana olan yönelimi göstermektedir.

Bunun yanında, NATO STO Military Applications of Internet of Things-IST-147 (COM)- IoT Askeri Uygulamaları Araştırma Çalışma Grubu 2016-2019 yılları arasında, Federated Interoperability of Military C2 (Command and Control-Komuta ve Kontrol) and IoT Systems- IST-176 (COM)- Askeri C2 ve IoT Sistemlerinin Federasyonla Birlikte Çalışabilirliği çalışma grubu 2019-2022 yılları arasında çalışmalarını sürdürmektedir.

Tez çalışmasının genelinde “Askeri IoT” ifadesi yer alacaktır. Bunun yanı sıra askeri alanda IoT, literatürde aşağıdaki gibi farklı ifadelerle de yer almaktadır.

- Internet of Battle Things (Kott ve diğerleri, 2016).
- Military IoT(Furtak ve diğerleri, 2016).
- M-IoT(Fongen ve Mancini, 2015).

- MIOT (Yushi ve diğerleri, 2012).
- Internet of Battlefield Things (Azmoodeh ve diğerleri, 2018, Farooq ve Zhu, 2018).

1.3.1. Askeri Sahada Uygulama Alanları

Askeri sahada IoT kullanım olanakları, esas olarak; C4ISR (Komuta, Kontrol, İletişim, Bilgisayar, İstihbarat, Gözetleme ve Keşif) sistemleri, ateş kontrol sistemleri, lojistik yönetimi, eğitim, simülasyon ve ona yardımcı olmak için asker teçhizatı, iletişim, durumsal farkındalık, sağlık ve güvenliğin güncel olarak izlenmesi gibi uygulamalar için geçerli olacaktır (Furtak ve diğerleri, 2016). ABD, Askeri IoT'nin benimsenmesine yönelik çalışmalarıyla, bu alana öncülük eden ülke olarak görülmektedir (Tonin, 2017). Halihazırda IoT teknolojilerini (Zheng ve Carter, 2015) tam ya da sınırlı uyarlı olarak kullanmaktadır. Şekil 1.11'de yer alan başlıklarda kullanım olanaklarına; Zheng ve Carter'ın çalışmasında yer alan ABD uygulamaları ile başlanarak (4.1.1-4.1.5) detaylı olarak yer verilecektir.

1.3.1.1. Komuta, Kontrol, İletişim, Bilgisayar, İstihbarat, Gözetleme ve Keşif

C4ISR sistemleri, gelişmiş durumsal farkındalık sağlamak için birçok platformdan çeşitli sensörler kullanır. Radar, sonar, video, kızılötesi veya pasif RF algılama verileri; gözetleme uyduları, havadan yayılan platformlar, İHA'lar, yer istasyonları ve operasyon alanında görev yapan askerler tarafından toplanmaktadır. Örneğin, Deniz Kuvvetleri, denizaltıların varlığını tespit etmek için sonar teknolojisini kullanan bağlı şamandıralar ağını işletmektedir. Hava Kuvvetleri, pilotlara gerçek zamanlı olarak ayrıntılı tehdit ve hedef verisi sağlamak için, keşif verileri ile savaş jetlerinden gelen sensör verilerini birleştirir. Kara Kuvvetleri, askerlerin bilinmeyen arazilerde daha iyi dolaşmasına yardımcı olmak için çevresel sensörler ve uydu görüntülerinden gelen verileri birleştirmektedir (Castro ve diğerleri, 2016). Bu veriler, onları analiz eden, komuta zincirinde aşağı ve yukarı bilgi sağlayan bir entegrasyon platformuna teslim edilir. Bu platformlar, alanda daha fazla koordinasyon ve kontrol olanağı sağlayan Ortak Operasyonel Resim (COP - Common Operational Picture) sunar (Fraga-Lamas ve diğerleri, 2016). İlgili (muharebe alanı vb.) alanların durumsal resminin ortaya konması,

durumsal farkındalığı arttırırken; müdahale, karar verme ve geri bildirim sürelerini azaltacaktır (Suri ve diğerleri, 2016).

Şekil 1.11. Askeri IoT Uygulama Alanları

Askeri IoT'nin önemli tasarımlarından biri de yeni nesil uçaklardır. F-35 (Joint Strike Fighter) ABD'nin en gelişmiş savaş uçağı durumsal farkındalığı artırmak için çeşitli verileri toplamak üzere tasarlanmış bir dizi sensörle donatılmış tamamen ağ bağlantılı bir uçaktır. Yerleşik sistemler, pilotun bir görevi tamamlamak için ihtiyaç duyduğu en alakalı bilgileri gösteren kişisel bir gösterge panosu oluşturmak için bu verilerin hepsini analiz eder ve sentezler. F-35'ten gelen veriler nihayetinde savaş alanında neler olup bittiğini daha iyi görebilmek için sahadaki diğer uçaklar, gemiler ve araçlar üzerinde yer alan diğer verilerle birleştirilir.

IoT teknolojileri, ülke seviyesinden şehre, savaş alanına ve hatta tek askere kadar uzanan, sürekli bir algılama spektrumu vizyonunun gerçekleştirilmesine yönelik önemli bir kilometre taşını temsil edecektir.

IoT, gelecekteki C4ISR işlemleri için önemli bir teknolojiyi temsil eder. Aslında, IoT teknolojileri aracılığıyla uygulanan birçok cihaz ve sistem tarafından toplanan doğru ve detay bilgiler, çapraz korelasyon ve analiz aşamalarından sonra, önemli ölçüde geliştirilmiş durumsal farkındalığı ortaya koyacaktır (Tortonesi ve diğerleri, 2016).

1.3.1.2. Ateş Kontrol Sistemleri

Askeri alanda tamamen otomatik sistemler ateşleme alanında yoğunlaşmıştır. Bu sistemler hızlı bir şekilde tepki vermek ve kesin doğruluk sağlamak için sensör verilerini kullanır. Örneğin, ABD Donanmasının Aegis Savaş Sistemi düşman hedeflerini yok etmek için güçlü bilgisayar ve radar teknolojisi kullanan tam otomatik ateşleme kabiliyetlerine sahip entegre bir deniz silahları sistemi olarak tasarlanmıştır. Aegis Savaş Sistemi, yüzey gemilerinde, geminin topçuları ve torpidolarından güdümlü füzelerden, füzesavar silahlara kadar silahların kontrolünü sağlar. AN/SPY radar sistemi, güdümlü mühimmatı bir seferde tam ve otonom olarak 100 hedefe kadar tespit edebilir, izleyebilir ve yönlendirebilir (Zheng ve Carter, 2015).

Bunun yanında yüksek değere sahip stratejik hedeflere ulaşmak ve etkisiz hale getirmek için İHA'lara büyük yatırım yapılmaktadır.

Mühimmatlar ağa bağlanarak akıllı silahların mobil hedefleri izlemesine ya da uçuşun yeniden yönlendirilmesine izin verebilir. En iyi örnek, ABD Donanmasının önde gelen hassas darbe silahı Tomahawk Land Attack Missile (TLAM)dır. Füzenin uçuşta yeni bir hedefe yönlendirilmesini ya da hedef alanın üzerine gelmesini sağlayan iki yönlü bir uydu bağlantısına sahiptir. Üzerinde bulunan kameradaki görüntüleri yeni hedefler belirlemesi ve diğerlerinden gelen hasarları değerlendirmesi için komutanlara göndermektedir (Zheng ve Carter, 2015).

1.3.1.3. Lojistik

ABD Ordusu lojistik yönetimi için IoT teknolojileri sınırlı ölçüde kullanmaktadır. Hizmet sınıflarına lojistik yönetimi sağlayan ABD Savunma Lojistik Ajansı (DLA - Defense Logistics Agency) ve Ulaştırma Komutanlığı (USTRANSCOM - The United States Transportation Command), gönderileri takip etmek ve stokları yönetmek için RFID gibi IoT cihazlarını kullanmaktadır.

Ayrıca DLA, dağıtım merkezlerindeki tanklardaki yakıt seviyelerini izlemek için dijital okuyucular kullanır. Sistem daha sonra sıcaklık gibi ortam koşullarına bağlı olarak verilen yakıt hacmini ayarlamak için yazılım analizi kullanır (Zheng ve Carter, 2015).

Tek bir asker seviyesinde; erzak, su, gıda, piller ve mermiler gibi gerekli malzeme ikmalleri verilen uyarılarla izlenebilir. Çevre, vücut tipi, bireysel tüketim gibi veriler toplanarak, analiz edilip tedarik yoluna gidilebilir (Suri ve diğerleri, 2016).

1.3.1.4. Eğitim ve Simülasyon

IoT teknolojisi askeri eğitim ve simülasyon için de kullanılmaktadır. Örneğin, Canlı eğitim "atış evleri" eğitim egzersizlerinde askerleri izlemek için kameralar, hareket sensörleri ve akustik sensörleri kullanılır. Askerleri gerçek zamanlı olarak koordine eden eğitmenler için veriler mobil cihazlara gönderilir. Egzersiz sonrası düzenlenmiş videolar ile birliklerin gözden geçirilmesi için temel istatistikler üretilir.

"Laser tag" oyununa benzer şekilde boş fişek ve lazerleri kullanarak, canlı piyade savaşını simüle eden Çoklu Entegre Lazer Nişan Sistemi (MILES - Multiple Integrated Laser Engagement System) Simülasyon alanındaki örneklerindendir. Eğitim programı, askerleri sensör yüklü kıyafetler ve boş fişek yüklenen, özel lazerlerle donatılmış silahlarla donatarak canlı savaşı simüle etmektedir. Giysideki sensörler bir lazer tarafından "vurulduğunda/öldürüldüğünde" kayıt alır. Eğitmenler bu simülasyonları gerçek zamanlı olarak geri bildirim sağlamak için izleyebilirler (Zheng ve Carter, 2015).

1.3.1.5. Mobilite

Ordu on yılı aşkın süredir taktiksel mobilite geliştirmektedir. ABD Ordusunun Nett Warrior programı, Android işletim sisteminin tescilli bir sürümünü kullanarak Android

cihazlarını geliştirdi. Bu aygıtlar, veri yeteneğine sahip telsiz ile bağlantı kurarak, sahadaki askerlere 3 boyutlu harita, izleme, dil çevirisi ve yüksek değerli hedeflerin profilleri gibi bir dizi uygulamaya bağlanmayı amaçlamaktadır. Ancak bugüne kadar, bu programlar sınırlı bir şekilde uygulanmıştır. Daha geniş dağıtım, bağlantı eksikliği, sınırlı işlevsellik ve kötü kullanıcı deneyimleri nedeniyle engellenmektedir (Zheng ve Carter, 2015).

1.3.1.6. Akıllı Şehir Operasyonları

Akıllı şehirlerde mevcut IoT altyapıları askeri operasyonlarda da kullanılabilir. Aslında, trafik izleme sistemleri ve video gözetleme ağları gibi mevcut IoT altyapısının algılama yeteneklerinden yararlanmanın, durumsal koşulların bilgisi açısından kritik bir avantaj sağladığı görülebilir (Tortonesi ve diğerleri, 2016).

Bunun yanında, ortam sensörleri tehlikeli kimyasalların varlığını izlemek için kullanılabilir. İnsan davranışlarını izleyen sensörler, şüpheli davranan kişilerin varlığını değerlendirmek için kullanılabilir. Önceden var olan bu altyapılar tarafından sağlanan bilgilerden yararlanmak kritik olabilir (Fraga-Lamas ve diğerleri, 2016).

1.3.1.7. Personel Algılama

Personel algılama çözümleri, biyometrik okumalar ve otomatik jest tanıma çözümleri ile kritik isimleri ele geçirmeyi, bunun yanında askeri personelin fiziksel (ve psikolojik) durumlarını gözlemlemeyi sağlar. Bu sayede komutanlar, askerlerinin niyetlerini daha etkin ve güvenilir bir şekilde anlayabilecektir. Birliklerinin durumu hakkında güncel bilgi almaları, daha iyi karar vermelerine yardımcı olabilir. Ayrıca, malzeme ve takviyenin otomatik olarak çağrılması da sağlanabilir (Tortonesi ve diğerleri, 2016).

1.3.1.8. Tıbbi Bakım

Asker sağlığı söz konusu olduğunda IoT; askerlerin dehidratasyon, uyku yoksunluğu, yüksek kalp hızı veya düşük kan şekeri gibi anormal durumlarından haberdar olabilir ve gerekirse bir hastane tıbbi müdahale ekibini uyarabilir. Bu geniş kapsamlı sağlık ve güvenlik izleme sistemleri, ihtiyaç duyulduğunda sağlık hizmetlerinin

sağlanması da dahil olmak üzere, etkili bir uçtan uca asker sağlık sistemine olanak sağlamaktadır (Fraga-Lamas ve diğerleri, 2016). Bu çabaların, doğru hasta tanımlama, tıbbi hataları azaltma ve kapsamlı tedavi bilgileri sağlama gibi girdilerle bakım kalitesini artıracağına inanılmaktadır.

Muharebe operasyonları sırasında tıbbi durumların ve yaralanmaların tedavisinde yardım, askeri ortamda giyilebilir ve sabit IoT sistemlerinin en çok konu olan uygulamalarından biridir. Askerlerin hayatını kurtaran tıbbi tedavilerde, hızı ve doğruluğu ile kullanımı yüksek potansiyele sahiptir (Wrona, 2015).

Ayrıca ABD Savunma Gelişmiş Araştırma Projeleri Ajansı, Harvard Üniversitesi'yle ortak hareketi izleyen ve kas-iskelet sistemi yaralanma riskini azaltmayı hedefleyen akıllı giysiler geliştirmek için çalışmaktadır (Castro ve diğerleri, 2016).

1.3.1.9. İşbirlikçi ve Kitle Kaynaklı Algılama

IoT görev atamaları ile sensörleri eşleştirerek; istihbarat, gözetleme ve keşif odaklı görevleri azaltabilir. Böylece, sensörler ve sensör platformlarının, kendi başına görev senaryolarını ele almak için aşırı ekipmanla yükümlü olması gerekmez. Örneğin, her biri kendi misyonuna sahip olan ancak yeni ya da beklenmedik gereksinimleri karşılamak için işbirlikçi durumunda bulunan birden fazla cihaz durumsal farkındalığı artırır. Askerlerin hayatta kalma ve görev başarısını artırır.

Kitle kaynaklı algılama, büyük alanların esnek gerçek zamanlı izlenmesi ve görev etkisine yönelik değerlendirmelerde bulunmak için akıllı şehirlerde potansiyel olarak mevcut olan tamamlayıcı hizmetler ile ucuz bir araç olmayı vaat etmektedir (Fraga-Lamas ve diğerleri, 2016).

1.3.1.10. Enerji Yönetimi

ABD Savunma Bakanlığı tesislerinde, verimlilik projelerine yatırım yaparak tesis enerjisine olan talebini azaltmaktadır. Verilerin ve tahmin algoritmalarının kullanıma başlatılması, kullanım örüntülerini daha iyi anlama ve askeri enerji maliyetlerini önemli ölçüde azaltma konusunda yardımcı olabilecektir (Fraga-Lamas ve diğerleri, 2016).

1.3.1.11. Gözetim

Güvenlik kameraları ve sensörleri, gelişmiş görüntü analizi, örüntü tanıma yazılımları ile birleştiğinde güvenlik tehditleri için uzaktan tesis izlemeyi kolaylaştırır. Bu güvenlik kamerası ağı hem iş gücünü hem de güvenlik risklerini azaltır. Deniz gözetimi ele alınacak olursa, İHA'lar, uydu sensörleri ve gemilerle, geniş alanlardaki denizcilik faaliyetlerini ve trafiği kontrol etmeyi mümkün kılar. Balıkçı teknelerini takip eder, çevre koşullarını ve tehlikeli petrol yüklerini denetler (Fraga-Lamas ve diğerleri, 2016). Birlik güvenliği benzer IoT uygulamalarla sağlanabilir.

1.3.2. Gereksinim ve Kısıtlar

Askeri operasyonları çok yakın bir gelecekte fazlasıyla etkileyecek olan IoT, birçok potansiyel fayda yanında pek çok zorluğu da beraberinde getirecektir. IoT teknolojilerinin askeri ekosisteme nasıl entegre edileceği, nasıl etkin bir şekilde kullanılacağı ile ilgili birçok gereksinim ve kısıt bulunmaktadır (Tortonesi ve diğerleri, 2016). Yakın gelecekteki araştırma ve teknoloji geliştirmeleri için ortaya çıkan gereksinimlere, Tablo 1.2'de (Fraga-Lamas ve diğerleri, 2016) yer alan başlıklar altında yer verilmektedir.

Tablo 1.2. Yakın Gelecekteki Askeri IoT Araştırma Başlıkları

ARAŞTIRMA	ALT BAŞLIKLARI
KİMLİK/TANIMA	Kimlik yönetimi IoT için açık çerçeve Soft Kimlik Anlambilim DNA tanımlayıcıları IP ve ID'lerin yakınsama ve adresleme şeması Kimlik kavramını genişletme (kimlik numarasından daha fazlası) Elektro Manyetik Tanımlama (EMID) Çoklu yöntem, bir kimlik
MİMARİ	Ağların mimarisi Uyarlamalı ve içerik temelli mimariler Kendini yöneten özellikler (kendini yapılandırma, kendini iyileştirme, kendini optimize etme, kendini koruma, kendini tanıma, kendini uyarlama, kendini geliştirme ve tahmin etme) Bilişsel ve deneysel mimariler Güvenilir okuyucular, uyarlanabilir kapsama alanı, nesnelerin evrensel kimlik doğrulaması, güç kaybından sonra etiketlerin geri kazanımı, daha fazla bellek, daha az enerji tüketimi, 3-D gerçek zamanlı konum / konum gömülü sistemler Kooperatif pozisyon siber-fiziksel sistemler

Tablo 1.2. (Devamı)

ALTYAPI	Çapraz alan adı uygulaması dağıtımı Entegre ıot, çoklu uygulama ve çoklu sağlayıcı altyapısı Genel amaç ıot: küresel keşif mekanizması
HABERLEŞME	Geniş spektrum ve spektrum farkında protokoller Çipte ultra düşük güç sistemi, çoklu protokol çipleri Çok fonksiyonlu yeniden yapılandırılabilir çipler Entegre çipli antenler Entegre çipli ağlar ve çoklu standart RF mimarileri Kesintisiz ağlar Ağ geçidi yakınsama Hibrit ağ teknolojileri yakınsama 5G gelişmeler Çarpmaya dayanıklı algoritmalar Tak ve kullan etiketleri, kendini onaran etiketler
AĞ	Kendini tanıma, kendini yapılandırma, kendi kendine öğrenme, kendini onarma ve kendi kendini organize etme özelliği olan ağlar Sensör ağı konumları şeffaflığı IPv6 özellikli ölçeklenebilirlik Her yerde IPv6 tabanlı IoT dağıtımı Yazılım tanımlı ağlar Servis odaklı ağ Çoklu kimlik doğrulama, entegre / evrensel kimlik doğrulama IPv6 tabanlı IoT (akıllı şehirler) Kimlik metriklerinin kombinasyonuna dayanan sağlam güvenlik
YAZILIM	Hedef odaklı: dağıtılmış istihbarat, problem çözme, nesneler arası iş birliği ortamları IoT karmaşık veri analizi IoT akıllı veri görselleştirme Hibrit IoT Kullanıcı odaklı: görünmez IoT, insan nesne iş birliği, Kullanıcı merkezli IoT Bilginin Kalitesi ve IoT servis güvenilirliği Yüksek derece dağıtılmış IoT süreçleri Yarı otomatik süreç analizi ve dağıtımı Tamamen otonom IoT cihazları Mikro işletim sistemleri İçerik farkında iş olay üretimi İş olaylarının birlikte çalışabilir ontolojileri
SİNYAL İŞLEME	Metin farkında veri işleme ve yanıtları Dağıtılmış enerji verimli veri işleme Bilişsel işleme ve optimizasyon Ortak sensör ontolojileri
KEŞİF	Otomatik rota etiketleme ve tanımlama yönetimi merkezleri Sensörlerin semantik keşfi Bilişsel arama motorları Otonom arama motorları Güvenlik, gizlilik ve gizliliğe saygı duyulurken, hizmetlerle bağlantı kurmak için ölçeklenebilir keşif hizmetleri

Tablo 1.2. (Devamı)

ENERJİ VERİMLİLİĞİ	Enerji hasadı Zorlu ortamlarda güç üretimi Geri dönüşümlü piller Nano güç işleme ünitesi Enerji geri dönüşüm Uzun menzilli kablosuz güç Her yerde, her zaman kablosuz güç
GÜVENLİK	Düşük maliyetli, güvenli ve yüksek performanslı kimlik / kimlik doğrulama cihazları Kullanıcı merkezli içerik fakında gizlilik Gizlilik farkında veri işleme Güvenlik ve gizlilik profilleri ve politikaları İçerik merkezli güvenlik Homomorfik Şifreleme, aranabilir Şifreleme IoT DoS / DdoS saldırıları için koruma mekanizmaları Kendinden uyarlamalı güvenlik mekanizmaları ve protokolleri Erişim kontrolü ve muhasebe şemaları Genel saldırı tespit ve kurtarma / esneklik Siber güvenlik Güven sağlamak için merkezi olmayan kendi kendini yapılandırma yöntemleri Kişilere, cihazlara ve verilere güveni değerlendirmek için yeni yöntemler Konum gizliliği koruma Kişisel bilginin çıkarım ve gözlemden korunması Güven Müzakeresi
BİRLİKTE ÇALIŞILABİLİRLİK	Otomatik kendinden uyarlanabilir ve çevik (agile) birlikte çalışabilirlik Azaltılmış birlikte çalışabilirlik maliyeti IoT doğrulama için açık platform Teknik ve semantik alanlar için dinamik ve uyarlanabilir birlikte çalışabilirlik
STANDARDİZASYON	M2M standardizasyonu Heterojen ağlarla çapraz birlikte çalışabilirlik standartları IoT verisi ve bilgi paylaşımı için standartlar Otonom iletişim protokolleri standartları Etkileşim standartları Davranış standartları
DONANIM	Akıllı biyo-kimyasal sensörler Nano teknoloji ve yeni malzemeler Etkileşen / İşbirlikçi etiketler Kendinden güç sensörleri Polimer bazlı bellek, ultra düşük güç EPROM / FRAM Moleküler sensörler Şeffaf görüntüler Geri dönüşümlü antenler Nano güç işleme üniteleri Geri dönüşümlü antenler Çok protokollü önyüzler Minimum enerji protokolleri Çok bantlı, çok modlu kablosuz sensör mimarileri uygulamaları Yeniden yapılandırılabilir kablosuz sistemler Sensör ve aktüatör verilerini okumak için çok standartlı protokollere sahip mikro okuyucular Bileşenlerin 3D entegrasyonu dahil Sistem İçinde Paket (SiP) teknolojisi

Aşağıda yer alan başlıklarda uygulamaların karşılaştığı ya da karşılaşacağı gereksinim ve kısıtlar kategoriler halinde derlenerek hazırlanmıştır.

1.3.2.1. İletişim Altyapısı

Ticari ortamda geliştirilen birçok IoT sistemi ve bileşeni, çoğu zaman Wi-Fi, Insteon, Z-Wave, ZigBee gibi bir protokolün ve internete bağlanan ağ geçitlerinin varlığını kabul ederek, iletişim için ağ bağlantılarının kullanılabilirliği hakkında varsayım yaparlar. Benzer şekilde giyilebilir sensörler, Bluetooth veya Uyarlanabilir Ağ Topolojisi (Adaptive Network Topology- ANT) gibi bir Kişisel Alan Ağı (PAN) olduğunu ve bu ağ aracılığıyla cihazın bir cep telefonuna erişebildiğini, daha sonra hücresel ağlar aracılığıyla internete güvenilir bağlantı sağladığını varsaymaktadır. Akıllı şehir cihazları, Internet'e bağlanmak için elektrik hattı, Wi-Fi veya hücresel iletişimin varlığını varsayarlar. Otomobiller, hücresel veya IEEE 802.11p gibi standartları kabul eder. Tek başına çalışan bilgi işlem cihazları bile tipik olarak bir çeşit hücresel iletişim kullanarak ağa bağlanır (Tortonesi ve diğerleri, 2016).

Askeri operasyonlarda ticari IoT'yi benimserken önemli ve başlıca sorun, askeri ağların, özellikle de taktik olanların, genellikle internete bağlanmadığı veya sınırlı ve pahalı (örneğin, SATCOM-Uydu haberleşmesi kullanmak) İnternet erişimine sahip olmasıdır.

Bu durum, çoğu bulut altyapılarına bağlanan cihazların benimsediği bilgi işleme yaklaşımıyla çelişir. Bu durumda veri akışı tipik olarak cihazdan bir ağ geçidine veya cep telefonuna, daha sonra üreticinin sunucularına (Wi-Fi veya hücresel olarak) aktarılır. Burada ham veriler merkezi olarak analiz edilir ve daha sonra kullanıcıya geri gönderilir. Bu modeller, güvenlik gerekçesiyle erişim için askeri ortamda savunulamaz.

Mevcut durumda askeri güçlerin (Kara, Hava, Deniz ve İç güvenlik) her birinin hem bağlantı hem de arka uç sistemleri için kendi altyapısı vardır. Bir muhabere bulut altyapısına geçiş, ortak operasyonlar için hem veri hem de varlıkların paylaşılması konusunda büyük operasyonel avantajlar sağlayabilir. Uygulandığı takdirde, bir savaş bulutu ileriye doğru hareket etmek için bilgi ve kontrol sağlayabilir (Tortonesi ve diğerleri, 2016).

Örneğin, bir F-16 uçağı ile insansız bir araç ya da insansız bir araç ile yer kuvvetleri arasındaki veri nasıl paylaşılır? Lockheed Martin, açık sistem mimarisinin yeni nesil ve eski savaş uçakları arasında gelişmiş birlikte çalışabilirliği nasıl sağlayabileceğini gösterdi. Basın açıklamasına göre, F-22 ve F-35 Kooperatif Aviyonik Testi (CAT-B) çeşitli platformlarda bilgi paylaşımını gerçek zamanlı olarak değerlendirmeyi amaçlamıştır (Wind,2015). F-22 üzerinde Link-16 iletişimi iletme ve alma becerisi, uçak sisteminin entegrasyon zaman çizelgelerinin yeniden kullanımı ve azaltılması, hava Kuvvetleri UCI (Universal Command and Control Interface) mesajlaşma standartlarını kullanma üzerine yapılan çalışmalar açıkça savaş bulutunun ilk adımlarındandır.

1.3.2.2. Sensör ve Cihaz Kullanımı

Güç ya da enerji üzerindeki kısıtlar, savaş ortamının uzun ömürlü sorunlarından biridir. Ticari bir ortamın aksine, sensörleri ve diğer IoT cihazlarını sabit güç kaynaklarına bağlamak her zaman mümkün değildir. Aynı şekilde periyodik olarak şarj etmek de kolay değildir. Askeri alanda, IoT sensörleri ve cihazlarının pil veya güneş enerjisi ile güçlendirilmesi muhtemeldir. Her iki durumda da beklenti, cihazların uzun süreler ya da en azından görev süresi boyunca aktif olmasıdır. Bu nedenle, sensörlerin ve cihazların güç kullanımında etkili olması gerekir. Sistem ya da kullanıcıların bunları makul bir şekilde kullanması gerekir. Örneğin, güneş enerjisiyle çalışan bir cihaz yeniden şarj edilmeden önce oldukça kısa bir görev döngüsüne sahip olabilir. Bu durum göz önüne alınarak planlama yapılması gerekir. Vücuda takılan cihazlarda, askerlerin mevcut ekipmanlarının üzerine ek piller taşımasını beklemek pratik değildir; bu da sistemin bu cihazlara olan taleplerin farkında olması ve bunları yönetmesi gerektiğini gösterir.

Enerji göz önüne alındığı gibi askeri teçhizatın da herhangi bir ticari eşdeğerden daha zorlayıcı çevre koşullarında (Mil-STD-810G'de belirtildiği) çalışacak olması düşünülerek tasarlanmalıdır. Askeri aygıtlara gerekli sağlamlaştırmanın yapılması gerekecektir. Bu işlemlerin, operasyonel yetenekler (örneğin güç hücresi boyutu veya iletim kapasitesi) üzerinde kısıtlamalar getirmesini beklemek makul olacaktır (Suri ve diğerleri, 2016).

1.3.2.3. Güvenlik İhtiyaçları

Askeri IoT sistemleri için güvenlik gereksinimleri, askeri ortamda konuşlandırılan diğer bilgi teknolojileri sistemleri için güvenlik gerekliliklerinden çok farklı değildir. Temelde Şekil 1.12'de görülen gizlilik, bütünlük ve erişilebilirlik ile ilgilidir. Askeri uygulamalarda gizlilik, IoT'deki kullanılabilirlik ve bütünlük özel bir öneme sahiptir. Güvenlik açıklarının varlığı, düşmanların sistemimizi kontrol altına almasına, bloke etmesine veya bize karşı kullanılmasına izin verebilir (Furtak ve diğerleri, 2016).

Şekil 1.12. Güvenlik gereksinimleri

- Gizlilik

IoT sistemleri söz konusu olduğunda, tüm iletişim kanallarının koruması yanında hem uç hem de arka düğümlerde saklanan ve işlenen verilerin korunmasını gerekliliği ortaya çıkar.

Örneğin, kablosuz algılayıcı ağlar ya da insansız araçlar söz konusu olduğunda, gizlilikten ödün vermek, askeri planlara ilişkin ipuçları vererek hem kuvvetleri hem de operasyonun hedeflerini tehlikeye atabilir. Arıca veri akışları sağlayarak; düşmanın durumsal farkındalık bilgisini artırıp, istenmeden destek sağlanabilir (Furtak ve diğerleri, 2016).

- Bütünlük

Operasyon resmine dahil olan ve komuta kararlarına etki eden akıllı nesnelerden gelen bilgilerin değiştirilmemesi ve kullanılabilecek kadar güvenilir olması anlamına gelmektedir. Bununla birlikte, akıllı nesnelere sağlanan komut ve durum bilgisinin de uygun bütünlükte olması önemlidir.

Örneğin, Aralık 2011'de İran'ın bir ABD keşif RQ-170 İHA'sını, kalkış noktasına geri dönmek için aldığı GPS sinyallerini aldatmak suretiyle düşürdüğü bilinmektedir (Furtak ve diğerleri, 2016).

- Erişilebilirlik

Askeri ortamlarda IoT'nin tam potansiyeli, sensör ve cihazlardan sağlanan bilgilerin gerektiği gibi erişilebildiği takdirde sağlanabilir. Benzer şekilde, komut ve kontrol bilgilerinin gerektiğinde aktüatör ve akıllı cihazlara sunulması önemlidir.

IoT ile ilgili "uyku-mahrumiyet saldırısı" olarak adlandırılan spesifik bir saldırı vardır. Bu tür bir saldırı, akıllı nesneler arasında ortak olan, özellikle enerji tasarrufu moduna girmelerini engelleyerek, batarya ile çalışan cihazları hedefler. Bu durum pil gücünün azalmasına ve pillerin yenilenmesi ihtiyacına neden olur. Özellikle savaş durumlarında sistemlerinin hayatta kalması çok önemlidir (Wrona, 2015).

1.3.2.4. Siber-Fiziksel Saldırılara Karşı Hassasiyet

Günümüzde siber saldırılar bilgisayarların ötesine, internete ve akıllı telefonlara, bağlı cihazlara kadar yayılmaktadır. IoT cihazları da dahil olmak üzere ağ merkezli silah sistemlerinin güvenlik tehditleri IoT'nin avantajlarıyla birlikte büyümekte ve hedef haline gelmektedir. Aslında, ağ, İnternet ve İntranet gibi fiziksel olarak ayrı ve uzak olsa da saldırganları durdurmaya yetmemektedir. Basitçe, güvenlik duvarı ve şifreleme cihazları gibi güvenlik çözümleri sunarak mevcut sistemlerin siber güvenliğini arttırmak artık etkili değildir (Cha ve diğerleri, 2018).

Güvenlik açıkları düşmanların, otomatik sistemlerimizi kontrol altına almasına veya devre dışı bırakmasına, görevlerini yerine getirememesine ve hatta kendi varlıklarımızı yine kendimize karşı düşmanca kullanmaya izin verebilir. Aşağıdaki başlıklarda bu güvenlik sorunları detaylandırılacaktır (Fraga-Lamas ve diğerleri, 2016).

- Cihaz ve Ağ Güvenliği

Her yeni teknoloji gibi, IoT potansiyel olarak askeri bilgi sistemlerinde yeni bir saldırı yüzeyi sunmaktadır.

IoT'nin potansiyeli büyük ölçüde her yerde bulunan cihazların (sensör ve aktüatörler) ve uygulamaların yaygınlığından, bunların arasındaki bağlantılardan

(iletişim kanalları) kaynaklanmaktadır. Ancak bu sayısız bağlantı, siber saldırganlar için çok sayıda potansiyel giriş noktası da yaratmaktadır. Bunun yanında IoT potansiyel güvenlik açıklarını içerebilen temel depolama ve işleme fonksiyonlarına da bağlıdır. Depolama ve işleme de bu teknolojinin başlıca önemli parçalarındandır (Furtak ve diğerleri, 2016).

Karmaşık bir ağın güvenliğini artırmanın yollarından biri, saldırganın belirli bir giriş noktasından erişebileceği düğüm sayısını sınırlamaktır. Ancak bu yaklaşım, IoT'yi bir değer kılan farklı sistemlerin entegrasyonu fonksiyonu ile çatışmaktadır (Furtak ve diğerleri, 2016).

Geniş bir cihaz yelpazesini güvence altına almak zordur. Cihazların birçoğu insan arayüzü olmadan sınırlı kapasiteye sahiptir ve verilerin gerçek zamanlı entegrasyonuna bağlıdır. Bu durum, kimlik doğrulama veya gelişmiş şifreleme gibi, güvenlikle ilgili geleneksel yaklaşımları karmaşıklaştırır; ağ üzerinde veri alışverişini engelleyebilir, cihazlarda daha fazla bilgi işlem gücü gerektirir veya insan etkileşimine ihtiyaç duyar.

- İçeriden kötüye kullanma

Siber riskler ve içeriden gelen tehditler büyük kuruluşlar için ciddi bir sorundur. Tek bir kullanıcıdan gelen tek bir hata, saldırganın sisteme erişmesine izin verebilir.

- Elektronik Savaş

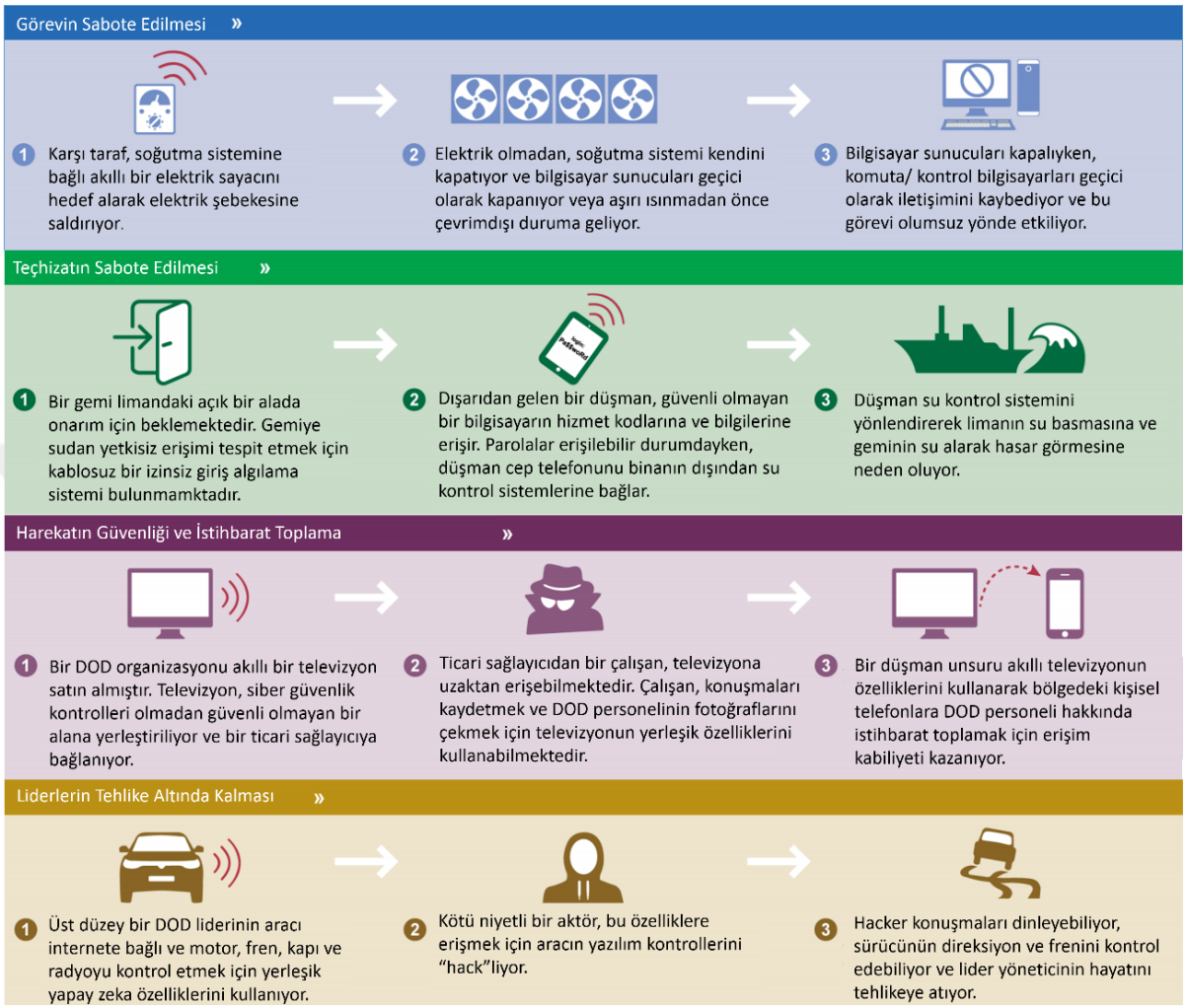
Çoğu teknoloji kablosuz olarak radyo frekansları üzerinden haberleşir. Düşman, parazit yapma tekniklerini kullanarak, cihazların temel altyapı ile iletişim kurmasını sağlayan sinyalleri engelleyebilir. Bunun yanında kablosuz bağlantılar, radyo frekansı emisyonları yoluyla konumun ortaya çıkma riskini artırır. Vericiler, menzil içindeki herhangi bir radyo alıcısı tarafından algılanabilir ve bir işaret olarak hizmet edebilir. Bu durum harekât görevini tehlikeye atabilir (Furtak ve diğerleri, 2016).

- Otomasyon

Ekipman ve araçların tam otomasyonu siber tehditlerin fiziksel alana kadar ulaşmasına neden olabilir.

Bu güvenlik risklerinin operasyonları, ekipmanları veya personeli olumsuz yönde etkileyebileceğini örnekleyen kavramsal tehdit senaryoları ABD Savunma Bakanlığı

tarafından belirlenmiştir. Şekil 1.13, bu senaryoların birkaç örneğini vurgulamaktadır (ABD Devlet Hesap Verebilirlik Ofisi, 2017).



Şekil 1.13. IoT Kavramsal Tehdit Senaryoları

İlk kavramsal IoT senaryosu, "görevin sabotajı", operasyonları olumsuz yönde etkileyebilecek birkaç güvenlik riskini göstermektedir. Altyapıyı izlemek ve kontrol etmek için kullanılan IoT cihazlarının artması, bir ağın veya sistemin saldırıya uğramasına neden olabilecek saldırı noktalarının sayısını artırabilir. Sonuç olarak, akıllı bir elektrik sayacının başarılı bir şekilde nüfuzu, endüstriyel kontrol sistemini olumsuz yönde etkileyen ve devam eden bir görevi bozan basamaklı etkilere neden olabilir. İkinci kavramsal IoT senaryosunda "ekipman sabotajı", zayıf parola yönetimi ve içeriden gelen bir tehdidin birleşimi, su basma sistemi gibi bir yardımcı program sistemine yetkisiz erişime neden olabilir. Gemiye zarar vermek için su kontrol sistemi manipüle edilebilir. Üçüncü kavramsal IoT senaryosu "harekât güvenliği ve istihbarat toplama" üzerinedir.

Akıllı televizyonlardan kaynaklanabilecek olumsuz etkileri göstermektedir. Senaryo, ticari amaçlar veya kötü niyetli amaçlar için bilgi toplamak amacıyla rakipleri tarafından hedeflenen sınırlı siber güvenlik kontrollerine sahip bir televizyonu içermektedir. Dördüncü kavramsal IoT senaryosu, "liderlerin tehlike altında kalması", düşmanın IoT özelliklerine sahip bir arabadan nasıl yararlanabileceğini göstermektedir. Burada düşman örneğin otomobilin cihazlarındaki özelliklerden yararlanarak konuşmaları izlemek, araç işlevlerini kontrol altına almak veya arabadaki üst düzer komutanların hayatını tehlikeye sokmak için kullanılabilir (ABD Devlet Hesap Verebilirlik Ofisi, 2017).

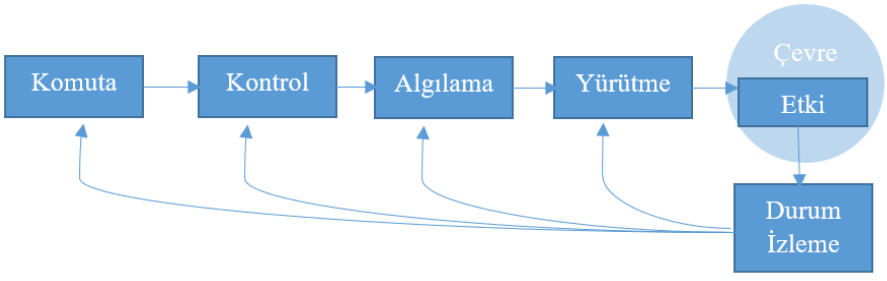
1.3.2.5. Komuta Kontrol

Bu başlığın temel sorusu şudur: "Zeki nesnelerden oluşan bir orduya nasıl kumanda edip, kontrol edebiliriz?"

İnsanlar ve akıllı nesnelerin yönetim işlevi farklı güçlükler getirecektir. Beklenmedik gelişmelere ayak uydurmak için yeterince güçlü olan bu yeni örgütsel forma uygun bir yönetim yaklaşımı tasarlamak için insan bilişinin ve makine zekasının karşılaştırmalı güçlü ve zayıf yönleri iyi anlaşılmalı ve kullanılmalıdır.

Ancak insanlar ve nesneler arasında insana benzeyen güvenin sağlanması zorlayıcı olacaktır. Akıllı nesneler aynı zamanda insanlar ile müzakere etmede nispeten başarısız ancak diğer nesnelerle görüşürken daha başarılı olacaktır. Karma bir insan-nesne takımında uygun rol ve görev tahsisini tanımlamak gerekecektir.

Şekil 1.14, dinamik bir bağlamda istenen etkilerin elde edilmesi için gerekli beş temel C2 fonksiyonunu göstermektedir. Bunlar: komuta, kontrol, algılama, yürütme ve durum izlemedir (Kott ve Albertve, 2017).



Şekil 1.14. Komuta Kontrol Fonksiyonları

Komuta işlevi, amaç oluşturmayı ve organizasyonun istenen sonuçlara ulaşmasını sağlayacak koşulları yaratmayı içerir.

Amaç oluşturma, daha küçük hedeflerin ve önceliklerin belirlenmesi, kuralların oluşturulması ve sınırlamaların belirlenmesidir. Başarı için koşullarının oluşturulması ise, rollerin ve sorumlulukların atanmasını, ilişkilerin tanımlanmasını içerir. İnsan ve diğer akıllı nesnelerin, karar vericilerin ister insan ister makine olsun, istedikleri bilgiye sahip olmaları ve komuta kontrol işlevlerini yerine getirmek için bu bilgileri iyi bir şekilde kullanabilmelerini sağlamak gerekmektedir (Kott ve Albertve, 2017).

Kontrol işlevi, eylemlere, değişen durumlara göre düzeltme yapılması durumudur. İnsanlar, ilgili yeni bilgileri toplayıp değerlendirmeye çalışırken, bilgi aşırı yüklemelerine eğilimlidirler. Zeki nesnelerin parlayabileceği yer burasıdır. Kontrolle ilgili eylemleri insanlardan daha hızlı yapabilirler (Kott ve Albertve, 2017).

Bu çevrede, hızlı tempodan dolayı insanlar, çevik bir uyarlama sırasında akıllı nesnelerin önerilerini veya eylemlerini anlamakta ve onlara güvenmekte zorlanacaklardır.

Algılama işlevi, bilgi, bilişsel ve sosyal alanlarda bir dizi yineleyici faaliyet içerir.

İnsanlardan ve akıllı nesnelerden oluşan bir ekip söz konusu olduğunda, insanlar ve makine istihbaratı bir durumla ilgili ortak bir anlayış geliştirmek için birlikte etkin bir şekilde çalışabilmelidir (Kott ve Albertve, 2017).

Yürütme, fiziksel aksiyonlar almayı veya alt organizasyona eylemleri için emirler vermeyi içerir. Bunların yanında, karar verme ağındaki diğer düğümlerle koordine etmek için karmaşık bir süreç içerir: zaman ve mekândaki eylemleri koordine etmek, eylemler arasında veya karşılıklı bağımlılığı yönetmek ve çatışmaları çözmek bunlardan bazılarıdır (Kott ve Albertve, 2017). Özellikle çatışma çözme hususu, akıllı nesnelerin henüz gelişmemiş olduğu becerilerdendir. Gelişmekte olan bu noktada, insanlar, özellikle insanlarla müzakere ederken, etkili müzakere becerileri konusunda tercih nedenidir.

Durum İzleme, alınan önlemlerin istenen etkileri üretip üretmediğini araştırmaya odaklanır. İnsanlar, akıllı nesnelere göre beklenmedik durumlarda daha iyi düşünürken, değişiklik gerektiğinde bunu fark etmede daha yavaş ve isteksiz olacaklardır (Kott ve Albertve, 2017).

1.3.2.6. Büyük Askeri IoT Bilgisinden Yararlanma

Askeri IoT'de, iletişim bant genişliği kadar önemli olan en ciddi kısıtlama, insan bilişim bant genişliği olacaktır. Asker savaşçılar, Askeri IoT tarafından üretilen muazzam miktarda bilgiyi işleyemez ve işlememelidir. Bunun yerine, mevcut durumları ve görevleriyle ilgili etkili göstergeler ve uyarılar gibi bilişsel ihtiyaçlarına yönelik ihtiyaçlarına odaklanmalıdırlar. Bilgileri yararlı hale getirmek için, Askeri IoT teknolojileri benzeri görülmemiş karmaşık veri hacmi ile uğraşmak zorundadır.

IoT verileri çoklu farklı heterojen kaynaklardan ve etki alanlarından gelebilir; sayısal gözlemler, farklı sensörlerden ölçümler veya sosyal medya akışlarından metinsel girdiler bunlardan bazılarıdır. Bu nedenle, akıllı nesnelerden doğrudan elde edilen veriler, kişiselleştirilmiş akıllı servisler sunmak ve durum açıklamak için yeterli değildir (Kott ve diğerleri, 2016).

Dikkat gerektiren her bir nesneye ve veriye yanıt vermek, Askeri IoT bağlamında uygun bir seçenek değildir. Aslında, Askeri IoT'nin önemli bir riski, insan savaşçılarına (ve akıllı nesnelere), bilginin alınmamış olmasından çok daha olumsuz bir sonuçla harekete geçirebilecek bilgiler vermesidir. Asker performansını olumsuz yönde etkileyebilecek ya da yanlış davranışlara yol açabilecek dikkat dağıtıcı veya ilgisiz (veya daha kötüsü, aldatıcı) bilgiler askerlere iletilmemelidir (Tortonesi ve diğerlerinin (2016).

Savunma ve kamu güvenliği veri ekosistemindeki en büyük boşluklardan biri dijital analitiktir (veri toplama, dönüşüm, değerlendirme ve paylaşma). Algılayıcılar tarafından toplanan büyük verilerin çoğu hiçbir zaman kullanılmaz. Kullanılan kritik verilerde genellikle gecikmelere neden olan manuel giriş ve işleme bağlıdır. Bu gecikmeler misyonların başarısız olmasına, durmasına neden olabileceği gibi karar vermeyi zorlaştırır. Bu yaklaşım külfetlidir. İnsan kaynaklı hatalardan dolayı risk teşkil eder (Fraga-Lamas ve diğerleri, 2016).

Akıllı nesneler, insan savaşçılarla birlikte gelecekteki savaş alanında her yerde bulunabilecektir. Görünüşleri, rolleri ve işlevleri çok çeşitli olacaktır. Farklı noktalardan gelen verinin işlenmesi için kullanılacak yapay zekanın, günümüzün yapay zekâ ve makine öğrenme teknolojilerinin sağladığından önemli ölçüde daha büyük olması gerekecektir. Savaş alanının doğası; çekişmeli, stratejik, hızlı ve tehlikeli olmama gereksinimlerini barındırır. Savaş alanının karmaşıklığı, insanlarla iş birliğinin

karmaşıklığı bir başka önemli itici güçtür. Çekişmeli öğrenme ve çekişmeli akıl yürütme gibi alanlarda büyük ilerlemeler gerekecektir. Büyük miktarda veriyi işlemek için çok yönlü çalışılmış makine-öğrenme yaklaşımları geliştirilmelidir (Kott, 2018).

1.3.2.7. Hata Toleransı

Askeri senaryoların çoğu, güvenlik açısından kritik gerçek zamanlı uygulamalar olarak sınıflandırılabilir. Hizmet ve performansın kalitesini garanti etmek, ağda hatalara, yanlış davranışlara neden olabilecek durumların önüne geçmek için, Askeri IoT'nin hataları tespit edebilmesi, bunun yanında düzelme ve iyileştirmeleri yapması şarttır.

Askeri IoT, güvenilmez donanım, sınırlı enerji, bağlantı kesintisinden kaynaklanan hatalar gibi pek çok sorunla uğraşmak zorundadır. Ayrıca sert ve hatta düşmanca fiziksel ortam (radyasyon gibi), savaş alanında yangın ve sensör donanımına sert nesnelerin düşmesi ve sensör cihazına zarar vermesi gibi hadiseler Askeri IoT için "normal" gerçekler olarak algılanmalıdır. Bu nedenle Askeri IoT uygulamasının tasarlanmasında yeniden organize olabilme, kendini tanımlama, hata toleransı ve güvenlik gibi bir dizi faktör ciddi olarak ele alınmalıdır (Chudzikiewicz ve diğerleri, 2015).

Bu noktada "hataya dayanıklı tekniklerin" ele alınması gerekir. Bu tekniklerin amacı, olası sensör arızalarını, aktüatör hatalarını, işleme elemanlarının hatalarını, haberleşme bağlantılarını ve sistem hatalarını tespit etmek, tanımlamak ve izole etmektir. Hata tespiti, beklenmeyen bir olayın meydana geldiği kabul edilen bir aşamadır. Askeri IoT uygulaması için çevrimiçi tespit en önemlisidir. Gerçek zamanlı hata tanımlama ve ağın normal çalışması sırasında iyileştirme hedeflenmelidir (Chudzikiewicz ve diğerleri, 2015).

1.3.2.8. Politika Belirleme

Riski en aza indiren ve IoT'nin faydasını en yüksek seviyeye çıkaran politikaların geliştirmesine yardımcı olacak politika ilkeleri belirlenmesi çok önemlidir. Bu ilkeler alan genelinde IoT kullanımı konusunda daha iyi ve daha geniş durumsal farkındalık sağlayacaktır. Temel düzeyde, politikalar izleme, gizlilik, güvenlik, bütünlük ve uygun IoT çözümleri konusunda özen gösterilmesini sağlamak için hazırlanmalıdır. ABD

Savunma Bakanlığı tarafından önerilen temel ilkelerin özeti aşağıda sunulmuştur (Chief Information Officer, 2016).

- Her IoT edinimi bir iş süreci tarafından desteklenmelidir.
- Her IoT uygulaması ve ilgili veri akışları bir güvenlik ve gizlilik riski analizi ile desteklenmelidir.
- IoT verileri, maliyetlerin risk ve değer ile orantılı olduğu her noktada şifrelenmelidir.
- IoT şebekeleri, anormal trafik ve ortaya çıkan tehditleri belirlemek için izlenmelidir.
- IoT verileri, analitik özelliklere gönderilecek ve bu bilgiden maksimum fayda sağlamak için karşılıklı korelasyon sağlayacak özellikte olmalıdır.
- IoT cihazları ve Ağları, tam IP ağına sınırsız erişime sahip olmak yerine, mümkün olduğu kadar küçük bir kontrollü ağ segmentine bağlanmalıdır.
- IoT cihazları yalnızca onaylı sözleşmeli araçlar aracılığıyla edinilmelidir.
- Fabrikadan montaja IoT cihaz tedarik zincirleri aktif olarak yönetilmelidir.
- IoT, tehditleri karşılamak ve faydaları gerçekleştirmek için proaktif bir şekilde yönetilmelidir.
- Operasyon ağ işlemleri, IoT cihazlarının ağ kimliğini doğrulayabilmeli ve sağladıkları bilgilerin doğruluğunu izleyebilmelidir.
- Operasyon ağ işlemleri, yetkisiz IoT cihazlarını tespit edebilmeli, izole edebilmeli ve kaldırabilmelidir.
- IoT ağlarının edinilmesi, test edilmesi ve işletilmesi ile ilgili politika ve süreçler denetlenmelidir.

İKİNCİ BÖLÜM

KURAMSAL TEMELLER

1970'lerin sonunda artan teknolojik ihtiyaçlar ve bunun yanında bu teknolojilerin kabul ve kullanımına yönelik artan problemler sistem kullanımına yönelik tahminleri içeren çalışmaları, araştırmacılar için ilgi çekici hale getirmiştir. Ancak o yıllarda yapılan pek çok çalışma, sistemlerin kabul ya da reddini tahmin etmede başarısız olmuştur (Chuttur, 2009).

İlerleyen yıllarda tüketicilerin yeni teknolojileri kabul etmelerini ve kullanım niyetlerini açıklamak için birtakım kuramlar önerilmiştir. Bunların bir kısmı aşağıda sıralanmıştır ancak kuramlar bunlarla sınırlı değildir.

- Mantıklı Eylem Teorisi (Theory of Reasoned Action) (Fishbein ve Ajzen, 1975)
- Planlı Davranış Teorisi (Theory of Planned Behavior) (Ajzen, 1985, 1991)
- Ayrılmış (Decomposed) Planlı Davranış Teorisi, (Taylor ve Todd, 1995)
- Teknoloji Kabul Modeli (TKM), (Technology Acceptance Model) (Davis, Bogozzi ve Warshaw, 1989)
- Yeniliklerin Yayılması Teorisi (Diffusion of Innovation) (Rogers, 1995)
- TKM Son Versiyonu (Venkatesh ve Davis, 1996)
- TKM 2 (Venkatesh ve Davis, 2000)
- Teknoloji Kabul ve Kullanım Birleştirilmiş Modeli (Unified Theory of Acceptance and Use of Technology), (Venkatesh, Morris, Davis ve Davis, 2003)
- TKM 3 (Venkatesh ve Bala, 2008)

Teknoloji kabulü üzerinde çalışmak isteyenlerin öncelikle TKM modelini anlaması önemli ve gereklidir (Chuttur, 2009). TKM'nin evrimini çevreleyen koşulları daha iyi anlayabilmek için de önceki teorilerin ve modellerin kısaca hatırlanmasına ihtiyaç vardır. Teknoloji kullanımı insan yaşamına her yönüyle nüfuz etmektedir. Bu sebeple teknolojinin neden reddedildiği veya kabul edildiği sorusunun cevabı aranmaktadır. Örneğin, insan davranışı ve tutumlarını öngörmek ve kavramak için "Mantıklı Eylem Teorisi" geliştirilmiştir. Bu teori, davranışlardan ziyade davranışsal niyetleri eleştirel

olarak değerlendirmiştir. Teori, aynı zamanda, gerçek davranışın, bir kişinin o davranış için sahip olduğu inançlarının yanı sıra önceki niyetleri ile belirlenebileceğini ima etmektedir. "Planlı Davranış Teorisi", Mantıklı Eylem Teorisinin sınırlamalarına dikkat çekmek için formüle edilmiş ve insanların belirli bir yer ve zaman içerisinde davranışta bulunma niyetini tahmin etmek ve tüm davranışlarını tanımlamak için önerilmiştir. Bu teori temelinde geliştirilen bir sonraki teori ise Ayrılmış Planlı Davranış Teorisi olmuştur (Durodolu, 2016). TKM ise, 1986 yılında Fred Davis'in (Davis, 1986), doktora önerisi olarak tanıtıldı. Mantıklı Eylem Teorisi'nin bir uyarlanması olan TKM, kullanıcıların bilgi sistemlerini veya teknolojilerini kabul etmesinin modellenmesi için özel olarak tasarlanmıştır (Lai, 2017).

2.1. TEKNOLOJİ KABUL MODELİ

TKM temel olarak, kişilerin teknoloji tercihlerini belirlemek, değişime nasıl tepki ya da cevap verebileceklerini ortaya koyabilmek için geliştirilmiştir.

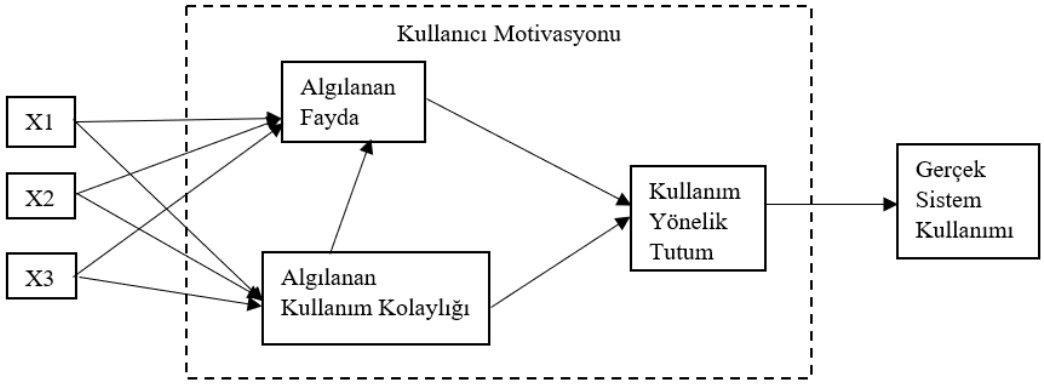
Teknolojik sistemlerin adaptasyon durumlarının açıklanması ve yeni sistemin kabul faktörlerinin ortaya koyulmasındaki başarısı ile oldukça yaygın kullanıma sahip olan TKM (Akça ve Özer, 2012, Lai, 2017), kullanıcıların herhangi bir teknolojiyi kabul etmesiyle ilgilenen araştırmaların çoğunda alıntılandığı için de bu kadar popüler hale gelmiştir. TKM, farklı durumlarda farklı örneklerle geniş bir şekilde test edilmiş ve bilgi sistemi kabul ve kullanımını açıklayan geçerli, güvenilir bir model olduğunu kanıtlanmıtır. İlerleyen yıllarda da TKM'ye yönelik birçok eklenti önerilmiş ve değerlendirilmiştir (Lai, 2017).

Davis, 1986 yılında TKM'yi Şekil 2.1'de gösterildiği gibi bilgisayar kullanım davranışını açıklamak için kullanmıştır. Temel TKM modelinde kullanıcı motivasyonu üç faktörle açıklanmıştır; Algılanan Fayda, Algılanan Kullanım Kolaylığı ve Kullanıma Yönelik Tutum (Davis, 1986).

Hipotezinde *kullanıma yönelik tutumu*, kullanıcının sistemi kullanma ya da reddetmesinde ana belirleyici olarak ön görmüştür. Bu tutum ise iki özel kavramdan etkilenmektedir. *Algılanan Fayda* kişinin bir sistemi kullandığında iş performansını artıracağına dair olan inancına işaret eder. Sistemin öğrenilip kullanılması ile daha faydalı işler yapacağına duyulan inanç olarak da ifade edilebilir. Algılanan fayda doğrudan

kullanım tutumunu etkilemektedir. *Algılanan Kullanım Kolaylığı* ise kişinin bir sistemi kullanırken fiziksel ve zihinsel olarak ilave bir gayrete gereksinim duymadığını algılama derecesi şeklinde tanımlanır. Sistemin zahmetsiz olması kullanıma yönelik tutumu etkiler. Algılanan kullanım kolaylığı ise hem algılanan faydayı ve hem de kullanıma yönelik tutumu etkiler (Davis, 1986, Akça ve Özer, 2012).

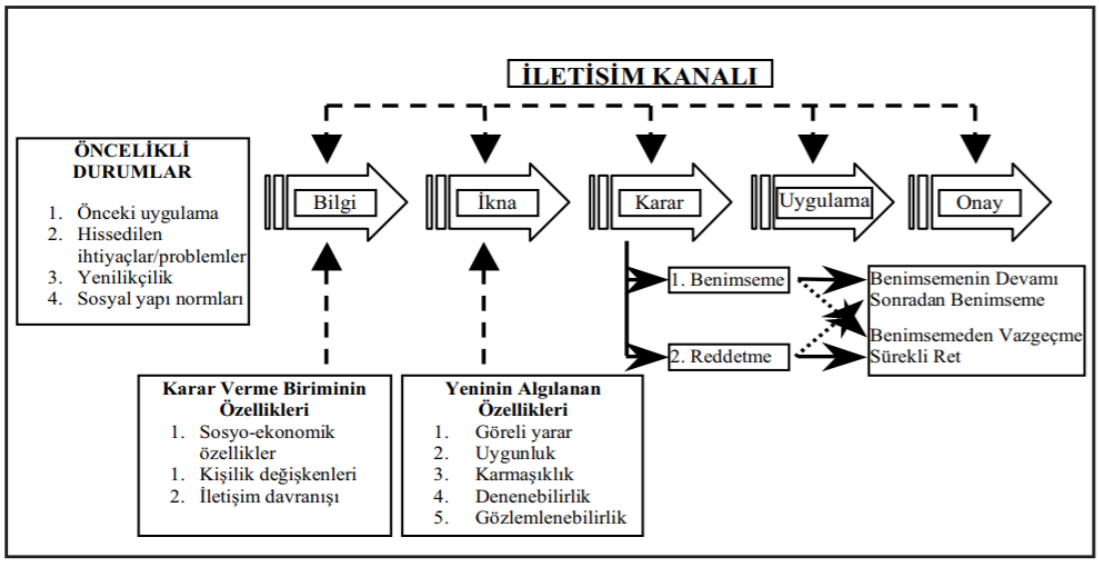
Son olarak hem Algılanan Fayda hem de Algılanan Kullanım Kolaylığı; X1, X2 ve X3 olarak ifade edilen sistem tasarım karakteristiklerinden etkilenir (Chuttur, 2009).



Şekil 2.1. Fred Davis Tarafından Önerilen Orijinal TKM Modeli

2.2. YENİLİKLERİN YAYILMASI TEORİSİ

Rogers, yenilik sürecinin yayılımını açıklamak için bu modeli geliştirmiştir. Yenilik (inovasyon), potansiyel kullanıcılar için yeni olarak algılanan bir fikir, uygulama veya nesne olabilir. Yayılma ise, yeniliklerin bir zaman çerçevesinde, belirli kanallar aracılığı ile bir sosyal sistemin, organizasyonun üyeleri arasında kabulü ve uygulamaya geçilmesini ifade etmektedir. Yeniliğin benimsenip benimsenmemesi ise bir belirsizliktir. Yeniliğin taşıdığı bu belirsizlik yeniliğin yayılmasında önemli bir faktördür. Yayılma anlık bir hareket değildir. Girdileri olan, içerisinde çeşitli hareket ve kararlar içeren bir süreçtir. Bu süreç; Şekil 2.2'de görüldüğü gibi 5 aşamadan oluşmaktadır (Rogers, 2003, Kılıçer, 2008). İlk aşama yenilikten haberdar olunduğu bilgi aşaması, sonrasında yeniliğin algılanan özelliklerinin girdisiyle oluşan ve yeniliğe yönelik tutumun geliştirildiği ikna aşaması, yeniliğin ret ya da kabulüne ilişkin karar aşaması, yeniliğin uygulamaya geçildiği uygulama aşaması ve son olarak onay aşamasından oluşmaktadır (Kılıçer, 2008).



Şekil 2.2. Yayılma Süreci

İnovasyonun algılanan özellikleri, inovasyonun benimsenmesinin farklı seviyelerini açıklamaya yardımcı olur. Rogers (1995, 2003) tarafından belirlenen bu özellikler Göreli Yarar, Karmaşıklık, Uygunluk, Denenebilirlik, Gözlenebilirlik olup aşağıda açıklanmıştır.

- **Göreli yarar**, belirli bir kullanıcı grubunun, inovasyonu yerine geldiği uygulama ya da fikirden daha iyi algıladığı görüşüdür. Kişi ya da organizasyon tarafından inovasyonun algılanan göreceli avantajı ne kadar büyük olursa, benimseme seviyesi de o kadar hızlı olacaktır. Göreceli avantaj, finansal veya finansal olmayan konularda olabilir. Avantajın derecesi ekonomik, sosyal prestij, rahatlık ve zevk terimleriyle de ilişkilendirilebilir. Ancak, göreceli üstünlüğe kimin dahil edildiğine dair kesin bir kural yoktur. Bireysel algılara ve kullanıcı grubunun ihtiyaçlarına bağlıdır (Rogers 1995, 2003, Dibra, 2015).

- **Karmaşıklık**, inovasyonun anlaşılması ve kullanılmasına yönelik algılanan zorluk derecesidir. Yeniliği anlamak ne kadar basit ise yenilik o kadar çabuk uyum sağlar. Anlaması ve kullanması karmaşık olan yenilikler, kullanıcıların yeni beceriler geliştirmelerini gerektirecektir (Rogers 1995, 2003, Dibra, 2015).

- Mevcut değerlere ve uygulamalara **uygunluk**, inovasyonun mevcut değerlere, geçmiş deneyimlere ve potansiyel ihtiyaçlara olan uygunluğu algılama derecesidir. Uygulamalarının değerleri ve normlarıyla uyumlu olmayan bir fikir,

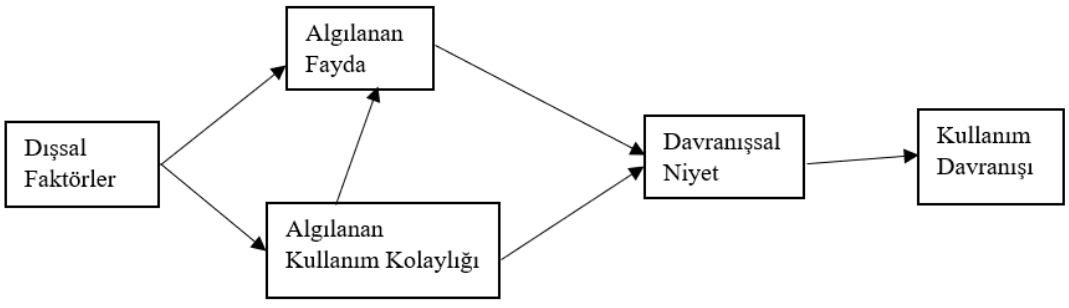
uyumlu olan bir inovasyonun uyarlanması kadar hızlı olmayacaktır (Rogers 1995, 2003, Dibra, 2015).

- **Denenebilirlik**, inovasyonun çoğu potansiyel uygulayıcıyı gerçekten ikna etmeden önce, sınırlı bulgularla kanıtlanma derecesidir. Eğer inovasyon test edilmezse başarılı olması beklenemez. Doğrulanabilir inovasyon, yeni kullanmayı düşünenler için bireye daha az belirsizlik gösterir ve deneyerek öğrenebilir (Rogers 1995, 2003, Dibra, 2015).
- Sonuçların **gözlenebilir** olma ayırt edici özelliği, inovasyon sonuçlarının diğerlerinden daha görünür olma derecesidir. Bir inovasyonun sonuçlarının birey tarafından fark edilmesi daha kolaysa, bunu benimsemeleri daha olasıdır. Böyle bir ayrım, çoğu zaman inovasyon hakkında değerlendirme ihtiyacı olanlar için tartışma ortamını teşvik eder (Rogers 1995, 2003, Dibra, 2015).

2.3. TKM'NİN UYARLAMA VE GELİŞTİRMELERİ

Davis'in (1989) kabul modeli 40.000'in üzerinde referans alınma ile çok geniş uygulama alanında kullanılmış ve geliştirilmiştir.

TKM'nin son versiyonunu, Şekil 2.3'de gösterildiği gibi Venkatesh ve Davis (1996) tarafından oluşturulmuş ve hem algılanan fayda hem de algılanan kullanım kolaylığının davranış niyetinde doğrudan bir etkiye sahip olduğu, dolayısıyla tutum yapısına duyulan ihtiyacı ortadan kaldırdığı belirtilmiştir.



Şekil 2.3. TKM Son Versiyonu

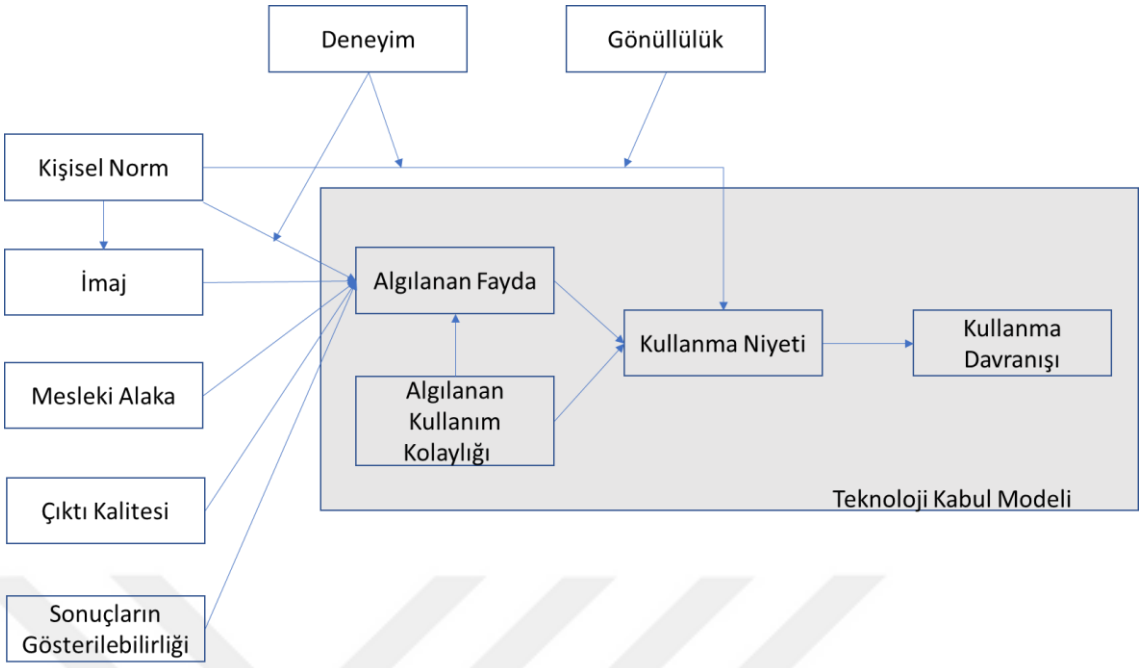
Dışsal Faktörler: Yeni becerilerin kullanımı ve benimsenmesinde TKM ile kullanılabilecek birçok dış değişken olduğunu doğrulanmaktadır. İnsanların yeni

beceriler edinme sürecini açıklamak için popüler olan 70'ten fazla dış değişkeni Tablo 2.1'de (Winarto, 2016) tanımlamaktadır.

Tablo 2.1. TKM Dışsal Faktörler

Organizasyonel Karakteristikler	**Sistem Karakteristikleri**	**Kullanıcı Karakteristikleri**	**Diğer Değişkenler**
Rekabetçi çevre	Sistem tasarımı	Yaş	Kültürel Yakınlık
Kullanıcı desteği	Sistem operasyonu	Bilişsel yetenek	Dış hesaplama desteği
İç eğitim	Sistem bakımı	Bilgi kaygısı	Kolaylaştırıcı durum
Yönetim desteği	Sistem geliştirme	Bilgisayar kaygısı	Öznel formlar
Politika desteği	Sistem denetimi	Bilgisayar okur-yazarlığı	Sosyal baskı
Organizasyonel yapı	Erişim ücreti	Eğitim seviyesi	Sosyal etki
Emsal etkisi	Arayüz	Tecrübe	Değişim Argümanı
Eğitim ve geliştirme	Kolaylık	Cinsiyet	
	Kullanıcı dostu olma	İçsel motivasyon	
	Bilgi kalitesi	Kişilik	
	Sistem kalitesi	Algılanan keyif	
	Siber güvenlik	Algılanan eğlence (oyun)	
		Öz-yeterlik İş yerinde görev süresi	

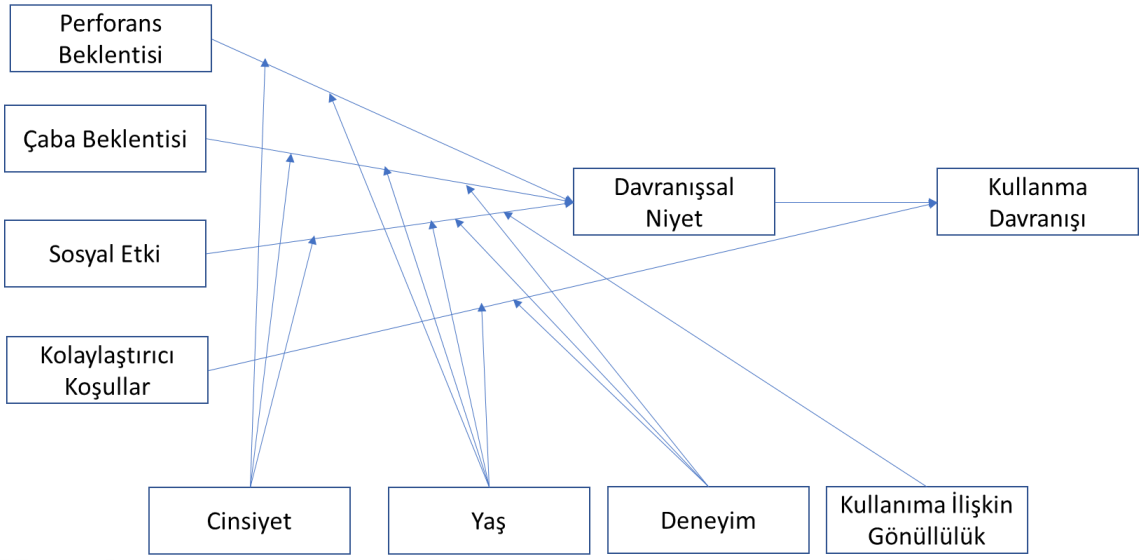
Temel modelde yer alan iki ana inancın: algılanan fayda ve kullanım kolaylığının arkasında yatan nedenlerin tespit edilmesi kolay değildir. Bu çevçere göz önüne alınarak TKM versiyonları geliştirilmiştir. Önemli geliştirmelerden bir tanesi Venkatesh ve Davis'in geliştirdiği (2000) Şekil 2.4'te görülen TKM 2'dir.



Şekil 2.4. TKM 2 Modeli

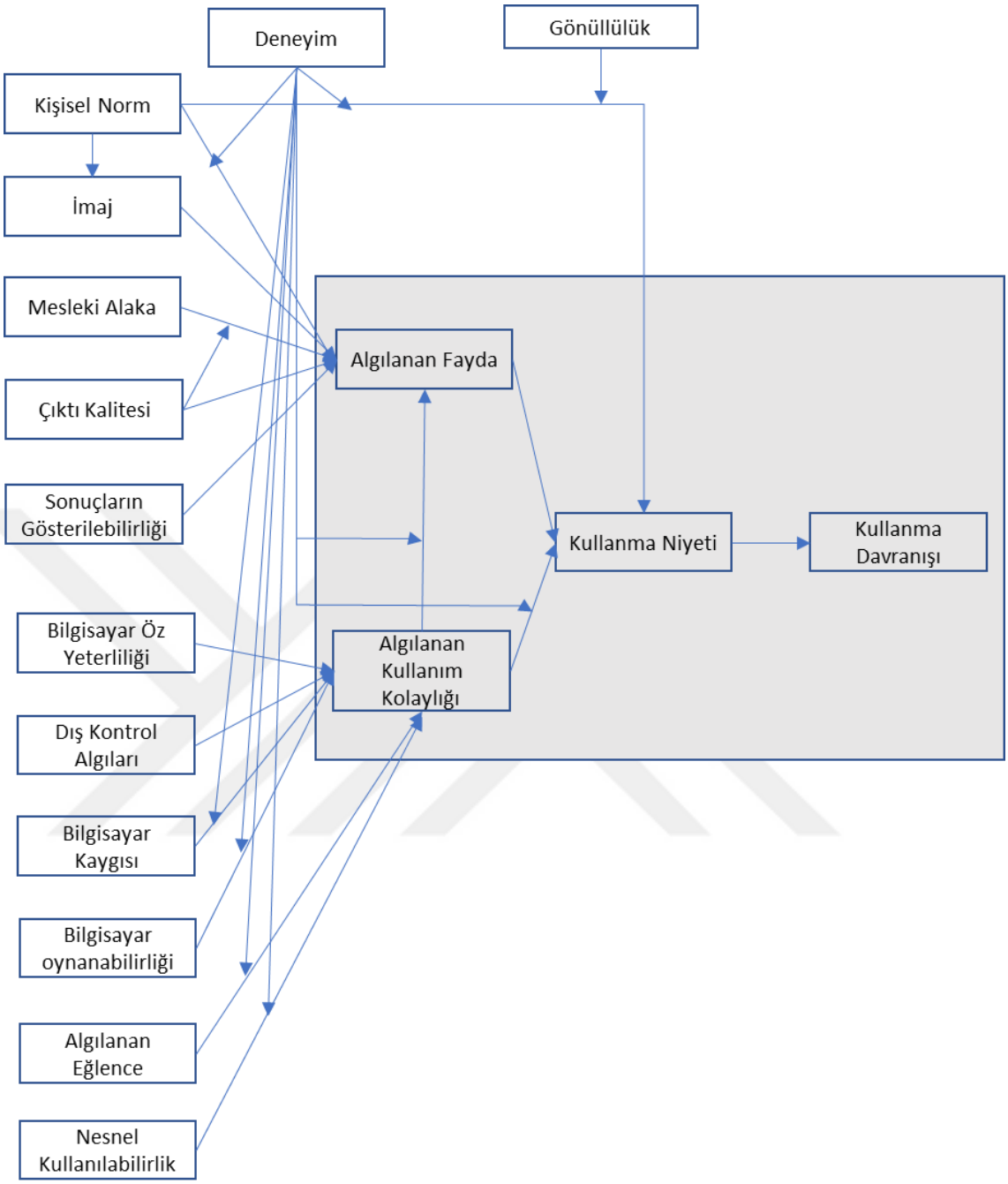
Bu modele göre, bireylerin yeni bir teknolojiyi kullanmada o sistemin; kullanımı kolay ve faydalı olmasının etkisinin arkasında ya da yanında, kişinin önem verdiği insanlarında gerekli bulması, statüsünde bir artış sağlaması, mesleğiyle ilgili olması, faaliyetlerinin sonuçlarının başarıyla çıktı vermesi, gönüllü olarak yapılması ve gösterilebilir somut faydasının bulunması başlıca etkenlerdir (Bağlıbel ve diğerleri, 2010).

Venkatesh ve diğerleri 2003 yılında ise daha önceki modellerin sentezi olan Teknoloji Kabul ve Kullanım Birleştirilmiş Modeli- TKKBM'yi ortaya koymuştur. Şekil 2.5'te gösterilen bu modelde niyet veya kullanımı doğrudan etkileyen belirleyici faktörler: performans beklentisi, çaba beklentisi, sosyal etki ve kolaylaştırıcı şartlar olarak kabul ve kullanım davranışında ana role sahiptir. Ana roller dışında dolaylı olarak niyet ve kullanımı etkileyen: cinsiyet, yaş, deneyim ve gönüllülük faktörleri de aracı değişkenler olarak bazı çalışmalarda ele alınırken bazılarına hiç dahil edilmemiştir (Oktal, 2013).



Şekil 2.5. TKKBM

Venkatesh ve Bala (2008), TKM2 (Venkatesh ve Davis, 2000) ve algılanan kullanım kolaylığı belirleyicileri modelini birleştirmiş (Venkatesh, 2000) ve Şekil 2.6'da gösterilen TKM3 olarak bilinen entegre bir TKM geliştirmiştir. TKM3'ü bireysel farklılıklar, sistem özellikleri, sosyal etki ve ortam koşullarını içeren dört farklı türü, algılanan fayda ve algılanan kullanım kolaylığı belirleyicileri olarak ele almıştır. TKM3 araştırma modelinde, kullanım kolaylığından algılanan faydaya, bilgisayar kaygısından algılanan kullanım kolaylığına ve algılanan kullanım kolaylığından davranışsal niyete değişimler deneyimler tarafından denetlenmiştir. TKM3 araştırma modeli, BT uygulamalarının gerçek dünya ortamlarında test edilmiştir (Lai, 2017).



Şekil 2.6. TKM3

2.4. GEÇMİŞ ÇALIŞMALAR

Literatürde farklı teknolojiler üzerinde pek çok çalışma yapıldığı görülmektedir. Geçmiş çalışmalar iki başlık altında derlenmiştir: ilk olarak IoT'nin kabulü üzerine yapılan çalışmalar ve sonrasında askeri alan içinde farklı teknolojiler üzerine yapılan kabul çalışmaları incelenmiştir.

2.4.1. IoT Alanında Kabul Çalışmaları

Kowatsch ve arkadaşlarının (2012) çalışmalarında kritik gizlilik faktörü ve kabul araştırmalarını birleştiren bir model oluşturmak amaçlanmıştır. IoT hizmetleri için geliştirilmiş, başarılı bir şekilde test edilmiş ve kritik gizlilik faktörlerini içeren bir çalışma olmadığı değerlendirilmiştir. Bu maksatla bu faktörlerin kişilerin IoT teknolojilerini kullanma davranışsal niyetine, kişisel ve organizasyonel verileri sağlama isteklerine etkisi araştırılmıştır. Çalışma politika yapıcılara, bilgi teknolojileri geliştiricilere, bilgi sistemleri araştırmacılarına IoT hizmetlerinin nasıl tasarlanabileceğine dair öneriler sunarak, bu bilgi eksikliğini gidermeyi hedeflemiştir. Teorik yapılar ve ilişkileri temel alarak Genişletilmiş Gizlilik Analiz Model'inden türetilmiştir. Ek olarak, TKM'den algılanan fayda ve kullanma niyeti de modele dahil edilmiştir. 92 bilgi teknolojisi meraklısı çevrimiçi bir anket vasıtasıyla çalışmaya katkı sağlamıştır. Sonuçlar, IoT hizmetlerini kullanmak için davranışsal niyetlerin algılanan gizlilik riskleri ve kişisel çıkarlar gibi çeşitli çelişkili başarı faktörlerinden etkilendiğini göstermektedir. Yani, adaptasyon sürecinin bu faktörler arasındaki dengeden kaynaklandığı belirtilmiştir. Ayrıca, mevzuat ve veri güvenliği gibi bağlamsal faktörlerin yanı sıra bilgi kullanımının şeffaflığının IoT hizmetlerinin benimsenmesini etkilediği çalışmada yer almıştır.

Gao ve Bai (2014) çalışmalarında tüketicilerin IoT teknolojisini kabul etmelerini belirleyen bütünleştirici bir faktörler modeli geliştirmeyi ve test etmeyi amaçlamıştır. Model, TKM'den algılanan fayda, algılanan kullanım kolaylığı, bir sosyal bağlam faktörü (sosyal etki), iki bireysel kullanıcı özelliği (algılanan zevk ve algılanan davranış kontrolü) ve güven faktörlerinden oluşmaktadır. Araştırma modelini test etmek için 368 Çinli tüketiciden elde edilen veriler kullanılmıştır. Sonuçlar, algılanan fayda, algılanan kullanım kolaylığı, sosyal etki, algılanan zevk ve algılanan davranış kontrolünün kabul üzerinde etkileri olduğunu güçlü bir şekilde desteklemiştir. Bununla birlikte, güven faktörünün niyetin öngörülmesinde önemli bir rol oynamadığı görülmüştür. Bireysel TKM modeliyle karşılaştırıldığında, entegre modelin, IoT kullanımına yönelik kullanıcının davranışsal niyetini açıklamada daha başarılı olduğu belirtilmektedir.

Bernsdorf ve diğerleri (2016), tüketicilerin IoT cihazlarını kabul ya da red etmelerinin başarıyla tespit edilmesi gerektiğinin altını çizerek, şirket perspektifine

odaklanmıştır. 146 katılımcı ile TKM ve bağlantılı dış faktörler ele alınarak bir anket yapılmış, tüketici anlayışı doğrudan tüketici verileri ile test edilmiştir. Sonuçlar tüketicilerin daha kolay bir günlük yaşama sahip olma ve daha akıllı evlerde oturma eğiliminde olduklarını göstermektedir.

Macik 2017 yılında yayınladığı makalede, genç tüketicilerin, algılanan maliyetler ve gizlilik endişelerine rağmen, gelişen bir teknoloji olarak kabul edilen IoT'yi benimseme konusundaki durumlarını ortaya koymaktadır. Çalışmasında analiz verileri Doğu Polonya'dan 223 genç tüketicinin örnekleminden alınmıştır. IoT'nin genç tüketiciler tarafından benimsenme seviyesi oldukça yüksek bulunmuş (cevap verenlerin% 80'inin en az bir IoT özellikli cihaz kullanması), ancak IoT cihazlarının sahiplerinin % 78'inin IoT kavramının farkında olmadığı tespit edilmiştir. Araştırmaya katılanlar, IoT'nin bilinçli kullanımından ziyade, bağlantı teknolojisi (Wi-Fi, Bluetooth) tarafından tanınan bağlantılı nesnelerin kullanımını açıkladıkları ifade edilmiştir. IoT'nin benimsenmesini etkileyen faktörler arasında performans beklentisi, alışkanlık yapıları ve bilgi teknolojisi alanındaki kişisel yenilikçiliğin, IoT'yi kullanma davranış niyetini etkilediği gösterilmiştir. Bazı cihaz grupları için cinsiyetin etkili olduğu ama gelir durumunun açıklayıcı bir değişken olmadığı da sunulan bir başka sonuç olarak yer almıştır.

2.4.2. Askeri Alanda Kabul Çalışmaları

Levy ve Green (2009) çalışmalarında, ABD Donanması'nın Muharebe Bilgi Sistemleri Kabul Modelini değerlendirmek için TKM'yi, Bilgisayar Öz Yeterliliği (Chau,2001) modeli ile genişleterek beş farklı ABD Donanması uçak gemisinden 237 denizcinin katılımıyla bir anket örneği kullanmış ve genişletilmiş model değerlendirilmiştir. Sonuçlar, algılanan kullanım kolaylığının, algılanan faydanın ve bilgisayar öz yeterliliğinin, teknoloji kabulünün geçerli öncülleri olduğunu (kullanım amacı ile belirtildiği gibi) göstermektedir.

Hathaway ve Cross (2016), çalışmalarında ABD Savunma Bakanlığı'nın yüksek bütçe kesintileri yanında, kritik askeri eğitimlerin tamamlanmasını beklemelerinin sonucu olarak eğitimde kullanılmak üzere tasarlanmış ve öğrencilere zorunlu olarak uygulanan eğitim teknolojisinin kabulünü incelemişlerdir. ABD C-130 uçak mürettebatı için uygulanan yeni eğitim teknolojisinin kabulünü ortaya koymak maksadıyla,

zorunluluk durumu göz önüne alındığından TKM3 modelini temel alan 27 soruyla eğitimi alan 18 katılımcının görüşlerini almıştır. Bu örneklem büyüklüğü, araştırmanın dar hedefleri ve askeri öğrencilerin homojenliği göz önüne alındığında, kişisel görüşme sürecinde deneyimleri iletmek için yeterli kabul edilmiştir. Toplanan ve derlenen sonuçlar, öğrencilerin teknolojiyi nasıl kullandıklarını, öğrencilerin neden teknolojiyi kullandıklarını ve eğitimlerinin değerini nasıl algıladıklarını anlatmıştır. Materyal sunum tarzının ve bir kişinin öğrenme tarzının, yeni teknolojiyi nasıl kabul ettiği ile bağlantılı olduğu, eğitmenlerin teknoloji hakkındaki girdilerine olan güven seviyesinin öğrenciler için önemli olduğu, askeri eğitim gibi zorunlu kullanım koşullarında, algılanan kullanım kolaylığının, bir kullanıcının bu teknolojiyi kabul etme istekliliğini artırdığı değerlendirilmiştir.

Elstad ve Reitan (2015) çalışmalarında, askeri alanda akıllı telefonlar ve tabletler gibi mobil bilgi platformlarının potansiyel kullanımı için tutum, uyumluluk, çaba ve performans beklentisi incelemesini sunmaktadır. Askeri organizasyonlar birçok zaman yeni teknolojilere öncülük etmekle birlikte bazı yeni teknolojilerin adaptasyonu içinde erken katılımcılardan olmayabilmektedir. Mobil bilgi platformları büyük olanaklara sahiptir. Ancak askeri organizasyonlar için, güvenlik ve güvenilirlik sorunları mobil bilgi platformlarının olanaklarını gölgeliyor gibi görünmektedir. 87 Norveç askeri personelinden veri toplayarak, ordunun mobil bilgi platformlarına dair beklentilerine odaklanmaktadır. Bu çalışma TKM ve TKKBM'yi baz alarak, askeri alanda akıllı telefonlar gibi mobil bilgi platformlarının kullanımına ilişkin çaba, tutum, uyumluluk ve performans beklentilerini ortaya koymaktadır. Çalışma sonucunda katılımcıların ilgilendikleri bilgiye doğrudan, zamanında sahip olma ve paylaşma ile ilgili mobil bilgi platformlarından yüksek beklentileri olduğunu ortaya koymuştur. Öte yandan, güvenlik ve gizlilik konularında mevcut iş süreçlerinin mobil bilgi platformlarının özelliklerine uygun olmadığı ortaya konulmuştur. Ancak hali hazırda bir dereceye kadar kullanılmakta olan ve ilerleyen yıllarda askeri süreçlerin muhtemel bir parçası olacak bu platformların yeterli etkiye erişebilmesi için bu kavram üzerinde daha fazla vurgu yapılması gerekmektedir.

Çiğdem ve Öncü (2015), "Bir Askeri Meslek Yüksekokulunda E-Değerlendirme Adaptasyonu" adlı çalışmalarında artan e-değerlendirme eğiliminin hızla tüm eğitim alanlarına yayılarak (giriş sınavları, yabancı dil sınavları, ticari eğitim sınavları) zaman

ve mekân kısıtı olmaksızın uygulanmasını anlatmışlardır. Türkiye'deki bir askeri meslek yüksekokulunda bilgisayar ağları dersi için MOODLE teknolojisi üzerinde uygulanan e-değerlendirme sürecini TKM 2 modeli referans alarak, bu derse kayıtlı 291 lisans öğrencisinden oluşan katılımcısı ile değerlendirmişlerdir. Öğrenciler e-değerlendirmenin faydalı olduğunu düşünürlerse, bunu kullanmadaki davranışsal niyetleri daha güçlüdür. Bu noktada diğer teknolojilerdeki algılanan faydadan farklı bir etkisi yoktur. Bu nedenle, algılanan yararı herhangi bir yolla iyileştirmek sistemin kullanımı üzerinde olumlu etkiye sahip olacaktır.

Yapay zekâ otonom yönetim teknolojisinin askeri alanda kabulü, asimilasyonu ve kökeninde Mantıklı Eylem Teorisi olan TKM objektifinden kullanımı üzerindeki etkisi, Carmack (2016)'ın doktora çalışmasının konusudur. Çalışmasının amacı, insan yaşamının yerini almak için tasarlanmış bir çeşit yapay zekâ öz-yönetim teknolojisini geliştiren veya kullanan Amerikan Birliği üyelerinin algılarını araştırmaktır. Yapay zekâ otonom yönetim teknolojini bilen10 emekli asker bu çalışmanın anketine katılımcı olarak katkı sağlamıştır. Özerk teknolojinin işlediği verilerin yönetimi ve korunması sivil ve askeri planlamacılar için büyük bir endişe kaynağı olarak görülmüştür.

ÜÇÜNCÜ BÖLÜM

ASKERİ ALANDA NESNELERİN İNTERNETİNİN KULLANIMI VE KABUL MODELİ

Son yıllarda IoT üzerinde hem akademik hem de ticari anlamda yaygın olarak çalışmalar yürütülmektedir. Bu açıdan bakıldığında bu çalışma, giderek önemi artan ve artık günlük hayatımızda da günden güne önemli bir unsur haline gelen IoT'nin, daha sınırlı bilgiye sahip olduğumuz askeri alan içinde tanımlanmasında ve özellikle alana özel gereksinimleri olan bu alan içinde kullanılabilirliğinin değerlendirilmesinde büyük önem arz etmektedir.

3.1. ARAŞTIRMANIN AMACI

Bu çalışmanın amacı askeri alanda IoT'nin, potansiyel kullanım alanlarıyla, fayda ve kısıtlarıyla derinlemesine incelenmesidir. Araştırmanın alt problemleri şu şekilde sıralanmaktadır:

- Askeri alanda IoT kullanılabilirliği mümkün müdür?
- Askeri alana ait kısıtlar var mıdır?
- Personelin kullanıma yönelik beklentileri nelerdir? Bu alanda teknolojinin kabul ve kullanımına yönelik faktörler nelerdir?

Bu sorular yanında aşağıdaki hipotezler değerlendirilecektir.

- Askeri IoT, askeri uygulamaların doğası gereği "sıradan" IoT'den farklıdır.
- Geleneksel askeri teçhizatın çeşitli uyarlamalarla IoT için kullanılması mümkündür.
- Geleceğin savaş ortamı ve savaş sanatı IoT ile temel değişikliklere uğrayacaktır.
- Yüksek düzeyde bağlı bir çalışma ortamı olarak gelecekteki askeri savaş alanının Doktrin ve Teknikleri, Taktikleri ve Prosedürleri temelde değişikliğe uğrayacaktır.

Literatürde askeri alanda IoT teknolojisinin uygulanması amacıyla yapılan ve yapılmakta olan çalışmalar bulunmakla birlikte, IoT'nin kullanım ve kabulünü, personel

tarafından algısını, benimsenme durumunu ortaya çıkarmayı amaçlayan bir çalışmaya rastlanmamıştır.

3.2. ARAŞTIRMANIN MODELİ VE HİPOTEZLERİ

Bu çalışmada, askeri alanda IoT kullanımına yönelik olarak önerilen kabul modeli, TKM ve YYT teorilerinin entegre edilmesi ile oluşmuştur. TKM ve YYT'yi daha önce entegre eden çalışmalar literatürde mevcuttur (Wu ve Wang, 2005, Mutahar vd., 2017). Birleştirilmiş bu entegre modele hem literatürde yapılan çalışma hem de gerçek alan tecrübeleri göz önüne alınarak "maliyet", "risk" ve "güven" faktörlerinin eklenmesi gerekliliği değerlendirilmiş ve model bu şekilde önerilmiştir. Bu faktörler sırasıyla aşağıda detaylandırılmaktadır.

TKM ve YYT, bazı yapılarda oldukça benzer ve birbirini tamamlar durumda bulunur. Bazı araştırmacılar bütünleştirilmiş modelin tek başına modellenmiş durumlarından daha güçlü bir model sağlayabileceğini belirtmişlerdir. Çalışmada YYT'den; göreli yarar, karmaşıklık ve uygunluğun yeni teknolojinin benimsenmesi ile ilişkili olduğu ileri sürülmüştür. Göreli yarar TKM'de yer alan **algılanan faydaya**, karmaşıklık ise **algılanan kullanım kolaylığına** benzemektedir (Wu ve Wang, 2005, Mutahar vd., 2017).

Bir teknolojinin kullanımı kolay ve çok erişilebilir olduğu düşünüldüğünde, kullanıcıların bilgi sistemini kullanma konusunda olumlu bir tutumu olması muhtemeldir. Organizasyonlarda, algılanan kullanım kolaylığı, kullanıcıların teknolojiye kolayca katılabileceği, etkileşim sürecinin basit ve kısa olduğu anlamına gelir. Bu bağlamda, kolayca katılım sağlanan teknolojiden algılanan fayda da yüksektir. Öte yandan, iş sistemlerinin ve süreçlerinin karmaşıklığı, kullanıcıların teknolojiye katılmalarını engelleyecektir. Geçmiş çalışmalar, algılanan kullanım kolaylığının teknolojiye yönelik kullanım tutumunun önemli bir belirleyicisi olduğunu belirtmektedir (Davis, 1989, Gao ve Bai,2014). Algılanan fayda ise, bireyin iş performansını artırmak için yeni teknolojiden algıladığı katkı derecesini ifade eder. Eğer kullanıcılar yeni sistemlerinin faydalı olduğunu düşünürlerse, onları kullanma konusunda olumlu bir tutuma sahip olacaklardır. Yani teknolojinin kullanıcı ihtiyaçlarını karşılaması gerekir ki kullanıma yönelik tutum gösterebilsinler (Akça ve Özer, 2012, Zhao ve diğerleri, 2018).

Kullanışlılık kullanım tutumu üzerindeki kilit faktörlerden biridir. Bu nedenle, aşağıdaki hipotezler ileri sürülebilir.

H1: Algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif bir etkisi vardır.

H2: Algılanan kullanım kolaylığının kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.

H3: Algılanan faydanın kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.

YYT'den "**uygunluk**" inovasyonun, potansiyel kullanıcıların önceki deneyimleri ve ihtiyaçları ile tutarlı olarak algılanma derecesidir. Yüksek uyumluluk faydalı algılanmaya ve kabul edilmeye yol açacaktır. Bir teknolojinin yani yeniliğin, organizasyon ya da bireylerin değer ve ihtiyaçlarıyla uyuşma derecesi bu teknolojinin benimsenmesinde etkilidir. Her yenilik mevcut değer ve inançlarla uyumlu olmayabilir. Bu nedenle uygunluğu fazla olan bir teknoloji, potansiyel benimseyiciler için daha az belirsiz olmakta ve böylece hem fayda sağlayacağına olan inanç artmakta hem de kullanım tutumu isteğini artırmaktadır. Bu algı ile uygunluk derecesi yüksek olan yenilikler bireyler tarafından daha hızlı benimsenip, hızla yayılmaktadır (Kılıçer, 2008).

H4: Uygunluk algılanan fayda üzerinde pozitif etkiye sahiptir.

H5: Uygunluk kullanıma yönelik tutum üzerinde pozitif etkiye sahiptir.

Sistem kullanım tahminini iyileştirmek için ek değişkenlerle entegrasyona ihtiyaç duyulduğu pek çok çalışmada gösterilmiştir. Kullanıcıların mevcut hizmetler ile yeni teknolojiler arasında geçiş yaparken ihmal edilemeyecek **maliyet**lerle uğraşmaları gerektiği görülmüştür (Wu ve Wang, 2005, Chunxiang, 2014). Dönüşüm maliyeti Göğüş ve Özer'in çalışmasında (2014) iki ana kategori altında anlatılmıştır: Yordamsal ve Finansal maliyetler. Yordamsal maliyeti ekonomik risk maliyeti, değerlendirme maliyeti, öğrenme maliyeti ve kurulum maliyetinden oluşur. Ekonomik risk maliyeti, yeni teknoloji etkinliği hakkındaki belirsizliği içerir. Değerlendirme maliyeti, diğer alternatifleri değerlendirmek için gereken zamanı ve çabayı yansıtır. Kurulum maliyeti, yeni bir yapılandırma/uygulamanın maliyetini ifade eder. Öğrenme maliyeti, yeni teknolojinin nasıl kullanılacağını öğrenmek için gereken çabadır. Askeri alan içinde maliyetler, kalem

kalem tartışılan ve komutanların karar verirken çok detaylı analiz ettikleri konulardır. Yukarıda bahsi geçen bu maliyetlerin, IoT'nin askeri olarak kabul edilmesinde belirleyici bir etkiye sahip olduğu değerlendirilmektedir.

H6: Beklenen maliyetin kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.

İnternet uygulamalarının kullanım oranlarının artmasıyla insanlar, çevrimiçi faaliyetlere veya işlemlere girerken ortaya çıkan çeşitli **risk**ler konusunda endişelenmeye başlamıştır. Kullanıcılar ürün, hizmet kalitesi ve çevrimiçi hizmetler konusunda kararsız kaldıklarında, kullanımından endişe duyabilirler. 1960'lardan bu yana tüketicilerin karar vermedeki davranışlarını açıklamak için algılanan risk teorisi uygulanmıştır. Ancak çevrimiçi işlemlerden bu yana algılanan risk tanımı da değişmiştir. Geçmişte algılanan riskler öncelikle sahtekarlık, ürün ya da hizmet kalitesi olarak kabul edilirken günümüzde algılanan risk, finansal, ürün performansı, sosyal, psikolojik, fiziksel veya zaman riskleri gibi türleri de ifade eder. Bazı kullanıcılar olgunlaşmamış teknolojiden kaynaklanan potansiyel riskleri algılarlar. Diğerleri çevrimiçi işlemlere ve etkinliklere güvenmeden önce tereddüt ederler. Pavlou bunu "kullanıcının istenen bir sonucu elde etmede zarar görme konusundaki öznel beklentisi" olarak tanımlamaktadır (Wu ve Wang, 2005). Diğer araştırmalar da algılanan riskin, tüketicilerin çevrimiçi işlemlere karşı tutumlarının önemli bir belirleyicisi olduğunu göstermiştir (Kowatsch ve diğerleri, 2012). Askeri alan içinde literatür araştırması göz önüne alındığında, risk'in başlı başına bir çalışma konusu olabilecek kadar etkili bir kaygı ve çekince olduğu görülmektedir. Ortaya çıkabilecek riskler yalnızca şahıs ya da şirketleri değil, ülke güvenliğini de tehdit edebilecektir. Bu nedenle, aşağıdaki hipotez önerilmiştir.

H7: Algılanan riskin, kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.

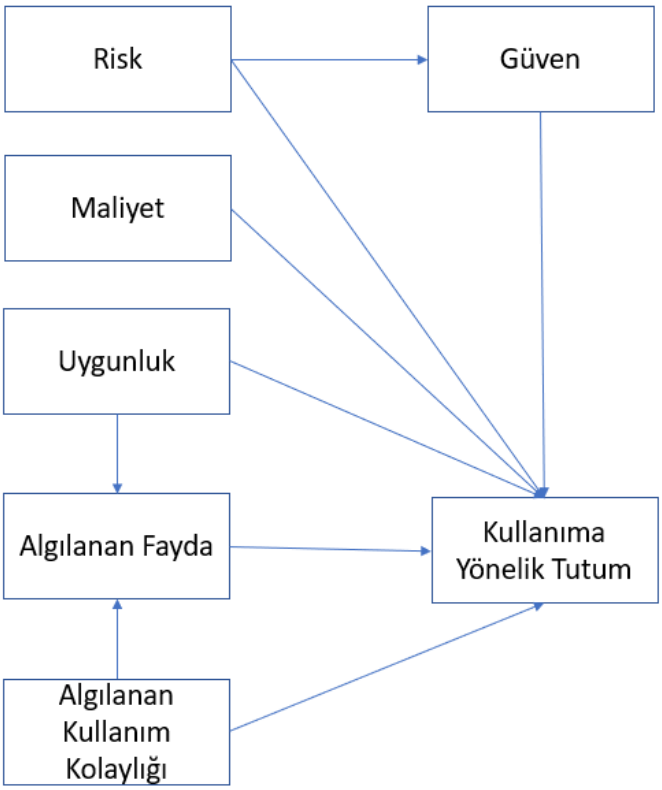
Son olarak "**Güven**" faktörü Chunxiang (2014) ile Zhao ve diğerlerinin (2018) çalışması baz alınarak eklenmiştir. IoT'deki cihazlar ve internet arasındaki bağlantının artması, güvenlik ve gizlilikle ilgili zorluklar ortaya koymaktadır. Hassas kişisel ve organizasyonel verilerin ihlali, kişi ya da kurumlara zarar vermek için kullanılabilir. Bu tüketicilerin IoT'ye olan güvenlerini etkileyip kullanma motivasyonlarını etkileyebilir. Neticede IoT'nin başarısı, tüketicinin IoT'deki güvenlik ve mahremiyet konusundaki

algılarına ve tüketicilerinin dijital güven düzeyine bağlıdır. Tüketici davranışını etkilemek için güven önemli bir unsur olduğundan, IoT'nin hem güvenliği hem de mahremiyeti konusundaki kullanıcı algıları arttıkça teşvik edilebilir (Khan ve diğerleri, 2018, Chunxiang, 2014). Son yıllarda güven birçok farklı alanda yaygın olarak incelenmiştir. Güvenin, ürün ve hizmetleri kullanmaya yönelik davranışlar üzerinde güçlü bir şekilde ilişkili olduğu görülmüştür (Zhao ve diğerleri, 2018). Bunun yanında mevcut birçok çalışma güveni etkileyen faktörler arasında **risk** faktörünü tek başına ya da gizlilik riski, güvenlik riski ya da performans riski gibi çeşitli başlıklar altında ele almıştır (Chunxiang, 2014). Her ne kadar güven faktörü, risk faktörünün tam zıttı olarak algılansa da model içerisinde her ikisinin de farklı algıları yakaladığına ve paralel olarak yer alabileceğine inanılmaktadır. Örneğin bir kişi IoT servis sağlayıcısına güvenebilir, ancak aynı zamanda elektronik olarak aktarılan kişisel ya da organizasyonel bilgilerle ilgili risklerin de farkında olabilir (Kowatsch ve diğerleri, 2012). Askeri alan için güvenlik, siber tehdit ve risk konularının son derece önemli olduğunu düşündüğümüzde, bu birbirine zıt iki faktörün hem birbirleriyle hem de kullanım tutumuyla olan ilişkisinin yer almasının gerekli olduğu değerlendirilmiştir.

H8: IoT cihazlarının askeri alanda kullanılmasına duyulan güvenin kullanıma yönelik tutum üzerinde olumlu yönde etkisi vardır.

H9: Algılanan riskin, güven üzerinde olumsuz etkisi vardır.

Şekil 3.1, bu çalışmanın araştırma modelini özetlemektedir.



Şekil 3.1. Araştırmanın Modeli

Modele dayalı varsayımlardan türetilen hipotezler aşağıda sıralanmıştır:

H1: Algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif bir etkisi vardır.

H2: Algılanan kullanım kolaylığının kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.

H3: Algılanan faydanın kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.

H4: Uygunluk algılanan fayda üzerinde pozitif etkiye sahiptir.

H5: Uygunluk kullanıma yönelik tutum üzerinde pozitif etkiye sahiptir.

H6: Beklenen maliyetin kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.

H7: Algılanan riskin, kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.

H8: IoT cihazlarının askeri alanda kullanılmasına duyulan güvenin kullanıma yönelik tutum üzerinde olumlu yönde etkisi vardır.

H9: Algılanan riskin, güven üzerinde olumsuz etkisi vardır.

3.3. ARAŞTIRMANIN YÖNTEMİ

Araştırmada, Askeri alanda IoT'nin kullanılabilirliğini, personelin kaygı ve beklentilerini, kullanımı etkileyen faktörleri ortaya koymak için anket yoluyla veri toplanması amaçlanmaktadır. Veri elde etmek için belirlenen katılımcı hedef kitlesi: orta seviye yönetici pozisyonunda bulunmuş ya da bulunmakta olan farklı ülkelerden (NATO ülkeleri ile sınırlı) asker ya da askeri alanda çalışan kişiler ve Türk Silahlı Kuvvetlerinde aktif görevde bulunmayan (emekli ya da sağlık gibi sebeplerle ayılmış) eski ordu mensupları olarak belirlenmiştir. Bu hedef kitle ile uluslararası bir bakış elde etmek hedeflenmiştir.

Anket üç bölümden oluşmaktadır:

- İlk kısımdaki veriler katılımcıların demografik özellikleri; cinsiyet, yaş, eğitim durumu, daha önce IoT kavramını duyup duymadığı ve kişisel olarak IoT kullanıp kullanmadığı bilgileri sorularak edinilmiştir.
- İkinci kısımda Tablo 3.1'de görülen anket ifadeleri yer almaktadır. Anket ifadeleri yazılırken, Davis (1986), Wu ve Wang (2005), Chunxiang'ın (2014) ve Weng ve arkadaşlarının (2018) çalışmalarında geçerliliği ve güvenilirliği test edilmiş sorular temel alınarak uyarlama yapılmıştır. İlgili çalışmalar başlangıçta IoT hizmetlerinin değerlendirilmesi için geliştirilmemiştir. Bu nedenle, yapıların ve anket maddelerinin tanımları mevcut çalışmada IoT bağlamında da geçerli olacak şekilde dikkatlice uyarlanmıştır. Sırasıyla; risk, maliyet, uygunluk, güven, algılanan fayda, kullanım kolaylığı ve kullanıma yönelik tutum faktörleri ile uyuşma düzeyleri ölçülmektedir. Katılımcılar, verilen ifadelere uyuşma düzeylerini 5'li likert ölçeği üzerinden (1=Kesinlikle katılmıyorum; 2=Katılmıyorum; 3=Kararsızım; 4= Katılıyorum; 5=Kesinlikle katılıyorum) değerlendirmektedir.
- Üçüncü ve son kısımda ise katılımcıların öneri ve çekincelerini belirtecekleri açık uçlu sorular yer almaktadır.

Anket'in Türkçesi EK 1, İngilizcesi EK 2'de yer almaktadır.

Tablo 3.1. Modelin Faktörleri

Faktör (Analizlerde yer alan kısaltmalar)	**İfade**
Risk (R)	Askeri operasyona yönelik olarak IoT kullanmanın potansiyel risk olduğunu düşünüyorum.
	Askeri lojistik alanda IoT kullanmanın potansiyel risk olduğunu düşünüyorum.
	Askeri eğitim alanında IoT kullanmanın potansiyel risk olduğunu düşünüyorum.
	IoT cihazlarının askeri ağlara erişiminin güvenlik açığı oluşturacağını düşünüyorum.
	Askeri alanda IoT kullanmanın gizliliği riske attığını düşünüyorum.
Maliyet (M)	Geleneksel askeri teçhizat bu teknoloji için yetersiz olacaktır.
	IoT için gerekli olan sensör vb. ekipmanın, büyük veri işleme altyapısı ve yazılımlarının maliyetli olduğunu düşünüyorum.
	IoT teknolojisine geçiş nedeniyle eski teçhizatların yenilenmesi süreci zaman (iş gücü) maliyeti getirecektir.
	Askeri IoT için ağ bağlantı işleminin yüksek maliyet getireceğini düşünüyorum.
Uygunluk (U)	IoT sistemlerini operasyona yönelik olarak kullanmak uygundur.
	IoT sistemlerini askeri lojistik alana yönelik olarak kullanmak uygundur.
	IoT sistemlerini askeri eğitim alanına yönelik olarak kullanmak uygundur.
	Geleneksel askeri teçhizatın çeşitli uyarlamalarla IoT için kullanılması mümkündür.
Güven (G)	Askeri alanda, IoT sistemler tarafından sağlanan servisler güvenilirdir.
	IoT donanımlarından sürekli veri almak mümkündür.
	IoT'nin sağladığı verilere güvenilerek operasyon planlanabilir.
	IoT verilerinden elde edilen sonuçlar karar süreçlerinde kullanılabilir.
Algılanan Fayda (AF)	IoT sistemler kullanmak askeri alanda (operasyon ya da lojistik) istenmeyen kayıpların azaltılmasını sağlar.
	IoT sistemleri, askeri operasyonlar üzerinde daha fazla kontrol sağlar.
	IoT sistemler kullanmak görevimin kritik yönlerini destekler.
	IoT sistemler görev performansımı artırır.
	Normalde mümkün olabileceğinden daha fazla iş yapmamı sağlar.
Kullanım Kolaylığı (KK)	Askeri alanda IoT sistemleri kullanmayı öğrenmek benim için kolaydır.
	IoT sistemiyle bütünleşmek çok fazla zihinsel çaba gerektirir.
	IoT sistemlerini askeri alanda kullanmada ehil olmak çok fazla çaba gerektirir.
	Genel anlamda, IoT sistemlerini askeri alanda kullanmayı kolay buluyorum.
Kullanıma Yönelik Tutum (T)	Genel anlamda askeri alanda IoT kullanmayı mantıklı buluyorum.
	Yükselen IoT, yüksek düzeyde bağlı bir çalışma ortamı olarak gelecekteki askeri savaş alanının Doktrin, Teknik, Taktik ve Prosedürlerini akıllıca değiştirecektir.
	IoT sistemlerini mücadele etkinliği ve koordineli karar verme gibi gerçek zamanlı veri ihtiyacı barındıran askeri alanda kullanmak bu alanın doğası için değerdir.

3.3.1. Ön Test

Anket uygulamasına geçilmeden önce hedef kitle örnekleminde 10 kişiye sosyal medya vasıtasıyla anket gönderilmiş ve bu kişilere;

- Çalışmanın maksadının anlaşılıp anlaşılmadığı,
- Anlaşılmayan soru ve anlaşılmayı güçleştiren ifadelerin yer alıp almadığı,
- Formun yapısı ve soru sırasında dikkatlerini çeken bir zorluk bulunup bulunmadığı sorulmuştur.

Ayrıca gerçek uygulamaya geçildiğinde, uygulayacak kişilerin ortalama ne kadar zamanlarını ayıracaklarını belirtmek için, ön test uygulayıcılarından ankete başlamadan önce zaman tutmaları istenmiştir.

Bu çerçevede ortalama 5-10 dakika içerisinde anketin doldurulduğu ortaya çıkmıştır. Katılımcıların tamamı tarafından çalışmanın maksadı anlaşılmış ve form yapısı kullanıcı dostu olarak görülmüştür. İfadeler içerisinde özellikle İngilizce olmasından kaynaklı gözden kaçan dilbilgisi ve kelime hataları düzeltilmiştir. Çalışmanın geçerliliği ve güvenilirliğini etkileyebilecek belirsizliklerden kaçınmak için yapılan ön test sonucunda ihtiyaç duyulan düzenlemeler yapılarak anket formu nihai haline getirilmiştir.

Ankete başlamadan önce yapılan bir başka işlem etik olarak uygulanmasına yönelik uygunluk onayının alınması olmuştur. Atatürk Üniversitesi Hukuku Müşavirliğine yazılan müsaade yazısı ve alınan onay yazısı Ek 3'te yer almaktadır.

3.3.2. Anketin Oluşturulması ve Veri Toplanması

Araştırma modelimizi doğrulamak, kişilerin IoT'nin askeri alanda kullanımında muhtemel gördükleri fayda ve tehditleri gözler önüne sermek maksadıyla çevrimiçi (online) bir anket yapılmıştır. Çevrimiçi anket fiziksel olarak dünyanın pek çok farklı yerinde bulunan geniş kitlelere erişebilmeyi mümkün kılmıştır. Atatürk Üniversitesi bünyesinde açık kaynak kodlu "LimeSurvey" (LimeSurvey) aracı ile geliştirilen bir platform üzerinden bahse konu anket hazırlanmıştır. LimeSurvey, MySQL, SQLite, PostgreSQL veya MSSQL veri tabanına dayalı, PHP dilinde yazılmış, ücretsiz ve açık kaynak kodlu çevrimiçi bir istatistiksel anket web uygulamasıdır. Web sunucusu tabanlı bir yazılım olarak, çevrimiçi anketler geliştirmek ve yayınlamak, yanıt toplamak,

istatistik oluşturmak, elde edilen verileri diğer uygulamalara aktarmak için bir web arayüzü sağlar. Ayrıca anket sonuçlarının temel istatistiksel ve grafik analizini sağlar. Anketler ya halka açık ya da sadece seçilmiş katılımcılara verilen "sadece bir kez" belirteçleri kullanılarak sıkı bir şekilde kontrol edilebilir. Ek olarak, katılımcılar isimsiz olabilir. LimeSurvey katılımcıların IP adreslerini izleyebilir. Üniversite yönetiminde oluşturulmuş kullanıcı dostu bu platform kullanılarak “edu” uzantılı bir web adresi ile katılımcılara sunulmuştur. Ankete katılan kişilere akademik çalışma maksatlı olarak anketin uygulandığı belirtilirken “edu” uzantılı bir adres göndermekte kuşkusuz katılım oranının artması anlamında faydalı olmuştur.

Çevrimiçi anket 22 Mart 2019 tarihinden itibaren İngilizce olarak erişime açılmıştır. Giriş sayfası Şekil 3.2’de yer almaktadır. Hedeflenen kitleye erişebilmek için kişisel sosyal medya hesaplarımdan (Facebook, Twitter, LinkedIn, Whatsapp ve e-posta) ankete katılım için davette bulunulmuştur. Ayrıca davette bulunulan kişilere (özellikle geniş bağlantı listeleri bulunan) aynı çerçevede bulunan kendi bağlantılarına da katılım için anketi iletmeleri rica edilmiştir.

Şekil 3.2. Anketin Giriş Sayfası

3.3.3. Araştırmanın Örneklem Büyüklüğü

Rastgele bir örneklemden genelleme yapmak ve örneklem hatalarından veya önyargılardan kaçınmak için, rastgele örneklemin yeterli büyüklükte olması gerekir. Literatürde sosyal araştırma ve bilgi sistemi araştırmalarında anket örneklem büyüklüğünün hesaplanmasıyla ilgili farklı çalışmalar görülmektedir. Bu çalışmada ana

kütleyi temsil edecek minimum örneklem büyüklüğü Bartlett ve diğerleri (2001) ve Taherdoost'in (2017) çalışmaları göz önüne alınarak aşağıdaki formül kullanılarak hesaplanmaktadır.

$$n = \frac{Z{\alpha_{/2}}^2}{E^2} p(1-p) \tag{3.1}$$

Formülde;

n, gerekli örneklem büyüklüğü,

p , n büyüklüğündeki rastgele bir örneklem kümesinde aranan gözlemlerin yüzdesi,

E, gerekli maksimum yüzde hata payı,

Z, gerekli güven seviyesine karşılık gelen değeri temsil eder.

Askeri alanda IoT'nin kullanımı araştırmasının uygulandığı ana kütlenin çeşitliliğinin göreceli olarak düşük olması ve ilgi/endişelerin askeri ortamda çok sapma göstermemesinden dolayı "Oran Varyansı" olarak da tanımlanan p yani, n büyüklüğündeki rastgele bir örneklem kümesinde aranan gözlemlerin oranının, %10 olarak tanımlanması yeterlidir. Çok sapma beklenilen ana kütleler için bu "Oran Varyansı" %50 olarak tanımlandığı zaman maksimum örneklem kümesine ulaşılmaktadır. Yönetim Bilimleri araştırmalarında kullanılan tipik güven seviyeleri %95 (0,05: 1,96'ya eşit bir Z değeri) veya %99'dur (0,01: Z = 2,57). %95'lik bir güven düzeyi, 100 örnekten 95'inin, belirtilen hata payı (E) dahilinde gerçek popülasyon değerine sahip olacağı anlamına gelir. Güven aralığının (α) %95, kabul edilebilir hata payının (E) %5 olduğunu kabul edildiğinde, söz konusu ana kütleyi temsil edecek minimum örneklem büyüklüğü aşağıdaki şekilde hesaplanabilir.

$$n = \frac{1{,}96^2}{0{,}05^2}(0{,}10)(1-0{,}10) \cong 138$$

3.3.4. Araştırmanın Sınırlılıkları

Bu çalışma katılımcıların konuya ilgisizliği, askeri alanın gizliliği sebebiyle çekinceleri ve anketin İngilizce olması gibi sebeplerle 145 kişiyle sınırlı kalmıştır. Demografik analizlerde yer alan sonuçlar göz önüne alındığında örneklem büyüklüğünün

oldukça eğitimli bir kitleden oluştuğu görülebilir. Bu husus da çalışmanın bir diğer sınırlılığıdır.

3.4. BULGULAR

Anket 242 kişiye ulaşmıştır. 97 kişinin konuya ilgisizlik, askeri alanın gizliliği gibi çekinceler ve anketin İngilizce olması gibi sebeplerle anketi yarıda bıraktığı değerlendirilmektedir. Anket 145 kişi tarafından tamamlanmıştır.

3.4.1. Demografik Analizler

Katılımcıların demografik bilgileri Tablo 3.2 ve Tablo 3.3'te gösterilmiştir.

Katılımcıların;

- %14,5'inin kadın, %85,5'inin erkektir.
- %40,7'sinin 34-39 yaşları arasındadır.
- %46,2'sinin ise yüksek lisans derecesi vardır.

Tablo 3.2. Demografik Bilgiler

Faktörler	Katılımcı Sayısı	Oranı (%)
Cinsiyet		
Kadın	21	14,5
Erkek	124	85,5
Yaş		
20-27	4	2,8
28-33	21	14,5
34-39	59	40,7
40-46	41	28,3
46 ve üstü	20	13,8
Eğitim Durumu		
Ön lisans	2	1,4
Lisans	48	33,1
Yüksek Lisans	67	46,2
Doktora	25	17,2
Diğer	3	2,1

Tablo 3.3. IoT'ye İlişkin Demografik Bilgiler

Faktörler	Katılımcı Sayısı	Oranı
Daha önce IoT kavramını duydunuz mu?		
Evet	106	73,1
Hayır	39	26,9
Kişisel olarak IoT kullanımınız var mı?		
Evet	73	50,3
Hayır	72	49,7

Katılımcıların %73,1'inin IoT kavramını daha önce duyduğu ancak katılımcıların yarıya yakınının kişisel olarak IoT kullanım deneyimi bulunmadığı görülmektedir.

3.4.2. Öneri ve Çekincelerin Analizi

Ankette demografik özellikleri sorgulayan sorular ile model ve hipotezlerin testi için yer alan anket ifadelerinin yanında iki tane de açık uçlu soru yer almaktadır. Anketin bu kısmının doldurulması anketin tamamlanması için zorunlu tutulmamıştır.

Bu sorular ölçekli anket sorularından bağımsız kişilerin konuya özgü görüş, öneri ve çekincelerini almayı hedeflemektedir. Aşağıda bu cevaplar ana başlıklar halinde değerlendirilmiştir.

1-Askeri alanda IoT kullanımına yönelik önerileriniz nelerdir? Bireysel ya da organizasyonel olarak ne gibi alanlarda kullanılabileceğini değerlendiriyorsunuz?

Anketi tam olarak tamamlayan 145 kişiden 75'i bu soruya cevap vermiştir. Cevaplar genel anlamda 3 grup anlayışı ortaya koymaktadır. Güvenlik çekinceleri sebebiyle askeri alanda IoT kullanımına tamamen karşı görüşte bulunan ilk grubun katılımcıların çok küçük (3-4 görüş) bir oranını oluşturduğunu söyleyebiliriz. Bu grup güvenlik ve gizlilik üzerine akreditasyonun eksiksiz sağlandığı zaman kullanım alanlarının düşünülebileceği düşüncesini savunmuşlardır. Bu teknolojinin askeri alanda kullanılmadan önce akıllı ev, şehir, ulaşım ve sağlık gibi sivil alanlarda kendini tam olarak kanıtlaması gerektiğini belirtmişlerdir.

İlk gruptan daha büyük olan diğer bir grup (10-15 görüş) ise bu teknolojiye daha ılımlı yaklaşmaktadır. Bu grup, IoT'nin basitten daha karmaşık alana ya da başka bir ifadeyle askeri alan içinde daha az riskli alanlardan daha çok riskli alanlaraa doğru adapte olması gerektiği anlayışındadır. Önce eğitim ve lojistik daha sonra ise harekât alanına geçiş olabileceği örnekleri verilmiştir. Geçişler esnasında alınılan derslerle gerekli düzenlemeleri yaparak bir sonraki adaptasyonu sağlamanın büyük fayda sağlayacağını değerlendirmişlerdir.

Son olarak ve çoğunluktaki grup ise her ne kadar çekinceler olsa da IoT'nin asker tğm alanlarda kullanılmasının gerekli hatta kaçınılmaz olduğunu savunmuştur. Askeri operasyonlarda IoT sistemlerinin kullanımıyla ilgili kaygılar olabileceği, ancak teknolojik gelişmelerin arkasında kalmak ve sistemleri yenilememenin, başarısızlığı kaçınılmaz kılacağını değerlendirmişlerdir.

Gerçeklik, basitlik, güvenilirlik, erişilebilirlik, birlikte çalışabilirlik, sağlamlık ve atiklik IoT'de olması gereken özellikler olarak aktarılmıştır. Zorlu savaş koşulları altında tüm sistemin hataya dayanıklı olması, taktiksel savaş alanında pek çok farklı senaryoya ayak uydurabilmesi gerekmektedir. Kullanıma yönelik öneriler aşağıdaki başlıklarda sıralanabilir:

- Harekât (Operasyon): İstihbarat toplama, gözetim, keşif, komuta ve haberleşme komuta kontrol kullanım örnekleri genel anlamda C4ISR'ı ifade etmektedir. Durumsal farkındalık oluşturulması, İHA- operasyon merkezi haberleşmesi verilen diğer örneklerdendir.
- Karar destek: Komutanlar yoğun zihinsel çaba ile aşırı zaman baskısı altında çalışmaktadırlar. Bu nedenle bazen yanlış karar verebilirler. IoT'nin devreye girmesi ile karar vericiye sunulan hareket tarzlarının büyük bir kısmı gerçek zamanlı, büyük veri ile muhabere resminin net bir şekilde gösterildiği, karar hızı ve kolaylığının daha da arttığı durumlar ile daha iyi (verimli), zamanında yönetim sağlanabileceğini, komutanlara çözüm önerileri sunabileceğini, yani özetle karar destek unsuru olarak algılanabileceği söylenebilir. IoT'yi askeri alanda kullanmak, yanlış kararların oranını azaltacaktır.

- Eğitim: Öğretmen, öğrenci ve sınıf iletişimini farklı boyutlara taşınabileceği belirtilmiştir. Akademik eğitimin yanında temel intibak eğitimleri ve uçuş eğitimlerine hızlı bir şekilde entegre edilebilir.
- Güvenlik: Güvenlik sensörlerini (kameralar vb.) otomatize ederek insan algılama ve tanıma sistemlerinin kullanımı, ülke genelinde sınırların bu teknoloji ile donatılması, hava kontrolü IoT'nin fayda sağlayabileceği değerlendirilen alanlardandır.
- Lojistik: IoT sistemlerinin, mühimmat ve destek malzemelerinin akışını kolaylaştırmak, stok seviyesi izlemek için kullanılabileceği ve savaş ritminin bu sensörler yardımıyla hesaplanabileceği belirtilmiştir. İlk aşamada kullanılması önerilen alanlardandır.
- Giyilebilir cihazlar ile donatılmış askerlerin (güvenlik personeli ve özel kuvvetler için bir zorunluluk) aşağıdaki bireysel ya da birlik durumları hakkında anlamlı bilgiler sağlayabileceği ifade edilmektedir.
    - Personel sağlığı: Askerin kalp atışı, konumu ve vücut ısısı gibi veriler,
    - Alan bilgisi: Birliğin yönü, hızı, çevrenin nemi, sıcaklığı verileri ile elde edilebilen bilgiler ihtiyaç duyulan merkezlerle de iletişim halinde olabilecektir.
- Kentsel operasyonlar: Kentsel operasyonlar alanında çok etkili ve kontrollü bir şekilde kullanılabileceği değerlendirilmektedir.

2- Askeri alanda IoT kullanımına yönelik en büyük çekinceniz nedir?

Anketi tam olarak tamamlayan 145 kişiden 84'ü bu soruyu cevaplamıştır. Cevapların neredeyse tamamına yakınında IoT'ye yönelik çekincelerin öncelikle gizlilik, güvenlik ve siber tehditler üzerine olduğu söylenebilir. Aşağıda belirtilen çekince ve görüşler temel maddeler halinde sıralanmıştır:

- Güvenlik: Sistemin siber saldırılara ya da her türlü güvenlik ihlallerine karşı kırılganlığı endişelerin neredeyse tamamında ve ilk sırada yer alan risk olarak görülmektedir. Veri akışının sürekliliği ve bilgi güvenliği askeri alanda en önemli hususlardan biridir. İnternet ortamı manipülasyon çabalarına açıktır. Verinin karşı taraf (düşman kuvvetler) tarafından ele geçirilmesi, kendi lehlerine kullanılması, verinin değiştirilerek bütünlüğünün bozulması endişe veren hususlardandır.

Kullanıcıların mobil cihazlarını kullanırken bile gizlilik kaygıları taşıdığı bir dönemde gerekli önlemlerin alınması şarttır. Ancak hali hazırda askeri alanda IoT kullanıcısı olan kişilerin bu konu hakkında bir girdisi de güvenlik önlemleri nedeniyle bazen bilgisayarları açmanın bile 5-10 dakika sürmesidir. Bu nedenle askeriyede IoT kullanımı çok güvenlik açısından hassas bir konudur. Bu kusurların üstesinden gelmek için, 'tasarım gereği güvenlik' kavramının göz önüne alınması gerekmektedir.

- Eğitim: IoT çok iyi planlama ve eğitimli insanlar gerektirir. Nitelikli ve donanımlı personel IoT döngüsünün içinde olmalıdır ve IoT teknolojisinin görev başarısında etkili olacaktır. Takım çalışması olmazsa olmaz olarak görülmektedir. Yeterli donanıma sahip olmayan ve bu sisteme dahil olmayan her asker (hem bilgelik hem de araçlar anlamında) ve teçhizat, sistemin bütünlüğü ve güvenilirliği için tehlike oluşturacaktır.
- Büyük veri ile baş etme: IoT ile insanlı ya da insansız kara, hava, deniz araçları, akıllı seyir füzeleri, askerlerin giyeceği akıllı iskelet sistemleri gibi pek çok sistemden veri yağacağı göz önüne alındığında; bu veriyi normal klasik sistemlerle, insan emeğiyle işlemek, analiz etmek, karar vericiye destek verecek nitelikli bilgiyi sunmak çok emek ve zaman gerektirecektir. Bu sistemler tarafından tüketilen bant genişliği miktarı oldukça fazla olacaktır ki bu durum aşırı yüke sebep olabilir.
- Hata toleransı: Endişelerden biri de gerekli verilere (sensörlere vb.) savaş zamanında çeşitli sebeplerden ulaşılamama durumudur. Sistemi tam olarak kurtarma yeteneğine sahip olmadan, geleneksel ekipman IoT ile çalışacak şekilde tamamen değiştirilirse veri anlamında her şeyi kaybetme riski ile karşı karşıya kalınacaktır. Bu nedenle, IoT sistemi arızalandığında veya sisteme ulaşılamaması durumunda alternatifi var mı sorusu öncelikli çekincelerdendir.
- Maliyet: Bu sistemlere geçişin ekonomik olarak çok maliyetli olacağı gerçekliktir. Ancak iyi tasarlanan ve hesaplanan sistemeler uzun vadede daha ekonomik bile olabilir.
- Geçiş süreci: İyi bir planlama, eğitim ve yönetim olmadıkça geçiş sihirli bir değnekle yapılamayacaktır. Bu süreç stratejik, operatif ve taktik anlamda planlama ve yönetim gerektirir.

3- Öne çıkan teknolojiler

Verilen öneri ve çekinceler incelendiğinde değerlendirilmesi teklif edilen bazı teknolojilere de kısaca yer verilecektir.

- Kenar Bilişim (Edge Computing): Kenar merkezli IoT mimarisi dört ana grubu içerir: bulut, IoT uç cihazları, uç ve kullanıcılar. Mimarinin tasarımı, her bir tarafın hem mevcut kaynaklarını hem de spesifik özelliklerini dikkate alır. Kullanıcılar, yaşamlarını daha kolay hale getirmek için akıllı IoT uygulamalarını kullanırken, IoT uç cihazlarıyla doğrudan etkileşimde bulunmak yerine, bulut veya kenar tarafından sağlanan etkileşimli arabirimler aracılığıyla IoT uç cihazlarıyla iletişim kurarlar. IoT uç cihazları fiziksel dünyaya gömülüdür. Fiziksel dünyayı algılarlar ve fiziksel dünyayı kontrol etmek için harekete geçerler, ancak hesaplama ağırlıklı görevlerde karmaşık değildirler. Bulutun neredeyse sınırsız kaynakları var, ancak genellikle fiziksel olarak aygıtlardan uzakta konumlandırılmaktadırlar. Bu nedenle, bulut merkezli bir IoT sistemi genellikle sistemin gerçek zamanlı gereksinimleri olduğunda verimli bir şekilde görevi gerçekleştiremez (Sha ve diğerleri, 2019). Kenar bilişimin göz önüne alındığı güvenlik ve gerçek zamanlı ihtiyaçları koordine eden bir mimari, askeri uygulamalar için gerçeklik haline gelebilir.
- Yapay Zekâ: Algoritma, bilgisayar gücü ve büyük veri ile beraber yapay zekâ, derin öğrenmeden, bilgisayarla görmeye, konuşma tanımaya, doğal dil işlemeye, satranç oyunundan robotik işlemlere kadar geniş bir yelpazede önemli atılımların parçası oldu. Bu gelişmelerden yararlanarak, akıllı kişisel asistanlar, kişiselleştirilmiş alışveriş önerileri, video gözetimi ve akıllı ev aletleriyle örneklendiği gibi bir dizi akıllı uygulama hızlıca yükseldi ve büyük bir popülerlik kazandı. Bu akıllı uygulamaların insanların yaşam tarzlarını önemli ölçüde zenginleştirdiği, insan verimliliğini artırdığı ve sosyal verimliliği artırdığı yaygın olarak kabul edilmektedir (Zhou ve diğerleri, 2019). Bu gelişmeler akıllı cihazların parçası olduğu bir ordu için önerildiği gibi kaçınılmazdır.
- Şifreleme: Güvenlik anlamında uygulama katmanı ile etkileşim halinde olan son kullanıcı personel tarafından ilk akla gelen ama aslında güvenliğin sadece bir parçası şifrelemedir. Sensör verilerinin bütünlüğü ve orijinalliği çok önemlidir. Ele alınan mimariye bağlı olarak farklı katmalarda farklı güvenlik ihtiyaçları

bulunmaktadır. Örneğin uygulama katmanı için heterojen ağlar arasında kimlik doğrulama, kullanıcının gizliliğini korumak için eğitim ve yönetim bilgi güvenliği, özellikle de şifre yönetimi ön plana çıkmaktadır. Destek katmanı, bulut bilişim ve güvenli çok partili hesaplama gibi birçok uygulama güvenliği mimarisine ihtiyaç duyar. Güçlü şifreleme algoritması, şifreleme protokolü, güçlü sistem güvenliği teknolojisi ve anti-virüs gereklidir. Ağ katmanında kimlik doğrulaması, hizmetin kesilmesine karşı önlemler (anti-DDoS), şifreleme ve iletişim güvenliği kurulmasına ihtiyaç vardır. Algılama katmanında önce düğüm kimlik doğrulaması, yasadışı düğüm erişimini önlemek için gereklidir. Düğümler arasında bilgi iletiminin gizliliğini korumak için veri şifreleme mutlak gerekliliktir. Daha güçlü güvenlik önlemleri, daha fazla kaynak tüketimi anlamına gelir ve tasarımlar bu husus da göz önüne alınarak yapılmalıdır (Suo ve diğerleri, 2012).

3.4.3. Betimsel Analizler

Çalışmada, test edilen gözlenen değişkenlere ait betimsel istatistikler Tablo 3.4'de verilmiştir. Yapılan analizler için gözlemlenen değişkenlerin normallik dağılımlarını ortaya çıkarmak ve içeriğin daha iyi anlaşılması için dağılım yapısının anlaşılmasını önemlidir.

Tablo 3.4'te yer alan ortalamaları incelediğimizde;

- Algılanan fayda için ortalama değer katılımcıların teknolojinin alanda kullanımının fayda sağladığına katıldığı yönündedir.
- Uygunluk ölçeklerine verilen ortalama cevaplar da algılanan faydada görüldüğü gibi katılımcıların ifadeye katıldığı hatta kesinlikle katıldığı kısmına yakındır.
- Risk ifadelerine verilen cevaplar değerlendirilirken ters ifadelerin dönüşümü yapıldığında ortalama puan göstermektedir ki ankete katılanların risk faktörü ifadelerinde risk olduğuna katıldığı ya da kararsız olduğunu belirtmişlerdir.
- Kullanım kolaylığı için ortalama değerlere bakıldığında katılımcıların kararsız olduğu ön plana çıkmaktadır.

- Maliyet ifadelerinin ters ifadeler olduğu ve dönüşüm yapıldığı göz önüne alındığında ortalama değerde, katılımcıların maliyet getireceğine katılma yönüne yakın olduğu görülmektedir.
- Güven için ortalama değerler kararsızlıklar ile beraber katılıyorum yönündedir.
- Kullanıma yönelik tutum faktörü ortalamaları ise açıkça kullanıma yönelik tutum sergilediklerini göstermektedir.
- Askeri operasyon, lojistik ve eğitim alanlarında ayrı değerlendirmeye alınan ifadeler incelendiğinde uygunluk (U1, U2 ve U3) anlamında her üç alan için göze çarpan ciddi bir ayrım olmadığı görülebilir. Ancak risk bazında ele alındığında (R1, R2 ve R3) IoT kullanımı, eğitimden, lojistiğe ve operasyona doğru artarak risk kaygılarını göstermektedir.

Tablo 3.4. Ölçeklere İlişkin Betimsel İstatistikler

Ölçek İfadeleri	Ortalama	Standart Sapma	Çarpıklık	Basıklık
AF1	2,39	0,827	0,571	0,487
AF2	2,17	0,915	0,641	-0,021
AF3	2,32	0,841	0,606	0,198
AF4	2,05	0,793	0,844	1,214
AF5	2,25	0,87	0,647	0,18
U1	2,08	0,943	0,803	0,332
U2	1,78	0,893	1,34	1,889
U3	1,85	0,836	1,233	2,213
U4	2,22	0,909	0,841	0,754
R1	3,35	1,077	-0,201	-0,929
R2	3,01	1,077	-0,014	-1,002
R3	2,59	1,058	0,359	-0,798
R4	3,46	1,099	-0,459	-0,549
R5	3,36	1,084	-0,325	-0,764
KK1	2,28	0,795	0,641	0,587
KK2	3,26	1,007	0,032	-0,907
KK3	3,09	1,034	0,239	-1,071
KK4	2,48	0,791	0,379	-0,362
M1	3,57	0,873	-0,426	-0,243
M2	3,54	1	-0,275	-1,01
M3	3,87	0,766	-1,088	1,852
M4	3,39	1,069	-0,253	-0,98
G1	2,59	0,83	0,756	0,592
G2	2,13	0,637	0,535	0,998
G3	2,55	0,971	0,544	-0,313
G4	2,02	0,777	0,955	1,654
T1	2,03	0,833	1,118	1,893
T2	1,75	0,829	1,308	2,017
T3	2,01	0,882	0,774	0,669

Tablo 3.4'de incelenecek diğer değerler ise çarpıklık ve basıklık değerleridir. Görüldüğü üzere çarpıklık değerleri -1,088 ile 1,34 arasında, basıklık değerleri ise -1,071 ile 2,213 arasında değişim göstermektedir. Çarpıklık ve basıklık değerleri göz önüne alındığında ölçeklere ilişkin veri setinin normal dağılım özelliği gösterdiği söylenebilir. Çarpıklık değerinin 2'nin altında, basıklık değerinin de 7'nin altında olması literatürde istenen sınırlardan biridir (Ursavaş ve diğerleri, 2014, Kalyoncuoğlu, 2018).

3.4.4. Güvenilirlik ve Geçerlilik

Anket oluşturulurken her ne kadar daha önceki çalışmalarda test edilmiş ve doğrulanmış ifadeler alana uyarlanarak kullanılmış olsa da faktörleri ölçen bu ifadelerin geçerliliği ve güvenilirliği test edilmelidir. İç tutarlılık güvenilirliği, tek tek ölçüm öğelerinin aynı bilgi kaynağındaki dengesini yansıtır. Cronbach-Alfa, çok maddeli ölçümlerle araştırmalarda en önemli ve yaygın istatistiklerden biri olarak tanımlanmıştır. Cronbach-Alfa, tutumları ve diğer duygusal yapıları ölçmeye yönelik ölçeklerin geliştirilmesinde yaygın olarak kullanılmaktadır.

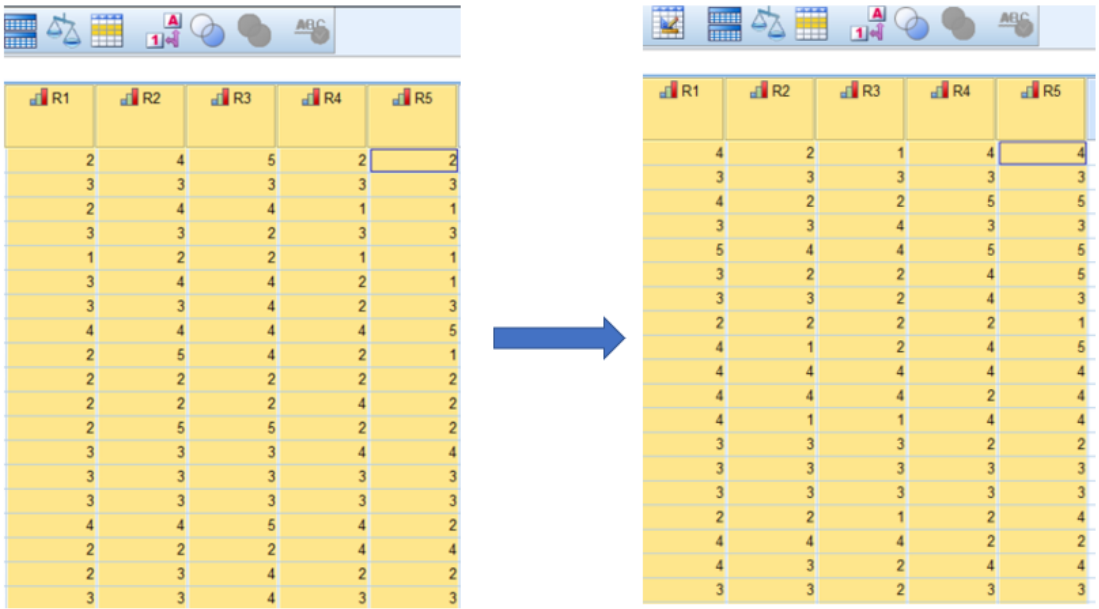
Hesaplanan Cronbach-Alfa değerlerini yorumlamak için yazarlar tarafından çok çeşitli tanımlayıcılar kullanılmıştır. Literatürde Cronbach-Alfa değerleri için; 0,93-0,94 mükemmel, 0,91-0,93 güçlü, 0,84-0,90 güvenilir, 0,81 sağlam, 0,76-0,95 oldukça yüksek, 0,73-0,95 yüksek, 0,71-0,91 iyi, 0,70-0,77 göreceli olarak yüksek, 0,68 biraz düşük, 0,67-0,87 makul, 0,64-0,85 yeterli, 0,61-0,65 orta, 0,58-0,97 yeterli, 0,45-0,98 kabul edilebilir, 0,45-0,96 yeterli, 0,4-0,55 tatmin edici değil ve 0,11 düşük olarak geniş bir sınıflandırma yapılmıştır. Bu sınıflandırma, Cronbach-Alfa hesaplanırken elde edilen değerleri tanımlamak için kullanılacak en uygun etiketler konusunda net bir fikir birliği olmadığını ayrıca farklı bilim insanları arasında kullanılan terimler arasında (örneğin, oldukça yüksek; yeterince yüksek; yeterli ve kabul edilebilir şekilde yeterli düzeyde örtüşmemektedir) net bir hiyerarşi olmadığını göstermekle birlikte (Taber, 2017), Cronbach-Alfa değeri için genel kabul gören en düşük alt seviye Robinson, Shaver ve Wrightsman'a (1991) göre 0,70 iken, Hair ve diğerleri (2008) bu değerin 0,60 olarak da alınabileceğini ifade etmiştir (Ursavaş ve diğerleri, 2014).

Cronbach-Alfa her biri aynı yapıyı yansıtan maddelerden oluşan bir testin iç tutarlılığını ölçer. Bu çalışmada her bir faktördeki maddeler aynı yapıyı yansıtan bir grup

olarak kabul edilmiştir. Bu nedenle, her madde kümesi için Cronbach-Alfa katsayısı bulunmuştur. Her bir ifadenin ayrı ayrı silinmesi durumunda faktörün Cronbach-Alfa değerinde meydana getirdiği değişiklik, Tablo 3.5'te "İfade Silinirse Cronbach-Alfa" başlığı altında yer almaktadır.

Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği testi ve Barlett küresellik testi faktör analizinden önce verinin faktör analizine uygunluğunu tespit etmek için yapılan diğer testlerdir. Özellikle KMO endeksi, değişken oranlı vakalar 1: 5'ten küçük olduğunda önerilir. KMO endeksi 0 ile 1 arasında değişmektedir, 0,50 ve üstü faktör analizi için yeterli olarak kabul edilmiştir. Bartlett'in küresellik testinde verilerin çok değişkenli normal dağılımdan geldiğini yani faktör analizine uygun olduğunu teyit etmek için p-değeri anlamlı olmalıdır (p <0,05) (Williams ve diğerleri, 2010).

Cronbach-Alfa, KMO ve Barlett küresellik testi için SPSS (sürüm 24) programı kullanılmıştır. Atatürk Üniversitesi anket sistemine girdi olan veriler, yine aynı sistemden SPSS dosyası olarak çıkartılmıştır. SPSS'te açılan dosyada öncelikle olumsuz önerme içeren (ters) ifadelerin likert değerleri dönüşümü yapılmıştır (Transform - recode into same variables). Risk ve Maliyet altındaki tüm ifadeler ve Kullanım Kolaylığı altında ise KK2 VE KK3 değişiklik yapılan ifadeler olup Şekil 3.3'te örneği gösterilmiştir.



R1	R2	R3	R4	R5
2	4	5	2	2
3	3	3	3	3
2	4	4	1	1
3	3	2	3	3
1	2	2	1	1
3	4	4	2	1
3	3	4	2	3
4	4	4	4	5
2	5	4	2	1
2	2	2	2	2
2	2	2	4	2
2	5	5	2	2
3	3	3	4	4
3	3	3	3	3
3	3	3	3	3
4	4	5	4	2
2	2	2	4	4
2	3	4	2	2
3	3	4	3	3

R1	R2	R3	R4	R5
4	2	1	4	4
3	3	3	3	3
4	2	2	5	5
3	3	4	3	3
5	4	4	5	5
3	2	2	4	5
3	3	2	4	3
2	2	2	2	1
4	1	2	4	5
4	4	4	4	4
4	4	4	2	4
4	1	1	4	4
3	3	3	2	2
3	3	3	3	3
3	3	3	3	3
2	2	1	2	4
4	4	4	2	2
4	3	2	4	4
3	3	2	3	3

Şekil 3.3. Ters İfadelerin Dönüşümü

Verilerin faktörler bazında güvenilirlik ve yeterlilik testleri sonuçları Tablo 3.5'de incelendiğinde 'Algılanan Fayda' için Cronbach-Alfa değeri 0,809 olarak bulunmuştur. 0,7'nin üzerinde olan bu değer güvenilir kabul edilir. AF1 ifadesinin silinmesi genel Alfa değerinde iyileşme sağlamaktadır. Ancak değer yeterli olduğundan faktör analizinde bir sorun oluşturması durumunda değerlendirilmesi daha uygun olacaktır.

Tablo 3.5. Algılanan Fayda Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alfa	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
AF1	0,809	0,818	0,803	245,838	10	.000
AF2		0,772				
AF3		0,742				
AF4		0,735				
AF5		0,786				

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,803 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.6'ya bakıldığında 'Uygunluk' için Cronbach-Alfa değeri 0,834 olarak bulunmuştur. 0,7'nin üzerinde olan bu değer güvenilir kabul edilir. U4 ifadesinin silinmesi genel Alfa değerinde iyileşme sağlamaktadır. Ancak değer yeterli olduğundan faktör analizinde bir sorun oluşturması durumunda değerlendirilmesi daha uygun olacaktır.

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,733 ile 0,5 yeterlilik değerinin üzerindedir P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.6. Uygunluk Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
U1	0,834	0,754	0,733	259,732	6	.000
U2		0,748				
U3		0,789				
U4		0,859				

Tablo 3.7'ye bakıldığında 'Risk' için Cronbach-Alfa değeri 0,849 olarak bulunmuştur. 0,7'nin üzerinde olan bu değer güvenilir kabul edilir.

Tablo 3.7. Risk Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
R1	0,849	0,791	0,743	365,406	10	.000
R2		0,803				
R3		0,848				
R4		0,823				
R5		0,82				

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,743 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.8'e bakıldığında 'Kullanım Kolaylığı' için Cronbach-Alfa değeri 0,757 olarak bulunmuştur. 0,7'nin üzerinde olan bu değer güvenilir kabul edilir.

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,599 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.8. Kullanım Kolaylığı Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
KK1	0,757	0,749	0,599	183,990	6	.000
KK2		0,729				
KK3		0,657				
KK4		0,658				

Tablo 3.9'a bakıldığında 'Maliyet' için Cronbach-Alfa değeri 0,699 olarak bulunmuştur. 0,7'nin tam olarak alt sınırında olan bu değer güvenilir kabul edilebilir. M1 ifadesinin silinmesi genel Alfa değerinde iyileşme sağlamaktadır. Ancak değer yeterli olduğundan faktör analizinde bir sorun oluşturması durumunda değerlendirilmesi daha uygun olacaktır.

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,693 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.9. Maliyet Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
M1	0,699	0,755	0,693	123,873	6	.000
M2		0,516				
M3		0,641				
M4		0,578				

Tablo 3.10'a bakıldığında 'Güven' için Cronbach-Alfa değeri 0,749 olarak bulunmuştur. 0,7'nin üzerinde olan bu değer güvenilir kabul edilir. G2 ifadesinin silinmesi genel Alfa değerinde iyileşme sağlamaktadır. Ancak değer yeterli olduğundan faktör analizinde bir sorun oluşturması durumunda değerlendirilmesi daha uygun olacaktır.

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,745 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında olduğundan Bartlett'in küresellik testi anlamlı sonuçlar vermektedir.

Tablo 3.10. Güven Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
G1	0,749	0,689	0,745	136,901	6	.000
G2		0,763				
G3		0,639				
G4		0,644				

Tablo 3.11'e bakıldığında 'Tutum' için Cronbach-Alfa değeri 0,764 olarak bulunmuştur. 0,7'ninüzerinde olan bu değer güvenilir kabul edilir. T2 ifadesinin silinmesi genel Alfa değerinde iyileşme sağlamaktadır. Ancak değer yeterli olduğundan faktör analizinde bir sorun oluşturması durumunda değerlendirilmesi daha uygun olacaktır.

Örneklem büyüklüğü yeterliliği için yapılan KMO testi sonucu değer 0,647 ile 0,5 yeterlilik değerinin üzerindedir. P-değeri 0,05'in altında anlamlı sonuçlar vermektedir.

Tablo 3.11. Kullanıma Yönelik Tutum Güvenilirlik ve Yeterlilik Testleri Sonuçları

İfade	Cronbach Alpha	İfade Silinirse Cronbach-Alfa	KMO Değeri	Bartlett's Testi		
				Yaklaşık Ki-Kare Değeri	sd	p-değeri
T1	0,764	0,574	0,647	123,303	3	.000
T2		0,795				
T3		0,66				

Güvenilirlik testlerinden sonra ölçeğin yapı geçerliliği testi için Faktör Analizine ihtiyaç duyulmaktadır. Faktör analizi, birbiriyle ilişkili değişkenleri bir araya getirmeyi, anlamlı değişkenler bulmayı amaçlayan çok değişkenli bir istatistiktir. Diğer analizlerde kullanılacak olan değişkenleri çok sayıda değişken arasından çıkarmayı sağlar (Hair ve diğerleri, 2008). Faktör yük değeri (katsayısı) ifadenin faktörle ilişkisini açıklamaya yarayan değerdir. Bu değerin yüksek olması beklenir. Bir ifadenin faktör yükünün 0,3'ün altında olması kabul edilemeyeceğinin ifadesidir. Genel kabul olarak; 0,60 ve üstü katsayısı yüksek, 0,30-0,59 arası ise orta düzeyde kabul edilir ve ifadenin çıkartılmasında dikkate alınır (Büyüköztürk, 2002).

Açıklayıcı Faktör Analizi (AFA), anket maddelerine verilen yanıtların oluşturduğu değişkenler arasındaki içsel ilişkileri analiz ederek faktör olarak adlandırılan ortak değişken gruplarının ortaya çıkarılmasını sağlayan en yaygın tekniklerden biridir. AFA için örneklem sayısının madde başına en az 5 olması gerektiği belirtilmektedir. Çalışmada yer alan 29 ifade göz önüne alındığında 145 kişilik katılımın gerekli olduğu ve sağlandığı görülmektedir (Ursavaş ve diğerleri, 2014). Tablo 3.12 ifadelerin AFA sonuçlarını ortaya koymaktadır. Faktör Yük değerleri 0,304-0,91 aralığında değerler almıştır. Orta düzeyin üzerinde, genel kabul olarak görülen 0,6'nın hemen altında bir değer olan 0,5 daha sonra yapılacak olan Doğrulayıcı Faktör Analizi (DFA) de göz önüne alınarak sınır kabul edilmiştir.

Tablo 3.12. İfadelerin Açıklayıcı Faktör Analizi Sonuçları

	1	2	3	4	5	6	7	Toplam varyansı açıklama oranı
AF1	0,448							%48,302
AF2	0,666							
AF3	0,805							
AF4	0,858							
AF5	0,621							
U1		0,800						%57,931
U2		0,910						
U3		0,769						
U4		0,509						
R1			0,865					%53,727
R2			0,786					
R3			0,600					
R4			0,694					
R5			0,692					
KK1				0,625				%46,379
KK2				0,489				
KK3				0,683				
KK4				0,871				
M1					0,304			%42,035
M2					0,859			
M3					0,568			
M4					0,727			
G1						0,652		%44,611
G2						0,457		
G3						0,775		
G4						0,741		
T1							0,898	%54,986
T2							0,548	
T3							0,736	

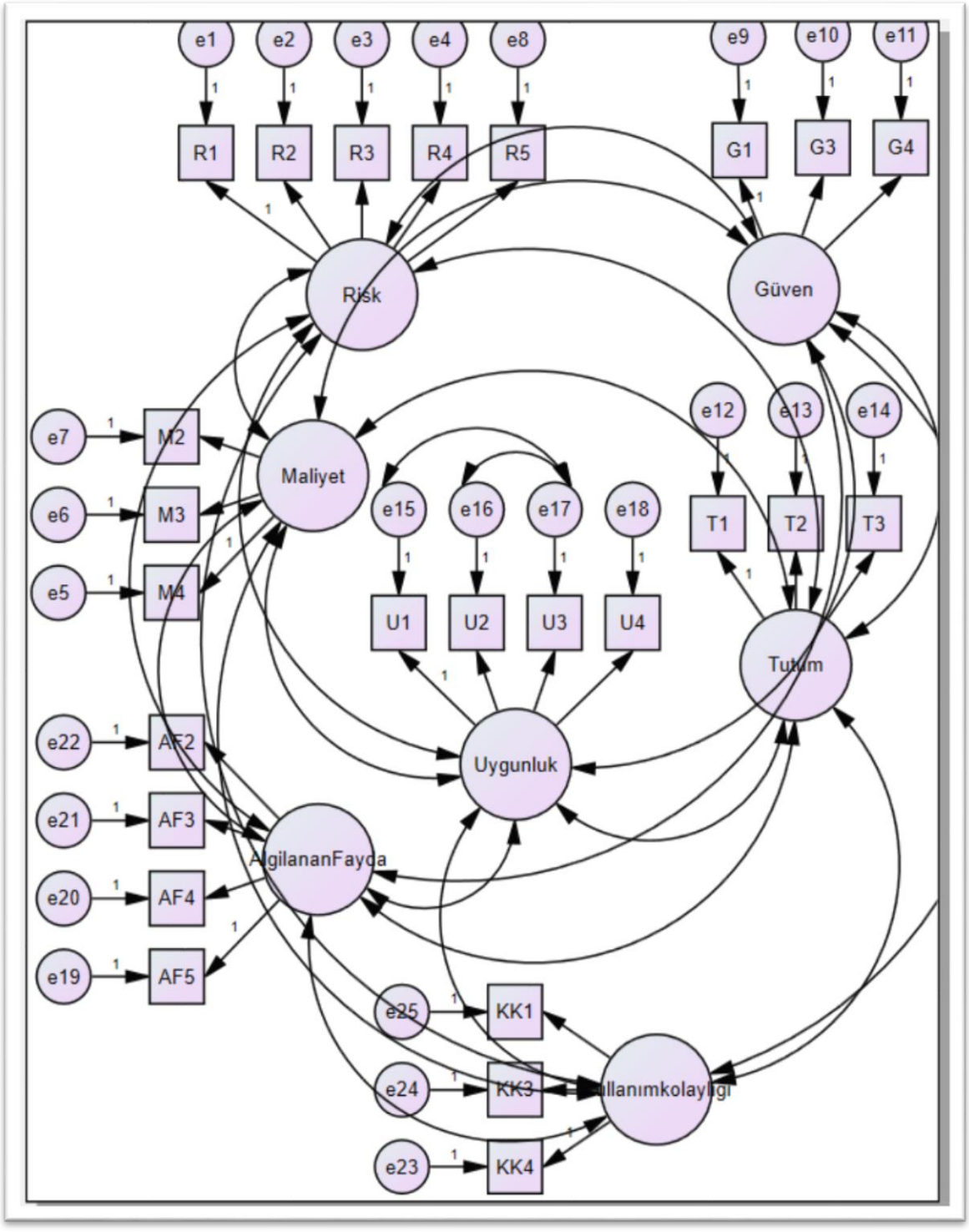
Faktör yük değeri 0,50'nin altında kalan M1, AF1, G2 ve KK2 ifadeleri ölçekten çıkartılmıştır. Modelden madde çıkarma işlemi adım adım yapılmıştır. Çıkarılan her bir madde sonrasında yeniden analiz yapılmış ve değerlendirilmiştir. Bu ifadelerin silinmesinin Cronbach-Alfa değerlerinde de yükselme sağladığı güvenilirlik analizinde ortaya çıkmıştı. Bunun yanında toplam varyansı açıklama oranında da artış görülmüştür.

Bir sonraki adım DFA'nın yapılmasıdır. Temelde keşfedici faktör analizi ile amacına bağlı olarak DFA arasında farklılık gösterir. Bu açıdan bakıldığında, her iki yöntem de bir korelasyon matrisinin altındaki faktör yapısını değerlendirmek için kullanılır, ancak AFA teoriyi "inşa etmek" için kullanılırken, DFA onu "onaylamak" için kullanılır. Bu nedenle, AFA, araştırmacı, ilgilenilen değişken veya yapı hakkında çok az şey bildiğinde kullanılır ve bu yaklaşım, gizli ve manifest değişkenler arasındaki ilişkilerin korelasyonuna ek olarak, tezahür değişkenlerinin altında yatan gizli faktörleri belirlemeye yardımcı olur. Diğer yandan, incelenen değişkenler hakkında net bir fikre sahip olduğumuzda, yani faktörleri oluşturduğumuz hipotezlerde, DFA kullanımı hipotezlenmiş yapıyı test etmeyi ve hipotezlenmiş modelin verilere uygun olup olmadığını kontrol etmeyi sağlar. Ancak yine de bu konuda farklı görüşler olduğu görülmektedir. Dolayısıyla, AFA ve DFA'yı niteliksel olarak ayrı iki kategori olarak değerlendirmek yerine, sürekliliği bie analizin iki parçası olarak düşünerek iki alt analizinde yapılması uygun görülmüştür (Lloret-Segura ve diğerleri, 2014).

DFA için ise literatürde geniş örneklem sayılarının daha iyi sonuçlar ortaya koyacağı şeklinde ifadeler olmakla birlikte bu büyüklüğü net olarak ifade etmek güçtür. Kline (2005) bu modeller için 100 kişiden oluşan örneklem sayısını küçük, 100-200 arasını orta ve 200'den büyük katılımcıları ise iyi olarak ifade etmiştir. DFA'nın maksimum olabilirlik yöntemini kullandığı dikkate çekilerek normallik varsayımına bakılması ve örneklem sayısının AFA'da da belirtildiği gibi ifade sayısının en az 5 katı olması gerekliliğinden bahsedilmiştir (Ursavaş ve diğerleri, 2014).

DFA ve YEM analizleri, AMOS 22.0.0 programı kullanılarak gerçekleştirilmiştir.

Aşağıda Şekil 3.4'de DFA için çizilen örtük değişkenleri içeren şekil yer almaktadır.



Şekil 3.4. DFA Çizimi

İlk gizli faktörü temsil eden elips çizildikten sonra, gözlemlenen değişkenler eklenmiştir. Dikdörtgen tek bir gözlemlenen değişkeni temsil eder. Gizli faktörden gözlenen değişkene regresyon yolunu işaret eden bir ok çizilir. Yine gözlenen değişkene

doğru ölçüm hatası teriminden (*e*) bir ok gider. Faktörler arasındaki Kovaryansı gösteren çift başlı oklar da Şekil 3.4'de görülmektedir (Shek ve Yu, 2014).

Analiz sonucunda elde edilen uyum iyiliği değerleri ve kabul edilebilir değerler Tablo 3.13'de verilmiştir.

Tablo 3.13. Uyum İyiliği Değerleri

İndeks	Model Değeri	Normal Değer	Kabul Edilebilir Değer
χ2 /sd	1,722	<2	<5
CFI	0,905	>0,95	>0,90
GFI	0,816	>0,9	>0,8
NFI	0,805	>0,9	>0,8
RMR	0,059	<0,05	<0,08
RMSEA	0,071	<0,05	<0,08

Normal ve kabul edilebilir değerler Forza ve Flippinel (1998), Greenspoon ve Saklofske (1998), Hair ve diğerleri (2010) ve Awang (2012)'ın çalışmalarından referans alınarak Tablo 3.13'de yer almıştır. İndeks değerleri aşağıda sırasıyla açıklanmıştır.

- χ^2/sd Değeri: Ki-kare indeksine göre örneklem büyüklüğünden daha az etkilendiğinden tercih edilen değerdir. Serbestlik derecesinin büyük olduğu durumlarda Ki-kare indeksi her zaman iyi uyum gösterir. Fakat χ^2 değerinin serbestlik derecesine bölünmesiyle bulunan χ^2/sd değeri Ki-kare indeksinin örneklem büyüklüğü ile olan pozitif ilişkisini engeller.
- CFI (Comparative Fit Index): Değişkenler arasında korelasyon ya da kovaryans ilişkisinin olmadığını varsayan ve null (boş) model ile karşılaştıran değerdir.
- GFI (Goodness of Fit Index): Modelin örneklemdeki kovaryans matrisini ne oranda ölçtüğünü gösterir.
- NFI (Normed Fit Index): Bu istatistik, modelin χ^2 değerini null modelin χ^2 ile karşılaştırarak değerlendirir. Boş / bağımsızlık modeli, ölçülen tüm değişkenlerin ilişkisiz olduğunu belirttiği için en kötü durum senaryosudur.
- RMR (Root Mean Square Residual): Bu değer sıfıra yaklaştıkça test edilen modelin daha iyi uyum iyiliği sağladığını gösterir.

- RMSEA (Root Mean Square Error of Approximation): Ana kütledeki yaklaşık uyumu ölçen diğer bir ölçüttür. Sıfır ile bir arasında bir değer alır (Hooper ve diğerleri, 2008, Çapık, 2015). Daha küçük değerler daha iyi uyum olduğu anlamına gelir. Diğer uyum değerlerinden farklı olarak daha karmaşık modellerin daha yüksek değer almasına neden olur.

Ölçüm modeli testi, veriler ve önerilen ölçüm modeli arasında iyi bir uyum sağlamıştır. Örneğin ki-kare / serbestlik dereceleri (427/248), χ^2/sd 1,722 ile 2 değeri altında yer almaktadır. Bu öneriye dayanarak verilere iyi bir şekilde uymaktadır. RMSEA değeri 0,071 ile önerilen kabul edilebilirlik aralığında (<0,05-0,08) yer almaktadır. CFI, GFI, NFI ve RMR değerleri de kabul edilebilir uyum içerisinde olduğunu göstermektedir.

Birleşme güvenilirliği (CR- Composite Reliability), ölçüm modelinin iç tutarlılığını değerlendirmek için hesaplanmıştır. Modele dahil edilen ölçeklerin CR'si Tablo 3.14'de görüldüğü gibi 0,85 ile 0,89 arasındadır. Sonuçlar 0,7 kritik değeri üzerindedir. Bu durum ölçeklerin tümünün güçlü ve yeterli güvenilirliğe sahip olduğunu ve geçerliliği ayırt ettiğini göstermiştir. Ayrıca açıklanan ortalama (AVE- Average Variance Extracted) varyansta 0,62 ile 0,68 değerleri arasında olup, 0,5 değeri üzerindedir (Fornell ve Larcker, 1981).

CR ve AVE değerleri hesaplanırken, formül 3.2 ve 3.3 kullanılmıştır. Microsoft Excel'de manuel olarak yapılan hesaplamada SPSS'ten alınan faktör yük parametreleri (λ_i) kullanılmıştır (Ping, 2004).

$$AVE = \frac{\sum_{i=1}^{n}(\lambda_i{}^2)}{n} \tag{3.2}$$

$$CR = \frac{(\sum_{i=1}^{n}\lambda_i)^2}{(\sum_{i=1}^{n}\lambda_i)^2 + (\sum_{i=1}^{n}\delta_i)} \tag{3.3}$$

Tablo 3.14. Uyum İyiliği Değerleri

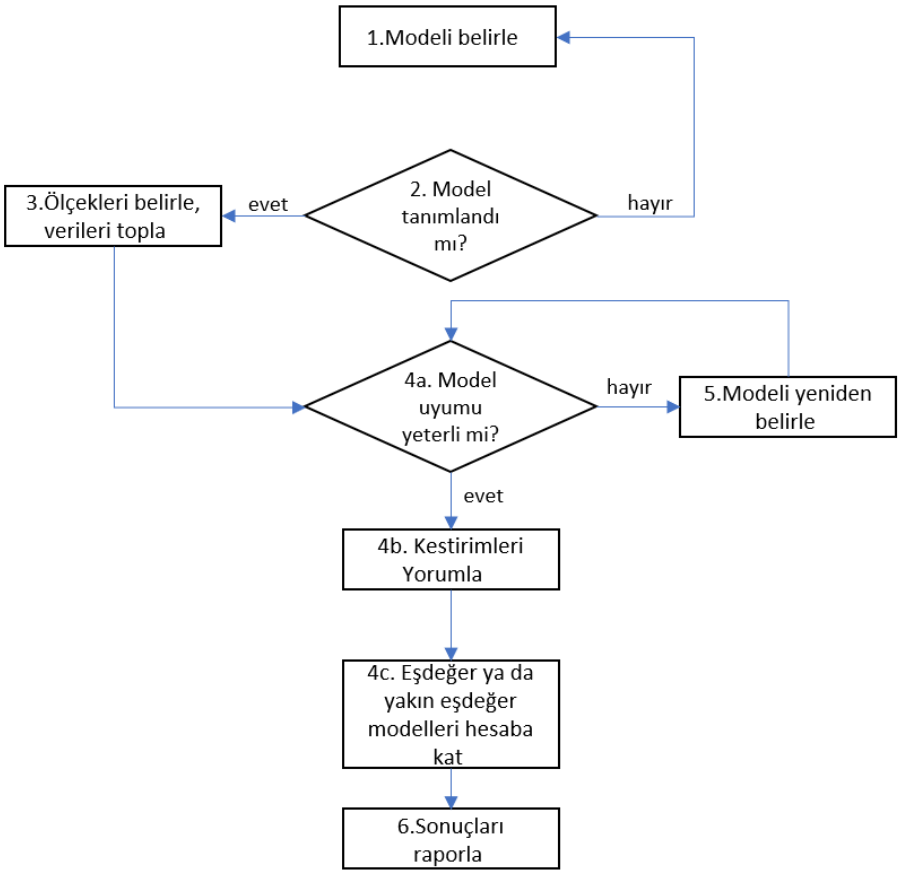
Faktörler	Birleşme Güvenirliği (CR) (>0,70)	Açıklanan Ortalama Varyans AVE (>50)
Algılanan Fayda	0,88	0,65
Uygunluk	0,89	0,67
Risk	0,89	0,62
Kullanım Kolaylığı	0,85	0,66
Maliyet	0,86	0,67
Güven	0,87	0,68
Kullanıma Yönelik Tutum	0,86	0,68

3.4.5. Yapısal Eşitlik Modeli

YEM ve diğer çok değişkenli teknikler arasındaki en belirgin fark, bir dizi bağımlı değişken için ayrı ilişkilerin kullanılmasıdır. YEM, istatistiksel program tarafından kullanılan yapısal modeli belirleyerek, bir dizi ayrı, ancak birbirine bağımlı, çoklu regresyon denklemini aynı anda tahmin edebilir. Araştırmacı hangi bağımsız değişkenlerin hangi bağımlı değişkenleri öngördüğünü ayırt etmek için, teori, önceki deneyim ve araştırma hedeflerini kullanır.

Bir ilişkideki bağımlı değişkenler, sonraki ilişkilerde bağımsız değişkenler haline gelebilir ve bu da yapısal modelin birbirine bağımlı olmasına yol açar. Dahası, aynı değişkenlerin çoğu bağımlı değişkenlerin her birini etkileyebilir, ancak farklı etkilere sahiptir. Yapısal model, bağımlı bir değişken diğer ilişkilerde bağımsız bir değişken olduğunda bile, bağımsız ve bağımlı değişkenler arasındaki bu bağımlılık ilişkilerini ifade eder. Önerilen ilişkiler daha sonra her bağımlı değişken için bir dizi yapısal denkleme (regresyon denklemine benzer) dönüştürülür. Bu özellik, YEM'i bağımlı ve bağımsız değişkenler arasında yalnızca tek bir ilişkiye izin veren, çok sayıda bağımlı değişkenleri (çok değişkenli varyans ve kanonik korelasyon analizi) içeren birinci nesil çok değişkenli istatistiklerden, tekniklerden ayırır (Hair ve diğerleri, 2008).

YEM'in temel adımları Şekil 3.5'te gösterilmektedir (Kline, 2011). Çalışma bu başlıklar ele alınarak adım adım ilerlemiştir.

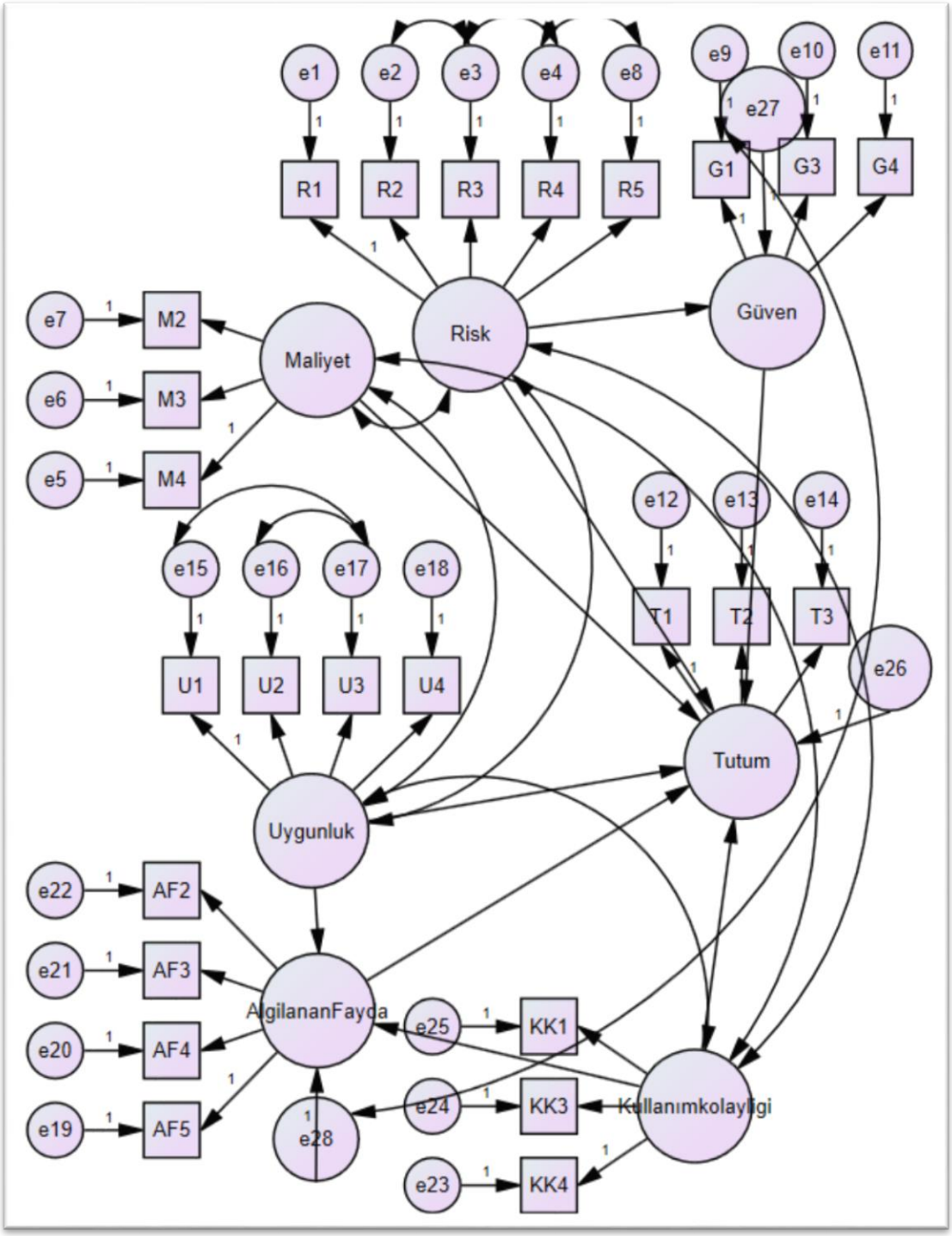


Şekil 3.5. YEM'in Temel Adımları

YEM, faktör analizi ve çoklu regresyonun bir kombinasyonu olarak tanımlanmıştır. YEM, DFA ile karşılaştırıldığında, gizli değişkenler arasındaki ilişkilerin iki bileşeni kapsar: bir ölçüm modeli (esasen DFA) ve yapısal bir model. Yapısal modelde, önerilen modeldeki gizli yapılar ve gözlemlenebilir değişkenler arasındaki ilişkileri, birkaç regresyon denklemi yerine tek bir çerçeve altında gösterir. DFA'dan farklı olarak Şekil 3.6'da faktörler arasındaki ilişki tek taraflı oklar kullanılarak gösterilmiştir.

Bu aşamada YEM ile ilişkili iki terimi açıklamak gerekmektedir: Eksojen ve Endojen değişkenler. Eksojen bağımsız değişkenlere ve endojen ise bağımlı veya sonuç değişkenlerine benzer olarak ifade edilebilir. Eksojen ve endojen değişkenler, test edilen modele bağlı olarak gözlenebilir veya gözlenemez. Yapısal modelleme bağlamında, eksojen değişkenler, incelenen diğer yapılar üzerinde etkisi olan ve nicelik modelindeki diğer faktörlerden etkilenmeyen yapıları temsil eder. Endojen olarak tanımlanan yapılar ise, modeldeki eksojen ve diğer endojen değişkenlerden etkilenir.

Bu şartlarda risk, maliyet, uygunluk, algılanan kullanım kolaylığı eksojen değişkenler iken; güven, algılanan fayda ve kullanıma yönelik tutum endojen değişkenlerdir.



Şekil 3.6. Modelin Yapısal Eşitlik Modeli

Analiz sonucunda elde edilen uyum indekslerinin (p< 0,001, χ^2= 482.370, sd= 253, χ^2/sd= 1,907 , RMSEA= 0,079, CFI= 0,889, GFI= 0,8, NFI=0.78, RMR= 0,81) eşik değerlerinin sınırında ve kabul edilebilir uyum gösterdiği söylenebilir (Forza ve Flippinel, 1998, Greenspoon ve Saklofske, 1998, Hair ve diğerleri, 2010 ve Awang, 2012).

İlişkisi sorgulanan 9 hipotezden 7'sinin istatistiksel olarak anlamlı olduğu Tablo 3.15'te görülmektedir.

Tablo 3.15. Yapısal Modelin Hipotez Testi

Etkiler	Standardize Edilmiş Parametre Değerleri (β)	Standart Hata	t	p-değeri
Güven <--- Risk	0,376	0,065	5,786	***
Algılanan Fayda <--- Uygunluk	0,336	0,063	5,343	***
Algılanan Fayda <--- Kullanım kolaylığı	0,14	0,05	2,824	0,005
Tutum <--- Güven	0,281	0,1	2,813	0,005
Tutum <--- Risk	0	0,061	-0,001	0,999
Tutum <--- Maliyet	-0,088	0,048	-1,845	0,065
Tutum <--- Uygunluk	0,555	0,08	6,982	***
Tutum <--- Algılanan Fayda	0,336	0,13	2,596	0,009
Tutum <--- Kullanım Kolaylığı	-0,027	0,042	-0,639	0,523

Tabloyu detaylı olarak incelersek, öncelikle riskin güven üzerinde anlamlı bir etkiye sahip oduğunu söyleyebiliriz. (β= 0,376, p< 0,05) Ancak, bu etkinin negatif olması beklenirken bu etki pozitif yönlüdür. Ayrıca risk ile tutum arasında herhangi bir anlamlı ilişki bulunmamaktadır (β= 0, p = 0,99). Uygunluk, hem algılanan fayda (β= 0,336, p< 0,05) hem de kullanıma yönelik tutum (β= 0,555, p< 0,05) üzerinde anlamlı bir pozitif bir etki göstermektedir. Kullanım kolaylığı, algılanan fayda üzerinde anlamlı bir pozitif etki gösterirken (β= 0,140, p< 0,05); kullanıma yönelik tutum üzerinde anlamlı bir etkisi olmadığı bulgusuna varılmıştır (β= -0,27, p = 0,523). Diğer taraftan güven kullanıma yönelik tutum üzerinde anlamlı bir pozitif (β= 0,281, p< 0,05) etkiye sahiptir. Maliyet ise kullanıma yönelik tutum üzerinde anlamlı bir etkiye sahiptir ve beklenildiği gibi bu etki negatif yönlüdür (β= -0,088, p< 0,010 kabul edilmiştir). Son olarak algılanan faydanın, kullanıma yönelik tutumu anlamlı ve pozitif (β= 0,548, p< 0,001) şekilde etkilediği sonucuna ulaşılmıştır.

Tablo 3.16'da özetlendiği üzere sunulan dokuz hipotezden H2 ve H7 hipotezleri istatistiksel olarak anlamlı (p> 0,05) olmadığından desteklenmemiş, H9 hipotezi ise

istatistiksel olarak anlamlı olmasına karşın beklenen negatif etkinin aksine pozitif etkisi olması ile tersine desteklenmiştir. Son olarak H1, H3, H4, H5, H6 ve H8 hipotezleri olmak üzere altı hipotez istatistiksel olarak anlamlı ve desteklenmiştir.

Tablo 3.16. Yapısal Modelin Hipotez Testi Sonuçları

H1: Algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif bir etkisi vardır.	Desteklendi
H2: Algılanan kullanım kolaylığının kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.	Desteklenmedi
H3: Algılanan faydanın kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.	Desteklendi
H4: Uygunluk algılanan fayda üzerinde pozitif etkiye sahiptir.	Desteklendi
H5: Uygunluk kullanıma yönelik tutum üzerinde pozitif etkiye sahiptir.	Desteklendi
H6: Beklenen maliyetin kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.	Desteklendi
H7: Algılanan riskin, kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.	Desteklenmedi
H8: IoT cihazlarının askeri alanda kullanılmasına duyulan güvenin kullanıma yönelik tutum üzerinde olumlu yönde etkisi vardır.	Desteklendi
H9: Algılanan riskin, güven üzerinde olumsuz etkisi vardır.	Tersine Desteklendi

Öncelikle desteklenmeyen hipotezler incelendiğinde; “H2: Algılanan kullanım kolaylığının kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır.” hipotezinin desteklenmemesi sonucunda betimsel istatistiklere bakıldığında personelin kullanım kolaylığı görmesiyle ilgili az da olsa katılım sağladığı ancak çoğunlukla kararsız olduğu görülebilir. Aynı şekilde kullanıma yönelik tutum incelendiğinde pozitif yönde tutum olduğu görülmektedir. Ancak kullanım kolaylığının kullanıma yönelik tutum üzerinde pozitif bir etki oluşturduğu görülmemiştir. Kullanımı kolay bulması ile kullanım tutumu arasında istatistiksel olarak pozitif ya da negatif bir ilişki tespit edilmemiştir. “H7: Algılanan riskin, kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır.” hipotezi desteklenmeyen bir diğer hipotezdir. Personel açık uçlu sorularda da yer verdiği gibi risk ve güvenlik konularında sıkıntı duymaktadır. Ancak sonuçlar göstermektedir ki

duyulan risk kullanım tutumuna engel olmamış; negatif ya da pozitif yönde istatistiksel olarak anlamlı bir etki oluşturmamıştır.

"H9: Algılanan riskin, güven üzerinde olumsuz etkisi vardır." hipotezi beklenmedik bir sonuçla; iki faktörün istatistiksel olarak ilişkili ama savunulanın aksine olumlu bir etki ortaya koyduğunu göstermiş, tersine desteklenmiştir. Personel hem güvenlik, gizlilik anlamında risk duymakta hem de IoT'den gelen veriye güven duyarak operasyon yönetilebileceğine yönelik tutum sergilemektedir.

"H1: Algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif bir etkisi vardır." hipotezi desteklenmiştir. Personelin teknolojiye kolayca katılabileceği, basit ve kullanımı kolay bulacağı teknolojiden fayda algıladığı görülmektedir.

"H3: Algılanan faydanın kullanıma yönelik tutum üzerinde pozitif bir etkisi vardır." hipotezi desteklenmiştir. Personel fayda sağlayacağını düşündüğü bu teknolojiyi kullanım konusunda olumlu bir tutuma sahiptir.

"H4: Uygunluk algılanan fayda üzerinde pozitif etkiye sahiptir." hipotezi desteklenmiştir. Personelin ihtiyaçları ile tutarlı olarak algıladığı alana uygun bulduğu teknoloji faydalı algılanmayı sağlamaktadır.

"H5: Uygunluk kullanıma yönelik tutum üzerinde pozitif etkiye sahiptir." hipotezi desteklenmiştir. Sahaya uygunluğu fazla olan teknoloji, personel için anlamlı olmakta ve böylece hem fayda sağlayacağına olan inanç artmakta hem de kullanım tutumu isteğini artırmaktadır.

"H6: Beklenen maliyetin kullanıma yönelik tutum üzerinde olumsuz yönde etkisi vardır." hipotezi desteklenmiştir. Yeni teknolojiye entegre olma, uyarlama, eğitim vb. maliyetlerin kullanım tutumunu olumsuz yönde etkilediği, kısıtlı bütçe planlamaları göz önüne alındığında maliyeti etkin çözümlerin önem arz ettiği pek çok çalışmada olduğu gibi bu çalışmada da gösterilmektedir.

"H8: IoT cihazlarının askeri alanda kullanılmasına duyulan güvenin kullanıma yönelik tutum üzerinde olumlu yönde etkisi vardır." hipotezi desteklenmiştir. Personel satın alma isteğinden, bir teknolojinin kabulüne kadar güven duyduğu konuya karşı pozitif kullanım tutumu sergilemektedir.

Ana hipotezler yanında Bölüm 3.1'de yer alan alt hipotezler değerlendirildiğinde; "Askeri IoT, askeri uygulamaların doğası gereği "sıradan" IoT'den farklıdır." hipotezinin hem literatür taraması ortaya çıkan fiziksel ve taktik alan gereksinimleri hem de personelin açık uçlu sorulara verdiği görüşleri ile desteklenmiştir.

"Geleneksel askeri teçhizatın çeşitli uyarlamalarla IoT için kullanılması mümkündür." hipotezi ise betimsel istatistik sonuçları (M3 ifadesi) değerlendirildiğinde geleneksel teçhizatın yetersiz kalacağı, uyarlamaların yüksek maliyet getireceği yönündedir.

"Geleceğin savaş ortamı ve savaş sanatı IoT ile temel değişikliklere uğrayacaktır. Yüksek düzeyde bağlı bir çalışma ortamı olarak gelecekteki askeri savaş alanının Doktrin ve Teknikleri, Taktikleri ve Prosedürleri temelde değişikliğe uğrayacaktır." hipotezi ise hem açık uçlu görüşler hem de betimsel istatistik (T2) değerlendirmesi sonucu en yüksek oranda katılım alan ifadelerden olmuş ve desteklenmiştir.

SONUÇ VE ÖNERİLER

Bu çalışmanın amacı temelde “Askeri alanda IoT kullanılabilirliği mümkün müdür?”, “Askeri alana ait kısıtlar nelerdir? ve “Personelin kullanıma yönelik beklentileri nelerdir?” sorularına cevap aramak ve bu alanda teknolojinin kabul ve kullanımına yönelik önerilen modeli ve hipotezleri değerlendirmektir.

Tezin birinci bölümünde; büyük veri ve kaynaklarından biri olan nesnelerin interneti unsurları ve teknolojileri çalışılmıştır. İlk bölümün son kısmı tamamen askeri alandan IoT kullanım alanları ve kısıtlarına ayrılmıştır.

Tezin ikinci bölümü olan Kuramsal Temeller, çalışmanın teorik alt yapısının kurulması için gerekli olan diğer kısım olarak planlanmış; çalışmamıza yön veren model ve teoriler incelenmiştir. Bu bölüm altında yer alan geçmiş çalışmalar öncelikle IoT alanında kabul çalışmaları başlığı altında incelenmiştir. Çalışmalarda; algılanan fayda, algılanan kullanım kolaylığı gibi ana faktörler yanında mevzuat ve veri güvenliği gibi bağlamsal faktörler, bilgi kullanımının şeffaflığı, sosyal etki, algılanan zevk, maliyet ve gizlilik endişeleri gibi etkiler dikkati çekmektedir. Tüketicilerin daha kolay bir günlük yaşama sahip olma ve daha akıllı evlerde oturma eğiliminde oldukları da gözler önüne sunulan bir başka gerçekliktir. Öte yandan askeri alanda kabul çalışmaları incelendiğinde; algılanan fayda, kullanım kolaylığı faktörleri yanında güven seviyesi, performans beklentisi, uyumluluk, veri yönetimi ve korunması beklentisi ön plana çıkıyor. Askeri organizasyonlar için, güvenlik ve güvenilirlik birçok değerin önünde geliyor. Askeri organizasyonlar birçok zaman yeni teknolojilere öncülük etmekle birlikte bazı yeni teknolojilerin adaptasyonu içinde erken katılımcılardan olmadığı bir gerçekliktir.

Üçüncü bölüm araştırmanın amacı, modeli, hipotezleri, yöntemi ve bulgularını kapsıyor.

Askeri sahada; algılanan fayda, kullanım kolaylığı faktörleri yanında güven seviyesi, performans beklentisi, uyumluluk, veri yönetimi ve korunması beklentisi ön plana çıkmaktadır. Bunun yanında, güvenlik ve güvenilirlik birçok değerin önünde gelmektedir. Askeri organizasyonların birçok zaman yeni teknolojilerin öncüsü olduğu bilinmekle beraber bazı yeni teknolojilerin adaptasyonu içinde erken katılımcılardan olmadığı bir gerçekliktir.

Literatür ve alan tecrübesi göz önüne alınarak hazırlanan modelin ve hipotezlerin testi için öncelikle anket (EK1-2) hazırlanmıştır. Demografik sorular, 5'li likert ölçeği ile yazılan ifadeler ve açık uçlu soruları içeren anket hem Türkçe hem de İngilizce olarak hazırlanmış, online uygulaması İngilizce olarak sunulmuştur. Çalışmanın geçerliliği ve güvenilirliğini etkileyebilecek belirsizliklerden kaçınmak için yapılan ön test sonucunda ihtiyaç duyulan düzenlemeler yapılarak anket formu nihai haline getirilmiştir.

Veri elde etmek için belirlenen katılımcı hedef kitlesi: uluslararası bir bakış elde etmek maksadıyla farklı ülkelerden (çoğunlukla NATO ülkeleri) asker ya da askeri alanda çalışan kişiler ve şu an Türk Silahlı Kuvvetlerinde aktif görevde bulunmayan (emekli ya da sağlık gibi sebeplerle ayılmış) eski ordu mensupları olarak belirlenmiştir.

Çalışmanın örneklem büyüklüğü için 138 katılımcı alt sınır olarak hedeflenmiştir. Atatürk Üniversitesi LimeSurvey altyapısı kullanılarak hazırlanan anket 242 kişiye ulaşmış, 145 kişi tarafından tamamlanmıştır.

Analiz aşamasına gelindiğinde ilk olarak demografik kısım ele alınmıştır. Katılımcıların, %14,5'inin kadın, %85,5'inin erkek olduğu görülmektedir. %58 katılımcı 40 yaşın altındayken, %42'si 40 yaşın üzerindedir. Katılımcıların %65'i lisansüstü eğitimi, sadece %33,1'i lisans eğitimi almıştır. Katılımcıların %73,1'inin IoT kavramını daha önce duyduğu ancak %49,7'sinin kişisel olarak kullanım deneyimi bulunduğu gözler önüne serilen bir başka sonuçtur.

Ankette yer alan iki açık uçlu sorunun cevaplarının değerlendirilmesi de personelin kişisel görüşlerini ortaya koyması açısından önemlidir.

"Askeri alanda IoT kullanımına yönelik önerileriniz nelerdir? Bireysel ya da organizasyonel olarak ne gibi alanlarda kullanılabileceğini değerlendiriyorsunuz?" sorusuna verilen cevaplar genel anlamda 3 grup anlayışı ortaya koymaktadır. İlk grup, güvenlik çekinceleri sebebiyle askeri alanda IoT kullanımına tamamen karşı görüşte, ikinci ve bu teknolojiye daha ılımlı yaklaşan grup, basitten daha karmaşık alana ya da başka bir ifadeyle askeri alan içinde daha az riskliden daha çok riskli alana doğru adapte olma anlayışında, üçüncü grup ise her ne kadar çekinceler olsa da kullanılmasının gerekli hatta kaçınılmaz olduğu görüşündedir. Kullanıma yönelik öneriler değerlendirildiğinde kullanım alanlarının harekât (operasyon), karar destek, eğitim, güvenlik, lojistik,

giyilebilir teknolojiler, kentsel operasyonlar başlıkları altında toplandığı görülmektedir. Bu sonuçlar yapılan literatür araştırması ile neredeyse tamamen örtüşmektedir.

"Askeri alanda IoT kullanımına yönelik en büyük çekinceniz nedir?" sorusuna verilen cevapların neredeyse tamamına yakınında IoT'ye yönelik çekincelerin öncelikle gizlilik, güvenlik ve siber tehditler üzerine olduğu söylenebilir. Eğitim, büyük veri ile baş etme, hata toleransı ve maliyet diğer genel başlıklar olarak sıralanabilir.

Betimsel istatistikler ile ölçek ifadelerine ait ortalama ve standart sapma değerleri ortaya konmuştur. İfadelerin çarpıklık değerleri -1,088 ile 1,34 arasında, basıklık değerleri ise -1,071 ile 2,213 arasında değişmekte olup veri setinin normal dağılım özelliği gösterdiği ortaya konmuştur.

Kayıp veri içermeyen veriler SPSS 24.0.0.0'a aktarılmış ve ters ifadelerin değiştirilmesi ve gerekli düzenlemeler yapıldıktan sonra güvenilirlik ve geçerlilik analizlerine başlanmıştır.

İlk olarak; ölçek güvenilirliği için her bir faktörün Cronbach-Alfa iç-tutarlılık katsayısı hesaplanmış ve değerlendirilmiştir. Cronbach-Alfa değeri 0,7'nin üzerinde güvenilir kabul edilir. Bu değerin sınırında ya da biraz altında olan faktörlerde iyileşme sağlayan ifadeler bu aşamada silinmemiş, faktör analizinde bir sorun oluşturması durumunda değerlendirmesi yapılmıştır.

Ölçeğin yapı geçerliliğinin testi amacıyla AFA yapılması gerekmektedir. Veri setinin faktör analizi için uygun olup olmadığının değerlendirilmesi amacıyla, Kaiser-Meyer-Olkin ve Bartlett Sphericity testleri yapılmış ve faktör analizine uygun olduğu görülerek AFA'ya başlanmıştır.

Faktör yük değeri 0,5 limiti altında kalan, aynı zamanda Cronbach Alfa değerini de olumsuz yönde etkileyen M1, AF1, G2 ve KK2 ifadeleri adım adım ölçekten çıkartılmıştır.

Daha önceden belirlenen faktörlerle oluşturulmuş yapının geçerliliğini arttırmak için DFA bir sonraki adımda yapılan analiz olmuştur. Bu analiz ve sonrası AMOS 22.0.0 ile gerçekleştirilmiştir. Bu aşamada sonuçların uyum indeksleri vasıtası ile değerlendirmesi yapılmıştır. Ölçüm modeli testi, veriler ve önerilen ölçüm modeli arasında iyi bir uyum sağlamıştır. Örneğin ki-kare / serbestlik dereceleri (427/248), 1.722

ile 2 değeri altında yer almaktadır. RMSEA değeri 0,071 ile önerilen kabul edilebilirlik aralığında (<0.05-0.08) yer almıştır. CFI, GFI, NFI ve RMR değerleri de kabul edilebilir uyum içerisinde olduğunu göstermiştir.

Hipotezlerin ve modelin testleri için bir dizi ayrı, ancak birbirine bağımlı, çoklu regresyon denklemini aynı anda tahmin eden bu özelliğiyle ayrı regresyon denklemleri yazmadan tek çerçevede çalışmamızı yürütmemizi sağlayan YEM'e geçilmiştir. Analiz sonucunda elde edilen uyum indekslerinin ($p< 0,001$, $x^2= 482,370$, sd= 253, $\chi^2/sd = 1,907$, RMSEA= 0,079, CFI= 0,889, GFI= 0,8, NFI=0,78, RMR= 0,81) eşik değerlerinin sınırında ancak kabul edilebilir uyum gösterdiğini göstermektedir. Sonuçların değerlendirmesi yapıldığında, sunulan dokuz hipotezden H2 ve H7 istatistiksel olarak anlamlı olmadığından desteklenmediği, H9'un ise istatistiksel olarak anlamlı olmasına karşın beklenen negatif etkinin aksine pozitif etkisi olması sebebiyle tersine desteklendiği görülmektedir. Son olarak H1, H3, H4, H5, H6 ve H8 hipotezleri olmak üzere altı hipotez istatistiksel olarak anlamlı bulunup, desteklenmiştir.

Desteklenmeyen hipotezler özetle; personelin kullanımı kolay bulması ile kullanıma yönelik tutum arasında istatistiksel olarak anlamlı bir ilişki olmadığını, aynı şekilde duyulan risk ile kullanım tutumu arasında pozitif ya da negatif bir ilişki görülmediğini ortaya koymuştur. Kullanım kolaylığı tutum ilişkisi değerlendirildiğinde; emir-komuta zinciri içerisinde askerler açısından yerine getirilen görevlerde kullanım kolaylığı faktörünün ön planda tutulmadığı şeklinde yorumlanabilir. Risk ile tutum arasındaki sonuçlar, askeri alanın doğal çevresinin risk olgusu çerçevesi içinde olduğu düşünüldüğünde personelin tutumunda doğrudan bir rol oynamadığını göstermektedir. Algılanan riskin, güven üzerinde olumsuz etkisi vardır." hipotezi de beklenmedik bir sonuçla; iki faktörün istatistiksel olarak ilişkili ama savunulanın aksine olumlu bir etki ortaya koyduğunu göstermiştir. Personel hem güvenlik, gizlilik anlamında risk duymakta hem de IoT'den gelen veriye güven duyarak operasyon yönetilebileceğine yönelik tutum sergilemektedir. Bu durum askeri çevre için eşsiz bir olgudur ve arkasındaki nedenlerle daha fazla incelenmelidir. Bu sonuç savaş alanındaki askerlerin çoğunlukla takımlarıyla yalnız oldukları ve risk altında güvenebilecekleri tek varlığın mevcut teknolojiler olacağı düşüncesinden gelmiş olabilecektir.

Desteklenen hipotezler yorumlandığında; algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif etkisi görülmektedir. Örneğin jet pilotları, hedefe göndermelerinin daha kolay olması nedeniyle, GPS veya lazer güdümlü havadan yere bombaları kullanmayı, geleneksel, güdümsüz, serbest düşme bombalarına göre daha yararlı bulmaktadırlar. Algılanan faydanın kullanıma yönelik tutum üzerinde pozitif etkisi vardır. Savaş alanındaki her askerin akıllı bir saati vardır; fiziksel aktiviteleri, coğrafyası ve daha fazlası ile ilgili tüm bilgileri takip edebilir. Yararlı bulduğu bu aracı kullanmayı gereklilik görür. Uygunluğun algılanan fayda üzerinde pozitif etkisi görülmüştür. İHA'lar buna en iyi örnektir. Stratejik hedefler üzerindeki operasyonlarda uyumluluğu, bu tür hedeflerdeki vurum başarısı pozitif algı oluşturmuştur. Jet uçaklarından çok daha ucuzdur ve pilotu kaybetme riski yoktur. Uygunluğun kullanıma yönelik tutum üzerinde pozitif etkisi ortaya konmuştur. Kara sınırlarının güvenliği ele alındığında; 24 saat izleme ve analiz kabiliyetine sahip kameralar, sensörler ve gelişmiş görüntü analizi yazılımları askeri beklentilerle birebir örtüşmektedir. Komutanlar birlik izlemeyi uygun kılan bu teknolojileri kullanıma yönelik tutum göstermektedirler. Beklenen maliyetin kullanıma yönelik tutum üzerinde olumsuz yönde etkisi olduğu görülmektedir. Askeri kaynaklar sınırsız değildir. Komutanlar her harcama için detaylı, koordineli, planlı bir değerlendirme ve karar sürecini izlerler. Henüz tam olarak olgunlaşmamış bir alana ayrılacak bütçenin kullanım tutumunda oluşturduğu çekinceler anlaşılabilmektedir. IoT cihazlarının askeri alanda kullanılmasına duyulan güvenin kullanıma yönelik tutum üzerinde olumlu yönde etkisi görülmüştür. Askerî harekât ortamları son derece dinamik ve öngörülemeyen sahalardır. Komutanlar ve astlar yanlış verilen kararların, yalnızca kendilerini değil birlikte görev yaptıkları silah arkadaşlarını, hizmet ettikleri insanları tehlikeye atabileceğini bilirler. Kullandıkları cihazlara güven duymaları karar verebilmelerini, bu görevleri yerine getirebilmelerini sağlar.

Desteklenen ve hatta desteklenmeyen hipotezler ve görüşler ile bu çalışma göstermiştir ki riskleri ve getirileri ile IoT, geleceğin savaş alanını, savaş sanatını köklü değişikliklere uğratacaktır. Ancak bu dönüşüm süreci kapsamlı bir vizyon ve stratejik bir plan gerektirecektir. Başarısız bir dönüşüm süreci silah olarak kullanılabilecek bu teknolojiyi hedef haline getirebilecektir.

Bu çalışma personelin IoT teknolojisine genel olarak bakış açısını göstermiştir. Bu teknolojiyi kullanım için önem verdiği hususlar gözler önüne serilmiştir. Yeni tasarlanacak sistemler ve geçiş süreçlerinde bu beklentiler dikkate alınmalıdır.

Gelecek çalışmalar teknik anlamda ele alındığında; anlık veri değerlendirmesinin hayati önem taşıdığı askeri alan içinde Kenar Bilişimin göz önüne alındığı güvenlik ve gerçek zamanlı ihtiyaçları koordine eden mimariler üzerinde yoğunlaşmalıdır. Yapay Zekâ uygulamaları alana özgü ihtiyaçlar göz önüne alınarak geliştirilmelidir. Askeri alan içinde görmezden gelinemeyecek en önemli husus ise güvenliktir. Silah olarak görülen bu teknoloji bir anda hedef haline gelebilir. Ancak şifreleme gibi güvenlik tedbirleri göz önüne alınırken teknolojinin içerdiği büyük veri hesaba katılarak, performans sonuçları göz önüne alınarak yapılacak geliştirmeler kaçınılmazdır.

Gelecek çalışmalar sadece teknik hususları içermekle sınırlı kalmamalıdır. Teknik olarak eksiksiz mükemmel bir sistem bile olsa bu teknolojiyi kullanacak insandır. Askeri sahada IoT kabulüne yönelik literatürde daha önce bir çalışmaya rastlanmamıştır. Bu çalışma gelecek yıllarda kullanılmaya başlanacak ve hatta kısmen kullanılmaya başlamış IoT teknolojini personel gözünden yorumlayan öncül çalışmalardandır. Çalışma verileri orta seviye yönetici seviyesindeki personelden toplanmıştır. Oldukça eğitimli bu kitle çalışmanın bir sınırlılığı olarak görülebilir. Farklı seviye personel gruplarının farklı beklenti ve ihtiyaçları bulunabilir. Gelecekteki araştırmalar farklı kullanıcı gruplarını ele alacak şekilde detaylandırılmalıdır. Ayrıca bu çalışmada askeri sahanın genelinde kullanımına yönelik bir kapsam belirlenmiştir. Gelecek çalışmalar belirli alanlarda kullanılan IoT sistemler üzerinden daha dar kapsamlarda ele alınarak incelenebilir.

Değişken koşullar altında insan yorgun, sıkılmış veya kayıtsız olabilir. IoT ise güvenlik açıklıkları olabilecek ve görmezden geleceği duyguları olan bir mekanizmadır. İşte insan ve makinaların bir arada olduğu bu düzende büyük bir güven ve yönetim problemi olması da kaçınılmazdır. Bu düzen farklı bir yönetim anlayışı ve stratejik liderlik gerektirecektir. Gelecek çalışmalar teknik ve yönetimsel olarak, ele alınan heterojen bileşenlerin olduğu düzeni izleyecek ve yorumlayacak yönetimsel yöntemleri ve ara yüzleri de konu almalıdır. Eğitimli personel bu geçişte kilit rol oynayacaktır.

KAYNAKÇA

A Power Saving Hybrid Technique for IoT (PDF Download Available). Available from: https://www.researchgate.net/publication/323857175_A_Power_Saving_Hybrid_Technique_for_IoT [Erişim Tarihi: Mar 21 2018].

ABD Devlet Hesap Verebilirlik Ofisi (2017). Internet of Things Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD, Highlights of GAO-17-668, a report to congressional committees.

Ahmed, A ve Patgiri, R. (2016). Big Data: The V's of the Game Changer Paradigm, IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems.

Akça, Y. ve Özer, G. (2012). "Teknoloji kabul modeli'nin kurumsal kaynak planlaması uygulamalarında kullanılması". *Business and Economics Research Journal*, 3 (2) 79-96.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., ve Ayyash, M. (2015). "Internet of things: A survey on enabling technologies, protocols, and applications". *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.

Awang, Z. (2012). *Structural equation modeling using AMOS graphic*. Penerbit Universiti Teknologi MARA.

Azmoodeh, A., Dehghantanha, A. ve Choo K.R. (2018). Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning, IEEE Transactions on Sustainable Computing (Issue: 99)

Bachlechner, D. ve Leimbach, T. (2016). "Big data challenges: Impact, potential responses and research needs", *IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 257–264.

Bağlıbel, M., Samancıoğlu, M., ve Summak, S. (2010). "Okul yöneticileri tarafindan e-okul uygulamasinin genişletilmiş teknoloji kabul modeline göre

değerlendirilmesi", *Mustafa Kemal Üniversitesi Sosyal Bilimler Dergisi*, 7 (13) 331-348.

Bartlett, J.E., Kotrlik, J.W. ve Higgins, C.C. (2001). "Organizational research: Determining appropriate sample size in survey research. Information Technology", *Learning and Performance Journal*, 19(1), 43–50.

Bernsdorf, C., Hasreiter, N., Kranz, D., Sommer, S., ve Rossmann, A. (2016). "Technology acceptance in the case of IoT appliances". *In DEC*, 49-63.

Bughin, J. (2016). "Big data, Big bang?", *Journal of Big Data*, 3(2), Springer.

Büyüköztürk, Şener. "Faktör analizi: Temel kavramlar ve ölçek geliştirmede kullanımı." *Kuram ve Uygulamada Egitim Yönetimi Dergisi*, 8(4), 2002, 470-483..

Çapık, Cantürk. (2015). "Geçerlik ve güvenirlik çalışmalarında doğrulayıcı faktör analizinin kullanımı". *Anadolu Hemşirelik ve Sağlık Bilimleri Dergisi*, Sayı: 17, 196-205.

Carmack, R. (2016). *Acceptance of Artificially Intelligent Autonomous Self-Governing Technology (AIASGT): A Qualitative Case Study*, (Doktora Tezi), Northcentral University/ Faculty of the School of Business and Technology Management.

Castro, D., New J. ve McQuinn, A. (2016). How Is the Federal Government Using the Internet of Things?, *Center for Data Innovatıon*.

Çelik, S. (2017). "Büyük veri teknolojilerinin işletmeler için önemi", *Social Sciences Studies Journal*, *3*, 873-883. 10.26449/sssj.119.

Cha, S., Baek, S., Kang, S. ve Kim, S. (2018). "Security Evaluation Framework for Military IoT Devices", *Security and Communication Networks*.

Chau, P. Y. K. (2001). "Influence of computer attitude and self-efficacy on IT usage behavior". *Journal of End User Computing*, 13(1), 26-33.

Chief Information Officer (2016). *DoD Policy Recommendations for The Internet of Things (IoT),* U.S. Department of Defense.

Chudzikiewicz, J., Furtak, J. ve Zielinski, Z. (2015). *Fault-tolerant techniques for the Internet of Military Things.* In Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy.

Chunxiang, L. (2014). "Study on Mobile Commerce Customer Based on Value Adoption", *Journal of Applied Sciences, 14,* 901-909.

Chuttur, M.Y. (2009). "Overview of the technology acceptance model: origins, developments and future directions". *Sprouts: Working Papers on Information Systems*, 9(37), 1–21. Indiana University, USA

Cigdem, H ve Oncu, S. (2015). "E-Assessment Adaptation at a Military Vocational College: Student Perceptions", *Eurasia Journal of Mathematics, Science & Technology Education,* 11(5), 971-988.

Dautov, R. ve Distefano, S. (2017). "Quantifying volume, velocity, and variety to support (big) data-intensive application development". *Proceedings of IEEE International Conference on Big Data*, Boston, Piscataway, 2843–2852.

Davis F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology". *MIS Quart, 13,* 319–339.

Davis, F.D. (1986). *A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results*, (Doktora Tezi), Cambridge: Massachusetts Institute of Technology.

Dibra, M. (2015). "Rogers theory on diffusion of innovation: The most appropriate theoretical model in the study of factors influencing the integration of sustainability in tourism businesses". *Procedia Social and Behavioral Sciences, 195,* 1453-1462.

Durodolu, O. (2016). "Technology Acceptance Model as a predictor of using information system' to acquire information literacy skills", *Libr. Philos. Pract.,* vol. 1450, no. e-journal, 3-28.

Durodolu, O. (2016). Technology Acceptance Model as a predictor of using information system' to acquire information literacy skills.

Elstad, A. ve Reitan, B. (2015). Mobile Information Platforms in The Military Domain, *NOKOBIT*, 23(1), 1-11.

Farooq M. J. ve Zhu, Q. (2018). "On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT)", *IEEE Transactions on Wireless Communications* (Issue: 99).

Fongen, A. ve Mancini, F. (2015). Integrity Attestation in Military IoT, Internet of Things (WF-IoT), *IEEE 2nd World Forum on Internet of Things*.

Fornell, C., ve Larcker, D. F. (1981). "Evaluating structural equation models with unobservable variables and measurement error". *Journal of marketing research*, 18(1), 39-50.

Forza, C. ve Flippini, R. (1998). "TQM impact on quality conformance and customer satisfaction: a causal model International" *Journal of Production Economics, 55,* 1-20.

Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. Ve González-López, M. (2016). "A review on internet of things for defense and public safety". *Sensors, 16,* 1644.

Furtak, J., Zieliński Z.ve Chudzikiewicz, J. (2016). "Security techniques for the WSN link layer within military IoT", *IEEE 3rd World Forum on Internet of Things (WF-IoT),* Reston, VA, 233-238.

Gao, L. ve Bai, X. (2014). "A unified perspective on the factors influencing consumer acceptance of internet of things technology", *Asia Pacific Journal of Marketing and Logistics*, 26(2), 211-231.

Ghazi, M. R. ve Gangodkar, D. (2015). "Hadoop, MapReduce and HDFS: a developers perspective". *Procedia Computer Science*. *48*. 45-50. 10.1016/j.procs.2015.04.108.

Gögüs, C. G., ve Özer, G. (2014). "The roles of technology acceptance model antecedents and switching cost on accounting software use". *Academy of Information and Management Sciences Journal*, 17(1), 1–24

Granjal, J., Monteiro, E. ve Sá Silva, J. (2015). "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", in *IEEE Communications Surveys & Tutorials*, 17(3), 1294-1312.

Greenspoon, P. J. ve D. H. Saklofske (1998). "Confirmatory factor analysis of the multidimensional students' life satisfaction scale", *Personality and Individual Differences 25*, 965–972.

Gurbuz, S. ve Aydin, G. (2017). "Classification of scientific papers with big data Technologies", 2017 *International Conference on Computer Science and Engineering (UBMK),* Antalya, 697-701.

Hair, J. F., Anderson, R. E., Babin, B. J. ve Black, W. C. (2010). "Multivariate data analysis: A global perspective" (Vol. 7): *Pearson Upper Saddle River*.

Hair, J.F., Anderson, R.E., Tatham, R.L., ve Black, W.C. (2008). *Multivariate Data Analysis*, (7th ed.). New Jersey: Prentice Hall Publisher, Upper Saddle River.

Hariri, R.H., Fredericks, E.M. ve Bowers, K.M. (2019). "Uncertainty in big data analytics: survey, opportunities, and challenges". *J Big Data 6*, 44.

Hathaway, M. ve Cross D. (2016). The Military Learner: The Acceptance of New Training Technology for C-130 Aircrews, *International Journal of Aviation, Aeronautics, and Aerospace*, 3(2), 1-29.

Hejazi, H., Rajab, H., Cinkler T. ve Lengyel, L. (2018). "Survey of platforms for massive IoT", *2018 IEEE International Conference on Future IoT Technologies* (Future IoT), 1-8.

Hooper, D., Coughlan, J., Mullen, M. (2008). "Structural Equation Modelling: Guidelines for Determining Model Fit". *Electronic Journal of Business Research Methods*, 6(1), 53-60.

Hu, H., Wen, Y. Chua, T. ve Li, X. (2014). "Toward Scalable Systems for Big Data Analytics: A Technology Tutorial," in *IEEE Access*, vol. 2, 652-687.

Jin, X., Wah, B.W., Cheng, X. ve Wang Y. (2015). "Significance and Challenges of Big Data Research", *Big Data Research 2*, 59–64.

Kalyoncuoğlu, S. (2018). "Tüketicilerin Online Alışverişlerindeki Sanal Kart Kullanımlarının Teknoloji Kabul Modeli İle İncelenmesi". *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 20*, 193-213, 10.32709/akusosbil.434874.

Karabay, B. ve Ulaş, M. (2017). Comparison of Commonly Used Tools in Big Data Processing*, 8th International Advanced Technologies Symposium*.

Khan, N., Alsaqer, M., Shah, H., Badsha, G., Abbasi, A. ve Salehian, S. (2018). "The 10 Vs, issues and challenges of big data", in *International Conference on Big Data and Education (ACM)*, 52–56.

Khan, W.Z., Aalsalem M.Y., Khan M.K. ve Arshad Q. (2016). "Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model". In: Park J., Jin H., Jeong YS., Khan M. (eds) *Advanced Multimedia and Ubiquitous Engineering. Lecture Notes in Electrical Engineering*, vol 393. Springer, Singapore.

Kılıçer, K. (2008). "Teknolojik Yeniliklerin Yayılmasını ve Benimsenmesini Arttıran Etmenler", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 8(2), 209-222.

Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: Guilford Press.

Kline, R.B. (2011) *Principles and Practice of Structural Equation Modeling*. New York: Guilford Press.

Kott, A. (2018). "Challenges and characteristics of intelligent autonomy for internet of battle things in highly adversarial environments", *2018 AAAI Spring Symposium Series.*

Kott, A. ve Alberts, D.S. (2017). "How Do You Command an Army of Intelligent Things?", *Computer*, *50*, 96-100.

Kott, A., Swami, A. ve West, B.J. (2016). "The Internet of Battle Things", *Computer*, 49(12), 70–75.

Kowatsch, T., Maass, W., van Kranenburg, R. ve Jacobs, T. (2012). *Social Acceptance and Impact Evaluation*. The Internet of Things Initiative.

Lai, P. (2017). "The literature review of technology adoption models and theories for the novelty technology". *Journal of Information Systems and Technology Management,* vol. 14, 21 – 38.

Levy, Y. ve Green, B. D. (2009). "An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of U.S. Navy combat information system", *Journal of Organizational and End User Computing*, 21(3), 1-23.

LimeSurvey: the online survey tool – open source surveys: https://www.limesurvey.org/

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang H. ve Zhao, W. (2017). "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", in *IEEE Internet of Things Journal*, 4(5), 1125-1142.

Lloret-Segura, S., Ferreres-Traver, A., Hernández-Baeza, A., ve TomásMarco, I. (2014). "Exploratory item factor analysis: A practical guide revised and up-dated]" *Anales de Psicología,* 30(3), 1151– 1169. doi:10.6018/analesps.30.3.199361

Macik, R. (2017). "The Adoption of The Internet of Things by Young Consumers – an Empirical Investigation", *Economic and Environmental Studies*, 17 (2), 363-388.

Meera, M. S. ve Rao, S. N. (2018). "Comparative Analysis of IoT protocols for a Marine IoT System, International Conference on Advances in Computing", *Communications and Informatics (ICACCI), Bangalore,* 2049-2053.

Mutahar, A. M., Daud, N. M., Ramayah, T., Isaac, O., ve Alrajawy, I. (2017). "Integration of Innovation Diffusion Theory (IDT) and Technology Acceptance Model (TAM) to Understand Mobile Banking Acceptance in Yemen: The Moderating Effect of Income". *International Journal of Soft Computing*, 12(3), 164–177.

Oktal, Ö., (2013). "Kullanıcıların Bilgi Sistemini Kabulünü Etkileyen Faktörlerin Utaut Pers- pektifinden İncelenmesi", *H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi*, 31(1), 153-170.

Oussous, A., Benjelloun, F.Z., Lahcen, A.A. ve Belfkih S. (2017). "Big data technologies: A survey", *Journal of King Saud University-Computer and Information Sciences*, 1-18.

Padhy, R. (2012). "Big Data Processing with Hadoop-MapReduce in Cloud Systems". *International Journal of Cloud Computing and Services Science (IJ-CLOSER).* 2. 10.11591/closer.v2i1.1508.

Ping Jr, R. A. (2004). “On assuring valid measures for theoretical models using survey data”. *Journal of Business Research*, 57(2), 125-141.

Roger, E. M., (1995). *Diffusion of Innovations*, Fourth edition, New York: Free Press.

Roger, E. M., (2003). *Diffusion of Innovations*, Fifth edition, New York: Free Press.

Sain, M., Kang Y. J. ve Lee, H. J. (2017). “Survey on security in Internet of Things: State of the art and challenges”. *19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong*, 699-704.

Salman, T., & Jain, R. (2019). A Survey of Protocols and Standards for Internet of Things. arXiv preprint arXiv:1903.11549.

Schreiber, J., Nora, A., Stage, F., Barlow, E. ve King, J. (2006). “Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review”. *Journal of Educational Research - J EDUC RES. 99*. 323-338. 10.3200/JOER.99.6.323-338.

Sezer, O.B, Dogdu, E., ve Ozbayoglu A.M. (2017). “Context Aware Computing, Learning and Big Data in Internet of Things: A Survey”, *IEEE Internet of Things Journal*, 5(1), 1-27.

Sha, K., Yang, T.A., Wei, W. ve Davari, S. (2019). “A survey of edge computing baseddesigns for IoT security”, *Digital Communications and Networks* 6.2 (2020): 195-202.

Sharma, C. ve Gondhi, D. N. K. (2018). “Communication Protocol Stack for Constrained IoT Systems”, *3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal*, 1-6.

Shek, Daniel ve Yu, Lu. (2014). “Confirmatory factor analysis using AMOS: A demonstration”. *International Journal on Disability and Human Development. 13.* 10.1515/ijdhd-2014-0305.

Suo, H., Wan, J., Zou, C. ve Liu, J. (2012). “Security in the Internet of Things: A Review”. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering*.

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., ... & Winkler, R. (2016, May). Analyzing the applicability of internet of things to the battlefield environment. In *2016 International conference on military communications and information systems (ICMCIS)* (pp. 1-8). IEEE..

Taber K. S., (2017). "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education", *Res. Sci. Educ.,* 1–24. DOI: 10.1007/s11165-016-9602-2.

Taherdoost H. (2017). "Determining Sample Size; How to Calculate Survey Sample Size", *International Journal of Economics and Management Systems*, no. 2, 237–239.

Teo, T. (2013). *Handbook of quantitative methods for educational research*. Rotterdam: SensePublishers.

Tonin, M. (2017). "The Internet of Things: Promises and Perils of a Disruptive Technology, NATO Parliamentary Assembly", *Science and Technology Committee,* 175 STCTTS 17 E bis.

Tortonesi, M., Morelli, A., Govoni, M., Michaelis, J., Suri, N., Stefanelli, C. ve Russell, S. (2016). "Leveraging Internet of Things within the Military Network Environment – Challenges and Solutions", *IEEE 3rd World Forum Internet Things* (WF-IoT).

Ursavaş, Ö. F., Şahin, S. ve Mcilroy, D. (2014). "Technology acceptance measure for teachers: T-TAM / Öğretmenler için teknoloji kabul ölçeği: Ö-TKÖ". *Eğitimde Kuram ve Uygulama,* 10(4), 885-917.

Vaccari C. (2014). *Big Data in Official Statistics* (PhD Thesis in Computer Science), University of Camerino.

Venkatesh V., Bala H. (2008). "Technology acceptance model 3 and a research agenda on interventions". *Decision Sciences*, 39(2), 273–315.

Venkatesh, V. ve Davis, F.D. (1996). "A Model of the Antecedents of Perceived Ease of Use: Development and Test". *Decision Sciences, 27,* 451-481.

Venkatesh, V., Morris, M. G., Davis, G. B. ve Davis, F. D. (2003). "User acceptance of information technology: toward a unified view", *MIS Quarterly*, 27(3), 425-478.

Vijayarani, S. ve Sharmila, S. (2016). "Research in Big Data – An Overview", *Informatics Engineering, an International Journal (IEIJ)*, 4(3), 1-20.

Voas, J., Agresti B. ve Laplante, P. A. (2018). "A Closer Look at IoT 's Things", in *IT Professional*, 20(3), 11-14.

Wakde, A., Shende, P., Waydande, S., Uttarwar S. ve Deshmukh G. (2018). "Comparative Analysis of Hadoop Tools and Spark Technology". *Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India*, 1-4.

Wang, H., Xu, Z., Fujita, H., & Liu, S. (2016). Towards felicitous decision making: An overview on challenges and trends of Big Data. *Information Sciences, 367,* 747-765.

Weng, F., Yang, R.J., Ho, H.J. ve Su, H.M. (2018). "A TAM-based study of the attitude towards use intention of multimedia among school teachers". *Appl. Syst Innov.* 1(3), 36–44.

Williams, B., Onsman, A. ve Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Journal of Emergency Primary Health Care*, 8(3).

Winarto, S. A. (2011). Analysis Effect of External Variables on System Usage and User Satisfaction Using Technology Acceptance Model (Empirical Study on Bank Pekreditan Rakyat in Semarang City Region). Faculty of Economics, Diponegoro University Semarang.

Wind, An Intel Company. (2015). *The Internet of Things For Defense*, White Paper.

Wrona, K. (2015). "Securing the Internet of Things a military perspective". *In Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT),* Milan, Italy.

Wu, J. ve Wang, S. (2005). "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model", *Information and Management*, 42(5), 719-729.

Yushi, L., Fei J. ve Hui, Y. (2012). "Study on Application Modes of Military Internet of Things (MIOT)", *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE).*

Zhao, J., Fang, S. ve Jin, P. (2018). "Modeling and Quantifying User Acceptance of Personalized Business Modes Based on TAM", *Trust and Attitude, Sustainability, MDPI, Open Access Journal*, 10(2), 1-26.

Zheng, D.E. ve Carter, W. A. (2015). *Leveraging the Internet of Things for a more efficient and effective military*, Technical Report, Rowman & Littlefield.

Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE*, *107*(8), 1738-1762.

EKLER

EK 1. Anket Formu-Türkçe

Bu anket çalışması, Nesnelerin İnterneti - Internet of Things'in (IoT) Askeri alanda kullanılabilirliğini incelemek, bu teknolojinin askeri alanda kabul modelini ortaya koymak maksadıyla yapılmaktadır. Anket sorularını cevaplarken, hali hazırda devam eden görevinizin yanında özellikle asker personelin geçmiş dönemde sahip olduğu **Kıt'a/Karagah** tecrübelerini göz önüne alması ankete büyük katkı sağlayacaktır. **Değerli katılımınız için teşekkürler.**

İlk defa duyanlar için kısaca **Nesnelerin İnterneti (IoT)**, çeşitli ağ çözümleri aracılığıyla, kullanıcı etkileşimi gerektirmeden (ya da sınırlı etkileşimle), sensörler ile donatılmış nesnelerin, birbirleriyle ve bilgisayarlarla ya da mobil cihazlarla genellikle bağımsız olarak iletişim kurdukları bir ekosistemdir. Akıllı saatler gibi giyilebilir cihazlar, sağlık bilgilerini toplayan sensörler, aydınlatma kontrolü gibi özellikleri olan akıllı ev sistemleri ve insan gücü ihtiyacını azaltırken güvenliği artıran otomatik güvenlik tarama sistemleri bu sistemin örneklerindendir.

Rabia SAYLAM (Öğr.Grv. - Doktora Öğrencisi)
Doç. Dr. Abdulkadir ÖZDEMİR (Danışman)

DEMOGRAFIK ÖZELLIKLER	
Cinsiyetiniz :	( ) Kadın ( ) Erkek
Yaşınız:	( ) 20-27 ( ) 28-33 ( ) 34-39 ( ) 40-46 ( ) 46 ve üstü
Eğitim Durumunuz:	( ) Ön Lisans ( ) Lisans ( ) Yüksek Lisans ( ) Doktora
Daha önce IoT kavramını duydunuz mu?	( ) Evet ( ) Hayır
Kişisel olarak IoT kullanımınız var mı?	( ) Evet ( ) Hayır

ANKET						
Sıra No	Sorular	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
1.	Askeri operasyona yönelik olarak IoT kullanmanın potansiyel risk olduğunu düşünüyorum.					
2.	Askeri lojistik alanda IoT kullanmanın potansiyel risk olduğunu düşünüyorum.					
3.	Askeri eğitim alanında IoT kullanmanın potansiyel risk olduğunu düşünüyorum.					
4.	IoT cihazlarının askeri ağlara erişiminin güvenlik açığı oluşturacağını düşünüyorum.					

5.	Askeri alanda IoT kullanmanın gizliliği riske attığını düşünüyorum.					
6.	Geleneksel askeri teçhizat bu teknoloji için yetersiz olacaktır.					
7.	IoT için gerekli olan sensör vb. ekipmanın, büyük veri işleme altyapısı ve yazılımlarının maliyetli olduğunu düşünüyorum.					
8.	IoT teknolojisine geçiş nedeniyle eski teçhizatların yenilenmesi süreci zaman (iş gücü) maliyeti getirecektir.					
9.	Askeri IoT için ağ bağlantı işleminin yüksek maliyet getireceğini düşünüyorum.					
10.	IoT sistemlerini operasyona yönelik olarak kullanmak uygundur.					
11.	IoT sistemlerini askeri lojistik alana yönelik olarak kullanmak uygundur.					
12.	IoT sistemlerini askeri eğitim alanına yönelik olarak kullanmak uygundur.					
13.	IoT sistemlerini mücadele etkinliği ve koordineli karar verme gibi gerçek zamanlı veri ihtiyacı barındıran askeri alanda kullanmak bu alanın doğası için değerdir.					
14.	Geleneksel askeri teçhizatın çeşitli uyarlamalarla IoT için kullanılması mümkündür.					
15.	Yükselen IoT, yüksek düzeyde bağlı bir çalışma ortamı olarak gelecekteki askeri savaş alanının Doktrin, Teknik, Taktik ve Prosedürlerini akıllıca değiştirecektir.					
16.	Askeri alanda, IoT sistemler tarafından sağlanan servisler güvenilirdir.					
17.	IoT donanımlarından sürekli veri almak mümkündür.					
18.	IoT'nin sağladığı verilere güvenilerek operasyon planlanabilir.					
19.	IoT verilerinden elde edilen sonuçlar karar süreçlerinde kullanılabilir.					
20.	IoT sistemler kullanmak askeri alanda (operasyon ya da lojistik) istenmeyen kayıpların azaltılmasını sağlar.					
21.	IoT sistemleri, askeri operasyonlar üzerinde daha fazla kontrol sağlar.					
22.	IoT sistemler kullanmak görevimin kritik yönlerini destekler.					
23.	IoT sistemler görev performansımı artırır.					
24.	Normalde mümkün olabileceğinden daha fazla iş yapmamı sağlar.					

25.	Genel anlamda askeri alanda IoT kullanmayı mantıklı buluyorum.					
26.	Askeri alanda IoT sistemleri kullanmayı öğrenmek benim için kolaydır.					
27.	IoT sistemiyle bütünleşmek çok fazla zihinsel çaba gerektirir.					
28.	IoT sistemlerini askeri alanda kullanmada ehil olmak çok fazla çaba gerektirir.					
29.	Genel anlamda, IoT sistemlerini askeri alanda kullanmayı kolay buluyorum.					

Öneri/Çekinceler	
Askeri alanda IoT kullanımına yönelik önerileriniz nelerdir? Bireysel ya da organizasyonel olarak **ne gibi alanlarda** kullanılabileceğini değerlendiriyorsunuz?	
Askeri alanda IoT kullanımına yönelik en büyük **çekinceniz** nedir?	

EK 2. Anket Formu-İngilizce

This survey study is carried out to examine the use of Internet of Things (Internet of Things) in the military field and to reveal the model of acceptance of this technology in the military field. In answering the survey questions, besides your current duty, the fact that taking into account your past **military field/HQ** experiences, if you are military personnel, will contribute greatly to the survey. **Thank you for your valuable participation.**

Who hear it for the first time, the Internet of Things (IoT) is an ecosystem in which the objects equipped with sensors communicate with each other and with computers or mobile devices independently through various network solutions, without the need for user interaction (or limited interaction). Wearable devices such as smart watches, sensors that collect health information, smart home systems with features such as lighting control and automated safety screening systems that increase safety while reducing the need for manpower are some examples of this ecosystem.

Rabia SAYLAM (Lecturer– Ph.D. Candidate)
Associate Professor Abdulkadir ÖZDEMİR (Advisor)

DEMOGRAPHIC QUESTIONS	
Gender :	( ) Female ( ) Male
Age:	( ) 20-27 ( ) 28-33 ( ) 34-39 ( ) 40-46 ( ) 46 and over
Education Status:	( ) Associate Degree ( ) Bachelor Degree ( ) Master's degree ( ) PhD Degree
Have you ever heard of the 'Internet of Things' term?	( ) Yes ( ) No
Have you ever used 'Internet of Things' devices made for personal usage?	( ) Yes ( ) No

SURVEY						
Order No.	Questions	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
1.	I think that using IoT for military operation is a potential risk.					
2.	I think that using IoT in military logistics is a potential risk.					
3.	I think that using IoT in military training is a potential risk.					
4.	I think that IoT devices' access to military networks would be a security breach.					
5.	I think that using IoT in the military field puts privacy at risk.					
6.	Traditional military equipment will be insufficient for this technology.					

7.	I think the equipment like sensors, large data processing infrastructure and software required for IoT are costly.					
8.	Due to the transition to IoT technology, the process of renewing old equipment will bring time (labor) cost.					
9.	I think the network connection process for military IoT will bring high cost.					
10.	It is convenient to use IoT systems for military operations.					
11.	It is appropriate to use IoT systems for military logistics.					
12.	It is appropriate to use IoT systems for military training.					
13.	IoT systems are value to the nature of this field where combat activity and coordinated decision-making require the need for real-time data.					
14.	It is possible to use traditional military equipment with various adaptations for IoT.					
15.	The rising IoT will change the Doctrine, Techniques, Tactics and Procedures of the future military battlefield wisely, as a highly connected working environment.					
16.	In the military field, the services provided by IoT systems are reliable.					
17.	It is possible to receive continuous data from IoT hardware.					
18.	Military Operations can be planned by relying on the data provided by IoT.					
19.	The results obtained from IoT data can be used in decision processes.					
20.	Using IoT systems reduces collateral damage in the military area (operation or logistics).					
21.	IoT systems provide greater control over military operations.					
22.	Using IoT systems supports critical aspects of my tasks.					
23.	IoT systems improve my task performance.					
24.	IoT systems allow me to do more work than normally possible.					
25.	I find it acceptable to use IoT in military in general.					
26.	Learning to use IoT systems in the military field seems easy for me.					
27.	Integrating with the IoT system requires a lot of mental effort.					

28.	To be able to use IoT systems in military field requires a lot of effort.					
29.	In general, I find it easy to use IoT systems in the military field.					

Suggestions / Concerns	
What are your suggestions for the use of IoT in the military field? What are the ways in which IoT systems can be used individually or organizationally?	
What is your biggest concern for the use of IoT in the military field?	

EK 3. Etik Kurulu Müsaade Yazısı

T.C.
ATATÜRK ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Etik Kurul Başkanlığı

Sayı : 88656144-000-E.1900101015 27.03.2019
Konu : Etik Kurul Onay Belgesi
(Doç.Dr.Abdulkadir ÖZDEMİR)

HUKUK MÜŞAVİRLİĞİNE

İlgi : 19.03.2019 tarihli ve 77040475-000-E.1900092159 sayılı belge.

İlgi'de kayıtlı yazınız gereği; Üniversitemiz İktisadi ve İdari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü öğretim üyesi ***Doç.Dr. Abdulkadir ÖZDEMİR*** danışmanlığında yapılacak olan Yönetim Bilişim Sistemleri Anabilim Dalı, 16013601002 numaralı doktora öğrencisi ***Rabia SAYLAM***'ın "***Büyük Veri Kaynağı Olarak Nesnelerin İnterneti (IoT)'nin Askeri Alanda Kullanılabilirliği***" konulu anket çalışması için Etik Kurul uygunluk-onay belgesi talebine ilişkin Etik Kurul Başkanlığımızın 27.03.2019 tarih ve 4 sayılı oturumunda alınan 23 no'lu kararı aşağıya çıkarılmıştır.

Bilgilerinizi ve gereğini arz ederim.

Prof.Dr. Sait UYLAŞ
Kurul Başkanı

Karar-23) Hukuk Müşavirliğinin; Üniversitemiz İktisadi ve İdari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü öğretim üyesi ***Doç.Dr. Abdulkadir ÖZDEMİR*** danışmanlığında yapılacak olan Yönetim Bilişim Sistemleri Anabilim Dalı, 16013601002 numaralı doktora öğrencisi Rabia SAYLAM'ın "***Büyük Veri Kaynağı Olarak Nesnelerin İnterneti (IoT)'nin Askeri Alanda Kullanılabilirliği***" konulu anket çalışması için Sosyal ve Beşeri Bilimler Etik Kurul Uygunluk-onay belgesi talebine ilişkin 19.03.2019 tarih ve E.1900092159 sayılı yazısı okundu.

Yapılan görüşmelerden sonra; ***Doç.Dr. Abdulkadir ÖZDEMİR*** danışmanlığında yapılacak olan Yönetim Bilişim Sistemleri Anabilim Dalı, 16013601002 numaralı doktora öğrencisi *Rabia SAYLAM*'ın "***Büyük Veri Kaynağı Olarak Nesnelerin İnterneti (IoT)'nin Askeri Alanda Kullanılabilirliği***" konulu anket çalışmasının gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak konuyla ilgili çalışmaların gerçekleştirilmesinde etik ve bilimsel yönden ***sakınca bulunmadığına*** mevcut oy birliği ile; ***Karar verildi.***

Atatürk Üniversitesi Merkez Kampüsü 25240 Yakutiye/ERZURUM Bilgi: Muhammet Emin ALAN
Elektronik Ağ: http://www.atauni.edu.tr
Kep Adresi: atauni@hs01.kep.tr

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Rabia SAYLAM
Doğum Yeri ve Tarihi	Denizli - 1986
Eğitim Durumu	
Lisans Öğrenimi	Hava Harp Okulu Bilgisayar Mühendisliği
Y. Lisans Öğrenimi	Hava Harp Okulu Bilgisayar Mühendisliği
Bildiği Yabancı Diller	İngilizce (2018 YDS : 87.50)
Bilimsel Faaliyetleri	Ulusal ve Uluslararası konferans ve dergilerde yayınlar
İş Deneyimi	
Stajlar	Hava Teknik Okullar Komutanlığı Muhabere Elektronik ve Bilgi Sistemleri Subayı Temel Eğitimi (6 ay)
Projeler	Hava Kuvvetleri Komutanlığı SAP Projesi
Çalıştığı Kurumlar	Hava Kuvvetleri Komutanlığı MSÜ Hava Harp Okulu
İletişim	
E-Posta Adresi	rsaylam@hvkk.tsk.tr
Tarih	02/07/2020